Release Notes for Cisco NAC Appliance, Version 4.5(1)

Revised: November 30, 2010, OL-16409-01

Contents

These release notes provide late-breaking and cumulative release information for Cisco® NAC Appliance, Release 4.5. This document describes new features, changes to existing features, limitations and restrictions ("caveats"), upgrade instructions, and related information. These release notes supplement the Cisco NAC Appliance documentation included with the distribution. Read these release notes carefully and refer to the upgrade instructions prior to installing the software.

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

Cisco NAC Appliance Releases

Cisco NAC Appliance Version	Availability
4.5.2.0 Cisco Clean Access Agent	July 9, 2009
4.5(1) ED	February 25, 2009
4.5 ED	October 21, 2008

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

System and Hardware Requirements

This section describes the following:

- Licensing
- Hardware Support
- Supported Switches for Cisco NAC Appliance
- VPN and Wireless Components Supported for Single Sign-On (SSO)
- Additional Support Information

Licensing

You must obtain and install Cisco NAC Appliance product licenses for the Clean Access Manager (CAM) and Clean Access Server (CAS) in order for your deployment to function. Install the CAM product license in the CAM License Form to initially access the CAM web admin console. Once you can access the CAM web console, upload the additional CAM HA license or CAS license(s) into the CAM (under **Administration > CCA Manager > Licensing**) in order to add CASs to the CAM, including the Cisco NAC network module. An OOB CAS license must be present to access the "OOB Management" module of the CAM. The **Licensing** page displays the types of licenses present after they are added.

Note that both CAM and CAS product licenses are generated based on the eth0 MAC address of the CAM. For High Availability (HA) pairs, you must generate an additional CAM HA license based on the eth0 MAC addresses of both Primary and Secondary CAMs and install it on the CAM whether you are adding a CAM HA-pair or CAS HA-pair.

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

Hardware Support

This section contains the following topics:

- Release 4.5 and Hardware Platform Support
- Release 4.5 and Cisco NAC Profiler

- Supported Switches for Cisco NAC Appliance

Release 4.5 and Hardware Platform Support

Starting from Cisco NAC Appliance Release 4.5, Cisco NAC Appliance software only supports and can only be installed on the following Cisco NAC Appliance platforms:

- Cisco CCA-3140
- Cisco NAC-3310
- Cisco NAC-3350
- Cisco NAC-3390
- Cisco NAC Network Module (NME-NAC-K9)

Note If upgrading a CCA-3140 appliance from 4.1(6) to 4.5 and later, refer to Known Issue with Upgrading CCA-3140 Appliance from Release 4.1(6) to 4.5, page 130 prior to upgrade.

Additionally, Cisco NAC Appliance Release 4.5 provides substantial changes and enhancements for product hardware support, installation and upgrade:

- A single product installation CD (ISO) provides the option to perform CD installation on CCA-3140 and NAC-3300 series appliance platforms. The installation package detects whether a CAS, CAM or SuperCAM was previously installed along with the software version.
- For NAC-3310 appliances, the **DL140** and **serial_DL140** boot installation directives are **no longer required** when installing the software starting from Release 4.5.
- **Web upgrade is no longer supported for upgrade to release 4.5**. To upgrade your CAM and CAS from 4.1(x) or 4.0(x) releases, you must copy the **cca_upgrade-4.5.1-NO-WEB.tar.gz** file to each CAM and CAS appliance and run the upgrade script via the command line. Refer to Upgrading to Release 4.5, page 111 and Known Issues with Web Upgrade in Release 4.1(x) and Earlier, page 127 for details.
- Neither the installation CD nor the upgrade file will execute if attempting to run them on a non-supported platform. Refer to Changes for 4.5 Installation/Upgrade, page 111 for additional details.
- Legacy customers on non-appliance platforms who wish to upgrade to release 4.5 will need to purchase a supported platform to install the release 4.5 software. Refer to Upgrading from Customer-Supplied Hardware to Cisco NAC Appliance Hardware Platforms, page 115 for additional details.

See also Features Optimized/Removed, page 22 for additional information.

Cisco NAC Network Module

The Cisco NAC Network Module for Integrated Services Routers (NME-NAC-K9) is a next generation service module for the Cisco 2811, 2821, 2851, 3825, and 3845 Integrated Services Routers (ISRs) that is supported starting from Cisco NAC Appliance, Release 4.1(2) and later. The Cisco NAC network module has the same software features as the Clean Access Server on a NAC-3300 series appliance, with the exception of high availability. NME-NAC-K9 does not support failover from one module to another.

Note Cisco NAC Network Module does not support Wireless Out-of-Band (OOB). The Wireless OOB feature introduced in Release 4.5 only supports Layer 2 OOB Virtual Gateway deployments that require no IP change. The NAC Network Module does not support this topology.

For further details, including software installation instructions, refer to *Getting Started with Cisco NAC Network Modules in Cisco Access Routers*.

Note You must run the same software version (e.g. 4.5) on all CAM/CAS appliances and CAS network modules in your network.

Release 4.5 and Cisco NAC Profiler

Release 4.5 includes version 2.1.8-37 of the Cisco NAC Profiler Collector component that resides on Clean Access Server installations. When upgrading Clean Access Server appliances (standalone or HA) to release 4.5, the upgrade script will check the version of the Collector and only upgrade it if version 2.1.8-37 is not already installed.

Refer to the *Release Notes for Cisco NAC Profiler* for software compatibility matrixes and additional upgrade and product information.

Supported Switches for Cisco NAC Appliance

Cisco NAC Appliance Wireless OOB Support

Table 1 lists the Wireless LAN Controller platforms that Cisco NAC Appliance supports for the Wireless Out-of-Band feature. Table 2 lists the recommended IOS versions for the switches used with Cisco NAC Appliance, Release 4.5. See Support for Wireless Out-of-Band Deployments, page 17 for further details.

Table 1 Recommended WLC Platforms to Support Wireless OOB in Release 4.5

Cisco Wireless LAN Controller Model	Cisco Wireless LAN Controller Version	Cisco NAC Appliance Version
Cisco 4400 Series Wireless LAN Controllers	5.1	4.5 and later
Cisco 2000 Series Wireless LAN Controllers		
Cisco Catalyst 3750G Integrated Wireless LAN Controller		
Cisco Catalyst 6500/7600 Series Wireless Services Module (WiSM)		
Cisco Wireless LAN Controller Module		

Note Starting from Release 4.5, administrators are able to update the object IDs (OIDs) of supported WLC platforms by performing a CAM update (under **Device Management > Clean Access > Updates**).

Table 2 lists the IOS versions and switch platforms that are tested and known to work with the Wireless OOB feature in Release 4.5. If you encounter issues with WOOB support and are running a minimum IOS version listed as supported for your existing hardware platform in *Switch Support for Cisco NAC Appliance*, you may need to upgrade the IOS on your switch to the version listed in Table 2.

Table 2 Switch IOS Versions Tested and Known to Work for WOOB in Release 4.5

Device Model	Recommended IOS Version
Catalyst 2960	12.2(35)SE5
Catalyst 3560/ 3560-E	12.2(25)SEE3
Catalyst 3750/ 3750-E	12.2(25r)SEE4
Catalyst 4500	12.2(31)SGA
Catalyst 6500	12.2(33)SXH1 12.2(33)SXH2a

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

- All switch models 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 3 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 3 VPN and Wireless Components Supported By Cisco NAC Appliance For SSO

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

[1] For additional details, see also Known Issues with Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs), page 131.

2. Release 4.5 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 4.5* and the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.5*.

Additional Support Information

Refer to *Support Information for Cisco NAC Appliance Agents* for additional details related to Windows/Mac OS X/Web Agent support.

Refer to *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for additional information on Cisco NAC Appliance hardware platforms and support information for Cisco NAC Appliance 4.1(x) and earlier releases.

Software Compatibility

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

- Release 4.5 Compatibility Matrix
- Release 4.5 CAM/CAS Upgrade Compatibility Matrix
- Release 4.5 Clean Access Agent Upgrade Compatibility Matrix

Release 4.5 Compatibility Matrix

Table 4 shows Clean Access Manager and Clean Access Server compatibility and the Clean Access Agent version supported with each 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 4 ***Release 4.5 CAM/CAS/Agent Compatibility Matrix***

Clean Access Manager [1, 2]	Clean Access Server [1, 2]	Cisco NAC Appliance Agents [3]		
		Windows	Mac OS X	Web Agent
4.5(1) [4]	4.5(1)	4.5.2.0 [5] 4.5.1.0 4.5.0.0	4.5.0.0 [5]	4.5.1.2
		4.1.7.0 [6]	4.1.3.0 [6]	-
		4.1.6.0 [6]		
		4.1.3.0 [6]		
		4.1.2.2 [6]		

Table 4 Release 4.5 CAM/CAS/Agent Compatibility Matrix (continued)

Clean Access Manager [1, 2]	Clean Access Server [1, 2]	Cisco NAC Appliance Agents [3]		
		Windows	Mac OS X	Web Agent
4.5	4.5	4.5.2.0 [6] 4.5.1.0 4.5.0.0	4.5.0.0 [5]	4.5.1.2
		4.1.7.0 [6]	4.1.3.0 [6]	-
		4.1.6.0 [6]		
		4.1.3.0 [6]		
		4.1.2.2 [6]		

1. Cisco NAC Appliance Release 4.5 only supports and can only be installed on the following Cisco NAC Appliance platforms: Cisco CCA-3140, Cisco NAC-3310, Cisco NAC-3350, Cisco NAC-3390, Cisco NAC Network Module (NME-NAC-K9). You cannot upgrade to or install release 4.5 on any other platform. See Hardware Support, page 2 and Changes for 4.5 Installation/Upgrade, page 111 for additional details.
2. Make sure that both CAM and CAS are of same version.
3. See Cisco NAC Appliance Agents, page 23 for details on each version of the Windows/Mac OS X/Web Agents.
4. When upgrading the CAM from version 4.1(1) and earlier, Agent files are automatically upgraded to the latest Agent version packaged with the CAM software image (e.g. 4.5.2.0). When upgrading the CAM from release 4.1(2) and later, the script will prompt you whether or not to upgrade the Agent files to the latest version. This allows administrators to schedule the Agent upgrade separately from the CAM/CAS server upgrade. Cisco recommends upgrading to the latest 4.5.2.0 Agent version as soon as possible.
5. 4.5.x.x Windows/Mac OS X Clean Access Agents are supported on 4.1(3) and later CAM/CAS releases for basic compatibility (login/logout) and AV/AS product support. The maximum available AV/AS support is based on the maximum version of the Clean Access Agent Setup or Patch (upgrade) file uploaded to the CAM as well as the maximum version of the Agent on the client. See *Support Information for Cisco NAC Appliance Agents, Release 4.5* for details. For full 4.5 features (including Mac OS posture), the 4.5.0.0 or later Agent must be run with the 4.5 CAM/CAS.
6. CAM/CAS release 4.5 supports 4.1.2.2 and later Agents for basic compatibility (login/logout) and AV/AS product support. The maximum available AV/AS support is based on the maximum version of the Clean Access Agent Setup or Patch (upgrade) file uploaded to the CAM as well as the maximum version of the Agent on the client. See *Support Information for Cisco NAC Appliance Agents, Release 4.5* for details. For full 4.5 features (including Mac OS posture) and 4.5 AV/AS product support, the 4.5.x.x Agent must be run with the 4.5 CAM/CAS.

Release 4.5 CAM/CAS Upgrade Compatibility Matrix

Table 5 shows 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 5 Release 4.5 CAM/CAS Upgrade Compatibility Matrix

Clean Access Manager [1]		Clean Access Server [1]	
Upgrade From:	To:	Upgrade From:	To:
4.1(x) [2] 4.0(x)	4.5(1) 4.5	4.1(x) [2] 4.0(x)	4.5(1) [3] 4.5

1. Cisco NAC Appliance Release 4.5 only supports and can only be installed on the following Cisco NAC Appliance platforms: Cisco CCA-3140, Cisco NAC-3310, Cisco NAC-3350, Cisco NAC-3390, Cisco NAC Network Module (NME-NAC-K9). You cannot upgrade to or install release 4.5 on any other platform. See Hardware Support, page 2 and Changes for 4.5 Installation/Upgrade, page 111 for additional details.

2. When upgrading the CAM from version 4.1(1) and earlier, Agent files are automatically upgraded to the latest Agent version packaged with the CAM software image (e.g. 4.5.2.0). When upgrading the CAM from release 4.1(2) and later, the script will prompt you whether or not to upgrade the Agent files to the latest version. This allows administrators to schedule the Agent upgrade separately from the CAM/CAS server upgrade. Cisco recommends upgrading to the latest 4.5.2.0 Agent version as soon as possible.
3. The Clean Access Server is shipped with a default version of the Cisco NAC Profiler Collector. See Release 4.5 and Cisco NAC Profiler, page 4 for details.

Release 4.5 Clean Access Agent Upgrade Compatibility Matrix

Table 6 shows Clean Access Agent upgrade compatibility when upgrading existing versions of the persistent Agents on clients after CAM/CAS upgrade.

Note Auto-upgrade does not apply to the temporal Cisco NAC Web Agent, since it is updated on the CAM under **Device Management > Clean Access > Updates > Update**.

Refer to *Support Information for Cisco NAC Appliance Agents* for additional details related to Windows/Mac OS X/Web Agent support.

Table 6 Release 4.5.x.x Agent Upgrade Compatibility Matrix

Clean Access Manager [1]	**Clean Access Server** [1]	**Clean Access Agent** [2]		
		Upgrade From:	**To Latest Compatible Windows Version:**	**To Latest Compatible Mac OS X Version:**
4.5(1) 4.5	4.5(1) 4.5	4.1.x.x [3, 4, 5] 4.0.x [3]	4.5.2.0 [6, 7, 8] 4.5.1.0 4.5.0.0	4.5.0.0 [6]

[1] Cisco NAC Appliance Release 4.5 only supports and can only be installed on the following Cisco NAC Appliance platforms: Cisco CCA-3140, Cisco NAC-3310, Cisco NAC-3350, Cisco NAC-3390, Cisco NAC Network Module (NME-NAC-K9). You cannot upgrade to or install release 4.5 on any other platform. See Hardware Support, page 2 and Changes for 4.5 Installation/Upgrade, page 111 for additional details.

[2] See Cisco NAC Appliance Agents, page 23 for details on each version of the Windows/Mac OS X/Web Agent.

[3] Auto-upgrade to the latest 4.5.x.x Agent is supported from any 4.0.0.0 and later Windows Agent and any 4.1.3.0 and later Mac OS X Agent. To upgrade earlier Mac OS X Agent versions, download the Agent via web login and run the Agent installation.

[4] When upgrading the CAM from version 4.1(1) and earlier, Agent files are automatically upgraded to the latest Agent version packaged with the CAM software image (e.g. 4.5.2.0). When upgrading the CAM from release 4.1(2) and later, the script will prompt you whether or not to upgrade the Agent files to the latest version. This allows administrators to schedule the Agent upgrade separately from the CAM/CAS server upgrade. Cisco recommends upgrading to the latest 4.5.2.0 Agent version as soon as possible.

[5] CAM/CAS release 4.5 supports 4.1.2.2 and later Agents for basic compatibility (login/logout) and AV/AS product support. The maximum available AV/AS support is based on the maximum version of the Clean Access Agent Setup or Patch (upgrade) file uploaded to the CAM as well as the maximum version of the Agent on the client. See *Support Information for Cisco NAC Appliance Agents, Release 4.5* for details. For full 4.5 features (including Mac OS posture) and 4.5 AV/AS product support, the 4.5.0.0 or later Agent must be run with the 4.5 CAM/CAS.

[6] 4.5.x.x Clean Access Agents are supported on 4.1(3) and later CAM/CAS releases for basic compatibility (login/logout) and AV/AS product support (Windows only). The maximum available AV/AS support is based on the maximum version of the Clean Access Agent Setup or Patch (upgrade) file uploaded to the CAM as well as the maximum version of the Agent on the client. See *Support Information for Cisco NAC Appliance Agents, Release 4.5* for details. For full 4.5 features (including Mac OS posture), the 4.5.0.0 or later Agent must be run with the 4.5 CAM/CAS.

[7] Cisco NAC Appliance release 4.5 no longer supports Windows ME/98/NT client operating systems and you cannot install the Windows Clean Access Agent version 4.5.0.0+ to Windows ME/98/NT client machines. For details, see Windows ME/98/NT OS Support Removed, page 23.

8. For checks/rules/requirements, version 4.1.1.0 and later Windows 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.

Determining the Software Version

Clean Access Manager (CAM) Version

- SSH or console to the machine and type: `cat /perfigo/build`
- CAM web console: **Administration > CCA Manager > Software Upload | Current Version**

Clean Access Server (CAS) Version

- SSH or console to the machine (or network module) and type `cat /perfigo/build`
- CAS web console (https://<*CAS_eth0_IP_address*>/admin): **Administration > Software Upload | Current Version**
- CAM web console: **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Misc > Upgrade Logs | Current Version**

Cisco NAC Appliance Agent Version (Windows, Mac OS, Web Agent)

- CAM web console: **Monitoring > Summary**
- Clean Access Agent taskbar menu: right-click **About** for Agent version; right-click **Properties** for AV/AS software installed and Discovery Host (used for L3 deployments).

Cisco Clean Access Updates

- CAM web console: **Device Management > Clean Access > Updates > Summary**

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 4.5(1), page 9
- New Features and Enhancements in Release 4.5(0), page 11

Enhancements in Release 4.5(1)

General Enhancements

- CAS Fallback Behavior Enhancement, page 10
- CAS HA Pair Link-Detect Configuration Enhancement, page 10
- DHCP Failover Behavior Enhancement, page 11
- Cisco NAC Appliance API Enhancement, page 11
- Supported AV/AS Product List Enhancements (Version 74), page 11

Cisco NAC Appliance Agents Enhancements

- Windows Clean Access Agent, page 23
- Mac OS X Clean Access Agent, page 24

- Cisco NAC Web Agent, page 25

General Enhancements

CAS Fallback Behavior Enhancement

In Cisco NAC Appliance Release 4.5(1), 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 4.5(1), 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 4.5(1), this enhancement also introduces a 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 4.5(1) 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)

Refer to "CAS Fallback Policy" in the *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide, Release 4.5(1)* for further details. s

CAS HA Pair Link-Detect Configuration Enhancement

Cisco NAC Appliance Release 4.5(1) 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 88.

DHCP Failover Behavior Enhancement

Cisco NAC Appliance Release 4.5(1) 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 88.

Cisco NAC Appliance API Enhancement

Two new functions are added to the Cisco NAC Appliance API (cisco_api.jsp):

- checkmac—queries the Device Filters list to check if a particular MAC address exists.
- getmaclist —fetches the entire Device Filters list.

See CSCsw67822, page 91.

Supported AV/AS Product List Enhancements (Version 74)

- See Clean Access Supported AV/AS Product Lists, page 26 for the latest AV/AS product charts.
- See Supported AV/AS Product List Version Summary (Windows), page 27 for details on each update to the list.

New Features and Enhancements in Release 4.5(0)

General Enhancements

- Policy Import/Export, page 12
- CAM/CAS SSL Certificate Management Enhancement, page 14
- CAM/CAS Software Upload Page Enhancements, page 15
- Database Snapshot Upgrade Enhancement, page 16
- Clean Access Manager High Availability User Interface Enhancement, page 16
- CAM/CAS Support Log Level Settings Enhancement, page 16
- CAM/CAS High Availability Configuration Able to Detect Hard-Drive Failure, page 16

Out-of-Band Enhancements

- Support for Wireless Out-of-Band Deployments, page 17
- Assign Restricted VLAN for OOB Client Machines When Disconnected, page 18
- Certified Device List/Online User List Enhancements, page 19
- Out-of-Band Shield Enhancement, page 20
- Out-of-Band Discovered Clients Cleanup, page 20

FIPS-Related Security Enhancements

- Pre-Login Banner, page 21
- Strong Password Support for Root Admin Users, page 21
- External Authentication Server Support for Web Administrator Login, page 22

Features Optimized/Removed

- Support for Cisco NAC Appliance/NME-NAC Platforms Only, page 22
- Windows ME/98/NT OS Support Removed, page 23
- Default CAM Web Console Password Removed, page 23

Cisco NAC Appliance Agents Enhancements

- Windows Clean Access Agent, page 23
- Mac OS X Clean Access Agent, page 24
- Cisco NAC Web Agent, page 25

Clean Access Supported AV/AS Product Lists Enhancements

- Supported AV/AS Product List Version Summary (Windows), page 27
- Supported AV/AS Product List Version Summary (Mac OS X), page 57
- Clean Access AV Support Chart (Windows Vista/XP/2000), page 34
- Clean Access AS Support Chart (Windows Vista/XP/2000), page 49
- Clean Access AV Support Chart (Mac OS X), page 58
- Clean Access AS Support Chart (Mac OS X), page 59

General Enhancements

Policy Import/Export

The Policy Import/Export feature allows administrators to propagate device filters, traffic and remediation policies, and OOB port and VLAN profiles from one CAM to several CAMs. All CAMs must run release 4.5 or later to enable Policy Sync. Policies are defined on a single CAM which you configure as the Policy Sync Master, and a maximum of 10 CAMs or 10 CAM HA-pairs are supported as Policy Sync Receivers. You can export policies using Manual Sync or Auto Sync. Auto Sync allows you to schedule an automatic Policy Sync once every *x* number of days.

Note On CAM HA-pairs, Policy Sync settings are disabled for the Standby CAM.

To perform Policy Sync, the Master and Receiver CAMs must be configured to authorize each other using the DN from the SSL certificate of each CAM or CAM HA pair. For production deployments, CA-signed SSL certificates should be used.

- Policy Sync Policies, page 13 lists the configurations that are subject to Policy Sync.
- Policies Excluded from Policy Sync, page 13 is a list (non-exhaustive) of policies that are not included in Policy Sync.

Policy Sync Policies

During Policy Sync, the Master configuration completely overrides (and clears) the existing Receiver configuration for the policies that are configured for Policy Sync, such as OOB profiles or user roles. Policy Sync enables the following global configurations to be propagated from a Master CAM.

- **Role-Based Policies**
  - User roles with associated global traffic control policies (IP-based, Host-based, L2 Ethernet) and session timers

    Note: This includes customized policies and the Default Host Policies, Default L2 Policies from Cisco Updates that are on the Master CAM.
  - Global device filters with access type: Role or Check
  - Clean Access Agent rules (Cisco and AV/AS), requirements, rule-requirement mappings, and role-requirement mappings

    Note: This includes customized checks/rules and Cisco Checks & Rules and Supported AV/AS Product List (Windows & Macintosh) from Cisco Updates that are on the Master CAM and associated to rules/requirements.
- **Non Role-Based Policies**
  - Global device filters with access type: Allow, Deny or Ignore
- **OOB Policies** (does not include switch information (i.e. Device/SNMP))
  - Port Profiles
  - VLAN Profiles

Note

- OOB policies should not be selected for Policy Sync if a Master is not configured for OOB, as this will clear any OOB policies on the Receiver CAM.
- If you have an OOB CAM and any legacy CAMs with IB-Only licenses, make sure to configure the OOB CAM as the Master CAM and the legacy CAMs as Receivers.

Note Policy Sync exports all global device filters created on the Master CAM to the Receiver CAMs. Any MAC address which is in the Master CAM's global Device Filter list will be exported, including Cisco NAC Profiler generated filters.

Policies Excluded from Policy Sync

Policies/configurations that are not listed under Policy Sync Policies are not subject to Policy Sync and are otherwise left alone on the Receiver CAM after a Policy Sync. The following non-exhaustive list describes the kinds of policies/configurations that are **not included** for Policy Sync:

- Cisco NAC Appliance Agents. The Master and Receiver CAMs retain the Agent versions and Agent download and distribution policies they already have. You will still need to require use of the Agent for a role and operating system (e.g. Agent Login/Distribution pages) on each CAM.
- Local configuration on the Receiver CAMs such as CAS-specific traffic policies or device filters. Local policies stay the same on the Receiver CAM and are not removed after a Policy Sync.
- OOB switch configurations such as **Device** Profiles and **SNMP Receiver** settings.
- Clean Access Agent Updates for Cisco NAC Appliance Agents (Windows/Mac OS/Web), OS Detection Fingerprinting, and Switch OIDs
- User Login pages, Local Users, or Bandwidth policies (see also CSCsu78379, page 75) associated with a user role.
- Subnet filters
- Authentication server configurations
- Certified Device List or Timers
- Network Scanning (Nessus) configuration

Note Cisco recommends that you configure auto update settings on the Master and Receiver CAMs (under **Device Management > Clean Access > Updates > Update**) and ensure that the Master CAM has the latest Cisco Updates before you perform a Policy Sync.

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

- New **Administration > CCA Manager > Policy Sync** configuration module
- Red-colored product banner for CAM web consoles of Policy Sync Receivers

For configuration information, refer to the "Policy Import/Export" section of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide*.

CAM/CAS SSL Certificate Management Enhancement

Release 4.5 updates the temporary SSL certificate generation, the CA-signed certificate request mechanism, and certificate/Private Key import and export operations (included in Release 4.1(6)) to better segregate and more clearly define the SSL certificate functions on the CAM and CAS.

When you perform a fresh install of release 4.5, the default Certificate Authority trust store contains only the private CA required to generate a temporary certificate suitable for lab environments. One of the first steps administrators must take once SSL communications between the CAM and CAS have been established is to generate Certificate Signing Requests (CSRs) from a trusted third-party certificate authority for the CAM and CAS and import the resulting certificates onto the CAM and CAS once they are generated and returned from the CA.

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

- **Administration > CCA Manager > SSL > X509 Certificate**
- **Administration > CCA Manager > SSL > Trusted Certificate Authorities**

This enhancement adds the following CAM web console page:

- **Administration > CCA Manager > SSL > x509 Certification Request**

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

- **Administration > SSL > X509 Certificate**

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

This enhancement adds the following CAS web console page:

- **Administration > SSL > x509 Certification Request**

For configuration information, refer to the "Manage CAM SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide* and "Manage CAS SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide*.

See also Known Issues with www.perfigo.com Root CA, page 129 for additional details.

CAM/CAS Software Upload Page Enhancements

Note **Web upgrade is no longer supported for upgrade to release 4.5**. To upgrade your CAM and CAS from 4.1(x) or 4.0(x) releases, you must copy the **cca_upgrade-4.5.1-NO-WEB.tar.gz** file to each CAM and CAS appliance and run the upgrade script via the command line. Refer to Upgrading to Release 4.5, page 111 and Known Issues with Web Upgrade in Release 4.1(x) and Earlier, page 127 for details.

With removal of the web upgrade functionality, previous web console pages are modified for release 4.5. For administrator convenience and backward compatibility, release 4.5 maintains the CAM/CAS web console pages that were related to web upgrade in prior releases, but modifies them to allow file upload and viewing of upgrade log information only. The "**Apply**" and "**Upgrade Agent?**" columns and functionality are removed. Note that upgrade log files are preserved on these pages for upgraded systems only.

This affects the following CAM/CAS web console pages:

- CAM: **Administration > CCA Manager > Software Upload** ("System Upgrade" has become Software Upload" and "Upgrade Agent" and "Apply" options are removed)
- CAM: **Device Management > CCA Servers > Manage [CAS_IP] > Misc > Upgrade Logs** (upload function removed completely; "Update" is now "Upgrade Logs", "Apply" and "Notes" options are removed)
- CAS: **Administration > Software Upload** ("Software Update" link changed to "Software Upload", "Apply" and "Notes" options are removed)

Note Starting from 4.5, successfully web-uploaded upgrade files are automatically placed in the /store directory of the CAM of the CAS, and the release 4.5 upgrade script will not run in any directory not under /store.

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.

See Known Issues with Web Upgrade in Release 4.1(x) and Earlier, page 127 for further details.

Database Snapshot Upgrade Enhancement

Release 4.5 enhances the database snapshot re-importing process for users who back up their CAM system snapshot before upgrading and are forced to re-import the database following an upgrade failure (as might be the case if a planned HA upgrade does not succeed). Although re-importing a snapshot from a previous Cisco NAC Appliance release is not allowed in release 4.0(x) or 4.1(x), this function is possible in Cisco NAC Appliance Release 4.5 because, as long as the CAM database schema does not change at the time of upgrade, you can now re-import an existing snapshot from a prior release and attempt the upgrade again.

The process and method of backing up the database and re-importing the snapshot does not change from previous releases, but the time it takes to re-import and the reliability of the process has also improved dramatically over prior releases.

Clean Access Manager High Availability User Interface Enhancement

In Cisco NAC Appliance release 4.5, the HA-Standby CAM web console now matches the HA-Active web console, but disables (greys out) or hides non-applicable menu options. Some additional HA-Active web console menu and submenu items are also enabled to the HA-Standby web console:

- The HA-Standby web console allows you to view the Clean Access Server list via the new **CCA Servers** sub-menu option under **Device Management**.
- The HA-Standby web console allows you to view the default system Monitoring > Summary page displayed when logging into the HA-Active web console.
- The HA-Standby web console displays **CCA Manager** management options similar to those found on the HA-Active web console. HA-Active web console options that are not available on the HA-Standby console are hidden or disabled (greyed out).

CAM/CAS Support Log Level Settings Enhancement

In Cisco NAC Appliance release 4.5, the CAM/CAS event log settings options have been expanded, offering greater granularity in available log levels and improved control over the type and detail of support log entries recorded for the various event log categories on the CAM/CAS. One key improvement is the ability to turn logging *off* altogether for one or more particular event log categories, thus reserving available logging disk space for more critical event log types.

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

- **Administration > CCA MAnager > Support Logs**—page now features six log levels for each of the five log categories: **OFF**, **ERROR**, **WARN**, **INFO**, **DEBUG**, and **TRACE**

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

- **Monitoring > Support Logs**—page now features six log levels for each of the five log categories: **OFF**, **ERROR**, **WARN**, **INFO**, **DEBUG**, and **TRACE**

CAM/CAS High Availability Configuration Able to Detect Hard-Drive Failure

In Cisco NAC Appliance release 4.5 deployments configured for High Availability, nodes that undergo hard disk failure now automatically reboot, thus triggering the High Availability failover mechanism. With previous releases of Cisco NAC Appliance, it was possible for an active CAM/CAS to experience a hard-drive failure yet still respond to heartbeat packets from the standby CAM/CAS, thus never failing over to the standby even though no user authentication/access could take place in the system and the administrator was no longer able to manage the “active” CAM/CAS. The only way to handle this issue was to manually shut the active CAM/CAS down so that automatic HA failover would kick in.

For more information, see CSCso51899, page 103.

Out-of-Band Enhancements

Support for Wireless Out-of-Band Deployments

Note Cisco NAC Appliance Release 4.5 introduces Wireless OOB support which only supports Layer 2 OOB Virtual Gateway deployments that require no IP change. Because the Cisco NAC Network Module does not support this topology, the NAC Network Module is not supported for Wireless OOB.

Release 4.5 introduces Out-of-Band support for wireless clients logging into the Cisco NAC Appliance system. Previous releases of Cisco NAC Appliance support wireless client machines, but only in In-Band mode, with all traffic between the client machine and the internal network always passing through the Clean Access Server. To address increasing demand for bandwidth from more and more client machines authenticating via Cisco NAC Appliance, administrators can now configure the CAM to manage client authentication information from one or more Wireless LAN Controllers (WLCs), similar to the way the CAM manages other switch devices in the network, prompting switches to change the Authentication (or Quarantine) VLAN to the Access VLAN for client ports and vice-versa. To support wireless Out-of-Band communication, the CAS remains inline only until the wireless user is authenticated and the WLC is able to switch the client machine VLAN assignment from the Authentication VLAN to the Access VLAN. After that, all traffic from the wireless client can bypass the CAS to access the network directly.

Note You can only deploy CASs supporting wireless client machine authentication in Virtual Gateway mode.

Some strict guidelines dictate how WLCs and Cisco NAC Appliance interact when authenticating wireless client machines and how they keep one another informed of client status:

- WLCs must be configured to interact with the CAM using SNMP read, write, and trap functions.
- Each SSID/dynamic interface on the WLC must have both an Authentication (Quarantine) VLAN and Access VLAN configured.
- If the Access VLAN is the same for two or more SSIDs, those SSIDs should also have the same Authentication (Quarantine) VLANs.
- Authentication and Access VLANs are defined on the WLC and changes between the two are transmitted to the CAM using SNMP traps—administrators do not assign VLANs from the CAM via user role assignments or otherwise.
- When a wireless user logs off, the WLC also sends SNMP information to the CAM to ensure the user ID is removed from the Online Users List. Likewise, if the administrator must kick any users out of the Online Users List, the CAM informs the WLC via SNMP and the WLC automatically assigns the wireless client to the Authentication (Quarantine) VLAN once more.
- If Single Sign-On (SSO) is required for wireless users, the WLC must also be configured to transmit RADIUS accounting packets to the CAS.

- Administrators need to configure a device profile for the WLC on the CAM (under **OOB Management > Profiles > Device > New**) and add the new device to the OOB devices list (under **OOB Management > Devices > Devices > New**) in order to manage the WLC like a switch.

Note Administrators do not need to configure any Port Profiles on the CAM to manage WLCs.

Cisco NAC Appliance only interoperates with Cisco Wireless LAN Controllers. Refer to Table 1, "Recommended WLC Platforms to Support Wireless OOB in Release 4.5" for a list of supported Cisco Wireless LAN Controller platforms.

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

- "Switch Management" left navigation module becomes "OOB Management"
- **OOB Management > Profiles > Group > List/Edit**—"Switch" column becomes "Device"
- **OOB Management > Profiles > Device > List/New/Edit**—"Switch" column becomes "Device"
- **OOB Management > Devices > Devices > List/New/Search**—"Switch" column becomes "Device"
- **OOB Management > Devices > Discovered Clients** — Two new tabs: Wired Clients, Wireless Clients
- **OOB Management > Devices** | new **WLC[x.x.x.x]** Wireless LAN Controller category "Config" icon only displays "Basic" and "Group" subtabs (no "Advanced" subtab like the Switch category) and the "Ports" icon available for switch device entries is grayed out/disabled for all WLC table entries.
- **Device Management > Filters > Devices > New/Edit**—Descriptions now include additional information on WLC behavior for Wireless Out-of-Band

For additional pages affected, see also Certified Device List/Online User List Enhancements, page 19.

For configuration information, refer to the "Configuring Wireless Out-of-Band Deployments" section of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide*.

Assign Restricted VLAN for OOB Client Machines When Disconnected

In Cisco NAC Appliance Release 4.5, administrators can now configure which VLANs should be assigned to switch ports after an OOB client goes offline and the CAM receives a linkdown SNMP trap from the switch. In Cisco NAC Appliance Releases 4.1(3) and 4.1(6), anytime an OOB client machine disconnected from the network, the CAM would automatically change the VLAN on the switch port to the Authentication VLAN. (In prior releases of Cisco NAC Appliance—release 4.1.2.1 and earlier—the CAM would simply allow the switch port to remain unchanged, thus the port would very often remain in the Access VLAN until the next client machine attempted to access the Cisco NAC Appliance network via that same port.) Release 4.5 allows you to configure which VLAN assignment to make using the enhanced dropdown menu options available with the existing **Remove out-of-band online user when SNMP linkdown trap is received** option. There are three settings you can use:

- **do nothing**—The CAM does not perform any unilateral VLAN reassignment for switch ports where OOB clients have disconnected from the network. Other options in your Port Profile configuration (for example, having enabled and configured the **Change to [Auth VLAN | Access VLAN] if the device is certified but not in the out-of-band user list** option) still affect the VLAN assignment. Essentially, unless otherwise configured, the switch port remains on the Access VLAN when you choose the **do nothing** setting.
- **change to Auth VLAN**—The CAM automatically assigns switch ports to the Authentication VLAN for OOB clients that have disconnected and for which a linkdown SNMP trap has been received.

- **change to Restricted VLAN**—You can configure the CAM to assign a specific VLAN profile or VLAN ID (that can be separate from both the Authentication and Access VLANs) to switch ports where OOB clients have disconnected from the network. The administrator can configure one or more custom VLANs (perhaps featuring varying levels of network access) for client machines that fall into this category and assign one of them to switch ports where OOB clients have disconnected. This "restricted" VLAN assignment can also be useful to provide basic level access for OOB users when the CAM has gone offline, for example.

If the administrator disconnects the client machine (the administrator kicks the user out of the OOB Online Users list), the CAM bounces the switch port and the port is automatically assigned to the Authentication VLAN by default. If the administrator disconnects the client and the **Remove out-of-band online user without bouncing the port** option is enabled, the client machine experiences the same net effect because when the CAM removes the OOB user from the OOB Online Users list, it also assigns the client machine to the Authentication VLAN.

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

- **OOB Management > Profiles > Port > New | Edit**—the existing **Remove out-of-band online user when SNMP linkdown trap is received** option now features a dropdown menu allowing you to configure the VLAN assignment for OOB client machines when they have disconnected and are reconnecting to the network.

For more information, see also CSCso76150, page 104.

Certified Device List/Online User List Enhancements

The Certified Devices List (CDL) allows administrators to track users and devices that have met posture assessment. The Online Users Lists (OULs) track In-Band and Out-of-Band authenticated users logged into the network. Unlike the In-Band and Out-of-Band Online User Lists (OUL), which allow you to specify which fields are displayed on the OUL, you cannot choose the fields displayed in the Certified Devices List (CDL).

- For prior 4.1(x) releases, the CDL specifies: **Clean Access Server**, **MAC Address**, **User**, **Provider**, **Role**, **VLAN**, **Time**, and **Switch**. In release 4.5, the CDL specifies: **CCA Server**, **MAC Address**, **User**, **Provider**, **Role**, **VLAN**, **Time**, and **Location**.

  For 4.5 OOB users, the new **Location** column on the CDL and OUL displays the location of the user (switch/port or WLC/SSID) in OOB mode. This location should match the one listed on the OOB Online User Page when the client passes posture assessment for the first time.

- In release 4.1(x), the **Switch** field was an inactive string/link for IB users. In release 4.5, **Location** fields associated with switch entries are simply left blank. for IB users.
- In release 4.1(x), the **Switch** and **Port** fields in the In-Band and Out-of-Band Online Users lists would inform the administrator where the client machine was connected to the access network. In release 4.5, to accommodate Wireless Out-of-Band user entries, the lists of online users now show identify client machine access points in the more generic **Location** column.

These enhancement affects the following CAM web console pages:

- **Device Management > Clean Access > Certified Devices > Certified Devices List | Location** field
- **Device Management > Clean Access > Certified Devices > Certified Devices List**—"Switch" column becomes "Location"
- **Monitoring > Online Users > View Online Users > Out-of-Band**—"Switch" and "Port" columns combine to become "Location"
- **Monitoring > Online Users > Display Settings > Out-of-Band**—"Switch" and "Port" checkboxes become single "Location" checkbox

See also Support for Wireless Out-of-Band Deployments, page 17.

Out-of-Band Shield Enhancement

Cisco NAC Appliance release 4.5 features enhanced SNMP polling behavior for Out-of-Band managed switches to ensure that the CAM is able to communicate with switches experiencing network issues when they return to normal operation. Previous releases of Cisco NAC Appliance would occasionally lose communication with managed switches altogether before the administrator was forced to step in and clear up the switch behavior and re-establish CAM-to-switch communication.

You can configure this feature using the following settings in the **smartmanager_conf** table of the CAM CLI:

- **OobSnmpErrorLimit**—This is maximum number of consecutive SNMP timeout failures. If the number of consecutive failures reaches this value, the switch is disabled. If the administrator specifies the limit so that it is equal to or is less than 0, this feature is disabled. The default value is 10.
- **OobSnmpRecoverInterval**—This is the internal time period (in minutes) that the recovery process waits to check disabled switches to see if they have come back online. The default value is 10.

For more information, see CSCsq75149, page 105.

Out-of-Band Discovered Clients Cleanup

Cisco NAC Appliance release 4.5 enhances existing Out-of-Band client and OOB Online Users list maintenance. Some system configurations can result in OOB clients and OOB online users remaining in the CAM Discovered Clients and OOB Online Users lists even when the switch through which they originally accessed the network is no longer a managed resource, and when clients log in only once and never sign into the Cisco NAC Appliance network again. This solution introduces two new verification features on the CAM:

- When a managed switch is deleted from the Devices list, the CAM now also deletes associated OOB online users and discovered clients.
- The CAM now features configurable timers for discovered client sessions to check if they have expired. If the session has expired and the client is not active, the CAM deletes those entries and removes the associated OOB online user entry from the Online Users List.

  Two optional processes can be activated every day to clean up the wired and wireless discovered clients respectively. (These two processes are disabled by default.) To enable these processes, set **OobDiscoveredClientCleanup** to **yes** in the CAM CLI's **smartmanager_conf** table. If enabled, the processes will run at 1:30AM for wired clients and 2:30AM for wireless clients.

  For wired discovered clients, the process removes the entry if any of the following conditions is met:

  - The switch is not managed.
  - The port is not managed.
  - The port is down and there is no OOB online user on that port.
  - The port is down and the **Remove out-of-band online user when SNMP linkdown trap is received** option is checked in the port profile (the OOB user is also removed in this case).

  For wireless discovered clients, the process removes the entry when any of the following conditions is met:

  - The WLC is not managed/associated with the CAM.
  - The MAC address is not known to the WLC.

For more information, see CSCsl77438, page 100.

FIPS-Related Security Enhancements

Although Cisco NAC Appliance is not certified for FIPS, release 4.5 includes the following FIPS-related security enhancements.

Pre-Login Banner

Cisco NAC Appliance release 4.5 introduces a new optional, customizable administrator welcome screen (called a "Pre-login Banner") that you can use to present a broad range of messages, including warnings, system/network status, access requirements, and so on to administrator users before they enter authentication credentials in the CAM/CAS. Administrators can specify the text of the Pre-login Banner by enabling this feature on the appliance during initial configuration, logging into the command-line console, and editing the **/root/banner.pre** file. The text of the Pre-login Banner appears in both the web console interface and the command-line interface when admin users log into the CAM/CAS.

This feature is disabled by default. You can enable or disable this feature during the initial CAM/CAS configuration CLI session or using the **`service perfigo config`** CLI command.

Strong Password Support for Root Admin Users

To offer increased security against potential unauthorized access to Cisco NAC Appliance, the CAM and CAS root admin password you specify during initial system configuration must now meet strong password standards requiring that the password be at least 8 characters long and contain at least two characters from each of the following classes:

- Lower-case letters
- Upper-case letters
- Numbers (digits)
- Special characters (like !@#$%^&*~)

For example, **`1o-9=OnE`** is a valid password, but the password **`10-9=One`** does not satisfy the requirements because it does not contain two characters from each category.

Note If the first character of a password is an upper-case letter, that character is not counted toward the minimum number of required upper-case letters (two) when determining whether or not the correct number of characters exists in the password.

If the last character of a password is a digit, that character is not counted toward the minimum number of required digits (two) when determining whether or not the correct number of characters exists in the password.

See Changes for 4.5 Installation/Upgrade, page 111 for additional information on admin passwords.

External Authentication Server Support for Web Administrator Login

In Cisco NAC Appliance Release 4.5, you can authenticate administrator user credentials through an external Kerberos, LDAP, or RADIUS authentication server just like regular users when they log in to the Cisco NAC Appliance network. When an administrator user who has been configured to authenticate via an external server logs in, the CAM directs the user credentials to the external authentication server for validation. This login behavior also applies to administrator users logging into an associated CAS. If the CAS has been added to the CAM and the administrator user profile is configured to validate credentials via an external authentication server, the users credentials are also directed to the external authentication server when the administrator user logs into the CAS.

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

- **Administration > Admin Users > New | Edit**—this configuration window now includes an **Authentication Server** dropdown list where you can authenticate administrator user credentials via **Built-in Admin Authentication** (local CAM) or using an external Kerberos, LDAP, or RADIUS authentication server configured under **User Management > Auth Servers > New | Edit**.

Note When specifying an external authentication server for admin login, the **Password** and **Confirm Password** fields that support Built-in Admin Authentication disappear from the configuration window.

Features Optimized/Removed

The following functions have been optimized or removed in Cisco NAC Appliance Release 4.5:

- Support for Cisco NAC Appliance/NME-NAC Platforms Only
- Web Upgrade Support Removed
- Default CAM Web Console Password Removed
- Windows ME/98/NT OS Support Removed

Support for Cisco NAC Appliance/NME-NAC Platforms Only

Cisco NAC Appliance Release 4.5 only supports and can only be installed on the following Cisco NAC Appliance platforms: Cisco CCA-3140, Cisco NAC-3310, Cisco NAC-3350, Cisco NAC-3390, Cisco NAC Network Module (NME-NAC-K9). You cannot upgrade to or install release 4.5 on any other platform. See Hardware Support, page 2 and Changes for 4.5 Installation/Upgrade, page 111 for additional details.

Web Upgrade Support Removed

Web upgrade is no longer supported to upgrade from release 4.0(x)/4.1(x) to release 4.5, or from release 4.5 to a later release. For details, refer to CAM/CAS Software Upload Page Enhancements, page 15 and Known Issues with Web Upgrade in Release 4.1(x) and Earlier, page 127.

Default CAM Web Console Password Removed

For new installations of Cisco NAC Appliance, there is no longer a default **cisco123** CAM web console password. Administrators must specify a unique password for the CAM web console (does not have to be a strong password). However, any existing CAM web console passwords (including the old default **cisco123**) are preserved during upgrade.

See Strong Password Support for Root Admin Users, page 21 for additional details on the enhancements to the root password.

Windows ME/98/NT OS Support Removed

Cisco NAC Appliance release 4.5 no longer supports Windows 98/Millennium Edition/NT client operating systems, and Clean Access Agent Version 4.5.0.0 and later cannot be installed on these operating systems. Windows 98/ME/NT Operating System dropdown menu options are retained on User Login and Clean Access Agent Requirement/Rule configuration pages on the CAM. However, Release 4.5 removes support for Windows 98/ME/NT for the Clean Access Agent and Clean Access Agent Supported AV/AS Product List.

Cisco NAC Appliance Agents

This section describes new features or enhancements for the Cisco NAC Appliance Agents:

- Windows Clean Access Agent, page 23
- Mac OS X Clean Access Agent, page 24
- Cisco NAC Web Agent, page 25

Windows Clean Access Agent

Version 4.5.2.0

- Version 4.5.2.0 of the Windows Clean Access Agent in Cisco NAC Appliance release 4.5(1) adds new AV/AS support as listed in Clean Access Supported AV/AS Product Lists, page 26.
- Applicable bugs are resolved as listed in Resolved Caveats - Agent Version 4.5.2.0, page 94.

Version 4.5.1.0

- Version 4.5.1.0 of the Windows Clean Access Agent in Cisco NAC Appliance release 4.5(1) adds new AV/AS support as listed in Clean Access Supported AV/AS Product Lists, page 26.
- The Exit button in the Windows Clean Access Agent system tray can now be disabled by setting a registry value: HKLM\SOFTWARE\Cisco\Clean Access Agent, “DisableExit” (Dword, value=1). See CSCsw52528, page 98.
- Applicable bugs are resolved as listed in Resolved Caveats - Agent Version 4.5.1.0, page 95.

Version 4.5.0 0

- Version 4.5.0.0 of the Windows Clean Access Agent in t in Cisco NAC Appliance release 4.5(0) adds new AV/AS support as listed in Clean Access Supported AV/AS Product Lists, page 26.

- Additionally release 4.5 no longer supports Windows 98/ME/NT operating systems for the Clean Access Agent. See also Windows ME/98/NT OS Support Removed, page 23.

Mac OS X Clean Access Agent

There are no changes to the Mac OS X Clean Access Agent in Cisco NAC Appliance release 4.5(1), and he version remains at 4.5.0.0.

Version 4.5.0.0 with Posture Assessment

With release 4.5, version 4.5.0.0 of the Mac OS X Clean Access Agent can perform posture assessment on Macintosh client machines for the supported AV and AS products listed in Supported AV/AS Product List Version Summary (Mac OS X), page 57. Mac OS X Clean Access Agent version 4.5.0.0 also supports a subset of the requirement types available on the current version of the Windows Clean Access Agent. The supported requirement types are:

- Link Distribution
- Local Check
- AV Definition Update
- AS Definition Update

After a Macintosh OS 10.4 or 10.5 user initiates login and the Mac OS X Agent determines that the client machine requires remediation, the user sees a Mac OS X Agent Assessment Report calling out each of the “failed” mandatory or optional requirements. When presented with the Mac OS X Agent Assessment Report window, users then determine which optional requirements to address (users must address all mandatory requirements) to ensure the client machine is compliant with configured Cisco NAC Appliance security guidelines. Once the user starts client remediation, the Mac OS X Agent addresses each requirement one-by-one as they appear in the Assessment Report until all mandatory requirements “pass” assessment and the user chooses to complete the remediation process and successfully log into the Cisco NAC Appliance system. If any mandatory requirements are not resolved, the user cannot complete the login process.

Additional Features

- When launching a browser, the Link Distribution requirement type will launch the default browser, which can be configured in the Safari browser preference settings. Users can use any browser to perform remediation, including Safari, Firefox, or Opera.
- The Mac OS X Agent fully supports UTF-8 for localization. For configuration details, refer to the “Mac OS X Agent Prerequisites” section of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5*.
- The Mac OS X Agent installer (built by Apple’s “Package Maker” system application) installs two application files on the client: **CCAAgent.app** to launch the Mac OS X Clean Access Agent, and **dhcp_refresh** to facilitate IP address refresh procedures. See CSCso50613, page 71 for additional details on dhcp_refresh.
- The Mac OS X Agent supports Auto-Upgrade. Users can upgrade client machines to the latest Mac OS X Agent by downloading the Agent via web login and running the Agent installation.

Mac OS X Posture Assessment Restrictions

- The client machine must be running Mac OS 10.4 or 10.5. The Mac OS X posture assessment Agent (version 4.5.0.0) does not support Mac OS 10.2 and 10.3.
- The Mac OS X Agent does not support IP-based certificates for authentication.

- The Mac OS X Agent does not support auto-remediation. The user must manually click the **Remediate** button on the Mac OS Agent (equivalent to the **Update** button on the Windows Agent) and manually remediate to make the client machine compliant with network security guidelines.
- The Mac OS X Agent does not support custom checks ("New Check") or custom rules ("New Rule"). You can only assign AV and AS rules to the Link Distribution, Local Check, AV Definition Update, and AS Definition Update requirement types for Mac OS X posture assessment/remediation.
- The Log file (~/Library/Application Support/Cisco Systems/CCAAgent/event.log) is encrypted. The user must use the decryption tool on Windows to see the log in clear text.

See also CSCsl75403, CSCso15754, CSCso50613 under Open Caveats - Release 4.5(1), page 60 for additional details.

For configuration information, refer to the "Mac OS X Clean Access Agent" section of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide*.

Cisco NAC Web Agent

Version 4.5.1.2

- Version 4.5.1.2 of the Cisco NAC Web Agent in Cisco NAC Appliance release 4.5(1) adds new AV/AS support as listed in Clean Access Supported AV/AS Product Lists, page 26.
- Applicable bugs are resolved as listed in Resolved Caveats - Agent Version 4.5.1.0, page 95.

Version 4.5.0

There are no changes to the Cisco NAC Web Agent in Cisco NAC Appliance release 4.5 except that the Cisco NAC Web Agent version is updated to version 4.5.0.

Clean Access Supported AV/AS Product Lists

The Cisco NAC Appliance Supported AV/AS Product List is a versioned XML file distributed from a centralized update server and downloaded to the Clean Access Manager via **Device Management > Clean Access > Updates > Update**. It provides the most current matrix of supported antivirus (AV) and anti-spyware (AS) vendors and products per version of the Clean Access Agent, and is used to populate AV/AS Rules and AV/AS Definition Update requirements for Clean Access Agents that support posture assessment/remediation.

You can access AV and AS product support information from the CAM web console under **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info**. For convenience, this section also provides the following summary and product charts. The charts list which 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 Agent.

- Supported AV/AS Product List Version Summary (Windows), page 27
- Clean Access AV Support Chart (Windows Vista/XP/2000), page 34
- Clean Access AS Support Chart (Windows Vista/XP/2000), page 49
- Supported AV/AS Product List Version Summary (Mac OS X), page 57
- Clean Access AV Support Chart (Mac OS X), page 58
- Clean Access AS Support Chart (Mac OS X), page 59

Note Release 4.5 removes support for Windows 98/ME/NT for the Clean Access Agent and Clean Access Agent Supported AV/AS Product List. See Windows ME/98/NT OS Support Removed, page 23.

Note Cisco recommends keeping your Supported AV/AS Product List up-to-date on your CAM (particularly if you have updated the Windows Agent Setup/Patch version or Mac OS Agent) by configuring the **Update Settings** under **Device Management > Clean Access > Updates > Update** to **Automatically check for updates starting from** <*x*> **every** <*y*> **hours**.

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 4.5* 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.”

Refer to Cisco NAC Appliance Agents, page 23 for additional details on Agent versions in this release.

Supported AV/AS Product List Version Summary (Windows)

Table 7 summarizes enhancements for each version update of the Supported Antivirus/Antispyware Product List for the Windows Clean Access Agent and Cisco NAC Web Agent. See Clean Access AV Support Chart (Windows Vista/XP/2000), page 34 and Clean Access AS Support Chart (Windows Vista/XP/2000), page 49 for details.

Table 7 Supported AV/AS Product List Versions

Version	Enhancements
Release 4.5(1)— 4.5.2.0 Windows Clean Access Agent/4.5.1.2 Cisco NAC Web Agent	
Version 78	Minor internally used data change
Version 77	**Added feature support for the following AV products**: • Cisco Security Agent, 6.x: added def date and version support • Parallels Internet Security, 7.x: added def date and version support **Added new AV products**: • 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 • 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

Table 7 Supported AV/AS Product List Versions (continued)

Version	Enhancements
Version 77 (continued)	• ThreatFire 4.1, 4.x • TrustPort Antivirus, 2.8.x • Verizon Internet Security Suite Anti-Virus, 8.x **Added feature support for the following AS products**: • 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 **Added new AS products**: • 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 76, 75	Minor internally used data change

Table 7 Supported AV/AS Product List Versions (continued)

Version	Enhancements
Release 4.5(1)— 4.5.1.0 Windows Clean Access Agent/4.5.1.2 Cisco NAC Web Agent	
Version 74	**Added New AV Products (Windows Vista/XP/2000):** • 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 **Added AV Def Date, Def Version and Live Update Support:** • Panda Security for Desktops, 4.x **Added AV Live Update Support:** • Malwarebytes Anti-Malware, 1.x **Added New AS Products (Windows Vista/XP/2000):** • Aliant Business Security Suite Anti-Spyware, 6.x • Verizon Internet Security Suite Anti-Spyware, 7.x

Table 7 Supported AV/AS Product List Versions (continued)

Version	Enhancements
Version 73	**Added New AV Products (Windows Vista/XP/2000):** • 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 • 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 **Added AV Def Version Support:** Sophos Anti-Virus, 4.x **Added AV Def Date Support:** Microsoft Forefront Client Security, 1.5.x **Added AV Live Update Support:** • 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

Table 7 Supported AV/AS Product List Versions (continued)

Version	Enhancements
Version 73 (continued)	**Added New AS Products (Windows Vista/XP/2000):** • 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 **Added AS Def Date Support:** • AVG 8.0 [AntiSpyware], 8.x
Release 4.5— 4.5.0.0 Windows Clean Access Agent/4.5.0 Cisco NAC Web Agent	
Version 72, 71	Minor internally used data change

Table 7 Supported AV/AS Product List Versions (continued)

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

Table 7 Supported AV/AS Product List Versions (continued)

Version	Enhancements
Version 70 (continued)	**Added AV Def Date Support:** • AVG 8.0 [AntiVirus], 8.x • AVG Anti-Virus Free, 8.x **Added AV Live Update Support:** • ViRobot Desktop, 5.0.x • ViRobot Desktop, 5.x **Added New AS Products (Windows Vista/XP/2000):** • ZoneAlarm Pro Antispyware, 8.x • ZoneAlarm Security Suite Antispyware, 8.x • CA eTrust Internet Security Suite AntiSpyware, 11.x • F-Secure Internet Security (AntiSpyware), 8.x • McAfee VirusScan AS, 13.x • Spy Emergency 2008, 5.x • Omniquad Total Security, 3.0.x • PC Tools Internet Security [Antispyware], 6.x • PC Tools Spyware Doctor, 6.x • Radialpoint Security Services Spyware Protection, 7.x • SUPERAntiSpyware Free Edition, 4.x • SUPERAntiSpyware Professional, 4.x • Spybot - Search & Destroy 1.6, 1.6.x • Norton AntiVirus [AntiSpyware], 16.x • Norton Internet Security [AntiSpyware], 16.x **Added AS Def Date Support:** • CA Yahoo! Anti-Spy, 2.x

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

Table 8 details Windows Vista/XP/2000 Supported AV Products as of the latest release of the Cisco NAC Appliance software.

Table 8 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (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
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)	-

Table 8 ***Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 2 of 15)***

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	**Virus Definition**	
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
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)	-
Bell				
BellSouth				
BellSouth Internet Security Anti-Virus	5.x	yes (4.0.5.1)	yes (4.0.5.1)	-

Table 8 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 3 of 15)

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

Table 8 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 4 of 15)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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
ESTsoft Corp.				
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
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

Table 8 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 5 of 15)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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)	-
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)	-

Table 8 ***Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 6 of 15)***

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

Table 8 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 7 of 15)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2, 3]
		Installation	Virus Definition	
Kaspersky Anti-Virus Personal	5.0.x	yes (3.5.0)	yes (3.5.0)	yes
Kaspersky Anti-Virus Personal Pro	5.0.x	yes (3.5.11)	yes (3.5.11)	yes
Kaspersky Anti-Virus for Windows File Servers	5.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
Kaspersky Anti-Virus for Windows File Servers	6.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Kaspersky Anti-Virus for Windows Servers	6.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Kaspersky Anti-Virus for Windows Workstations	5.0.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
Kaspersky Anti-Virus for Windows Workstations	6.x	yes (4.0.6.0)	yes (4.0.6.0)	yes
Kaspersky Anti-Virus for Workstation	5.0.x	yes (4.0.5.1)	yes (4.0.5.1)	yes
Kaspersky Internet Security	6.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Kaspersky Internet Security 7.0	7.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Kaspersky Internet Security 8.0	8.x	yes (4.1.3.2)	yes (4.1.3.2)	yes
Kaspersky(TM) Anti-Virus Personal 4.5	4.5.x	yes (3.5.0)	yes (3.5.0)	yes
Kaspersky(TM) Anti-Virus Personal Pro 4.5	4.5.x	yes (3.5.0)	yes (3.5.0)	yes
Kingsoft Corp.				
Kingsoft AntiVirus 2004	2004.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Kingsoft AntiVirus 2007 Free	2007.x	yes (4.1.3.2)	yes (4.1.3.2)	-
Kingsoft Internet Security	7.x	yes (3.6.5.0)	yes (3.6.5.0)	yes
Kingsoft Internet Security 2006 +	2006.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Kingsoft Internet Security 9	2008.x	yes (4.1.7.0)	yes (4.1.7.0)	-
Lavasoft, Inc.				
Lavasoft Ad-Aware 2008 Professional [Antivirus]	7.x	yes (4.1.6.0)	yes (4.1.6.0)	yes
McAfee, Inc.				
McAfee Internet Security 6.0	8.x	yes (3.5.4)	yes (3.5.4)	yes
McAfee Managed VirusScan	3.x	yes (3.5.8)	yes (3.5.8)	yes
McAfee Managed VirusScan	4.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
McAfee VirusScan	10.x	yes (3.5.4)	yes (3.5.4)	yes
McAfee VirusScan	11.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
McAfee VirusScan	12.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
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

Table 8 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 8 of 15)

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

Table 8 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 9 of 15)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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)	-
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

Table 8 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 10 of 15)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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)	-
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

Table 8 *Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 11 of 15)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	**Virus Definition**	
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
SalD Ltd.				
Dr.Web	4.32.x	yes (3.5.0)	yes (3.5.0)	yes
Dr.Web	4.33.x	yes (3.5.11.1)	yes (3.5.11.1)	yes
Dr.Web	4.44.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
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)	-
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

Table 8 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 12 of 15)

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

Table 8 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 13 of 15)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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)	-
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

Table 8 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (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 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
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

Table 8 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 15 of 15)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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 AS Support Chart (Windows Vista/XP/2000)

Table 9 details Windows Vista/XP/2000 Supported Antispyware Products as of the latest release of the Cisco NAC Appliance software.

Table 9 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 1 of 8)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
360Safe.com				
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)	-

Table 9 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 2 of 8)

		AS Checks Supported (Minimum Agent Version Needed)[1]		
Product Name	**Product Version**	**Installation**	**Spyware Definition**	**Live Update[2]**
AOL Safety and Security Center Spyware Protection	2.x	yes (3.6.1.0)	yes (3.6.1.0)	-
AOL Spyware Protection	1.x	yes (3.6.0.0)	yes (3.6.0.0)	-
AOL Spyware Protection	2.x	yes (3.6.0.0)	yes (4.1.3.0)	-
Anonymizer, Inc.				
Anonymizer Anti-Spyware	1.x	yes (4.1.0.0)	yes (4.1.0.0)	-
Anonymizer Anti-Spyware	3.x	yes (4.1.0.0)	yes (4.1.0.0)	-
Authentium, Inc.				
Cox High Speed Internet Security Suite	3.x	yes (4.0.4.0)	-	yes
Bell				
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

Table 9 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (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	5.x	yes (3.6.1.0)	yes (4.0.6.0)	yes
CA eTrust PestPatrol Anti-Spyware	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
CA eTrust PestPatrol Anti-Spyware Corporate Edition	5.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
CA eTrustITM Agent (AntiSpyware)	8.x	yes (4.1.6.0)	yes (4.1.6.0)	yes
PestPatrol Corporate Edition	4.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
PestPatrol Standard Edition (Evaluation)	4.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
EarthLink, Inc.				
Aluria Security Center AntiSpyware	1.x	yes (4.1.0.0)	yes (4.1.0.0)	-
EarthLink Protection Control Center AntiSpyware	1.x	yes (3.6.0.0)	yes (3.6.0.0)	-
EarthLink Protection Control Center AntiSpyware	2.x	yes (4.0.6.0)	-	-
EarthLink Protection Control Center AntiSpyware	3.x	yes (4.1.3.0)	-	-
Primary Response SafeConnect	2.x	yes (3.6.5.0)	-	-
F-Secure Corp.				
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

Table 9 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 4 of 8)

		AS Checks Supported (Minimum Agent Version Needed)[1]		
Product Name	**Product Version**	**Installation**	**Spyware Definition**	**Live Update[2]**
SpywareBlaster v3.5.1	3.5.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
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
Lavasoft, 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)	-
Lavasoft Ad-Aware 2008	7.x	yes (4.1.6.0)	-	-
Lavasoft 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

Table 9 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 5 of 8)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
MicroSmarts LLC				
Spyware Begone	4.x	yes (3.6.0.0)	-	-
Spyware Begone	6.x	yes (4.1.0.0)	-	-
Spyware Begone	8.x	yes (4.1.0.0)	-	-
Spyware Begone Free Scan	7.x	yes (3.6.0.0)	-	-
Spyware Begone V7.30	7.30.x	yes (3.6.1.0)	-	-
Spyware Begone V7.40	7.40.x	yes (3.6.1.0)	-	-
Spyware Begone V7.95	7.95.x	yes (4.1.0.0)	-	-
Spyware Begone V8.20	8.20.x	yes (4.1.0.0)	-	-
Spyware Begone V8.25	8.25.x	yes (4.1.0.0)	-	-
Spyware Begone! Version 9	9.x	yes (4.1.3.2)	-	-
Microsoft Corp.				
Microsoft AntiSpyware	1.x	yes (4.0.6.0)	-	yes
Windows Defender	1.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Windows Defender Vista	1.x	yes (4.0.5.0)	yes (4.0.5.0)	yes
NETGATE Technologies s.r.o				
Spy Emergency 2008	5.x	yes (4.1.7.0)	-	-
Omniquad				
Omniquad Total Security	2.0.x	yes (4.1.3.0)	yes (4.1.3.0)	yes
Omniquad Total Security	3.0.x	yes (4.1.7.0)	yes (4.1.7.0)	-
PC Tools Software				
PC Tools Internet Security [Antispyware]	5.x	yes (4.1.3.0)	-	-
PC Tools Internet Security [Antispyware]	6.x	yes (4.1.7.0)	-	-
PC Tools Spyware Doctor	5.x	yes (4.1.3.2)	-	yes
PC Tools Spyware Doctor	6.x	yes (4.1.7.0)	-	yes
Spyware Doctor	4.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Spyware Doctor	5.x	yes (4.0.6.0)	-	yes
Spyware Doctor 3.0	3.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
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

Table 9 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 6 of 8)

		AS Checks Supported (Minimum Agent Version Needed)[1]		
Product Name	**Product Version**	**Installation**	**Spyware Definition**	**Live Update[2]**
Panda Software				
Panda Titanium 2006 Antivirus + Antispyware [AntiSpyware]	5.x	yes (4.1.3.2)	yes (4.1.3.2)	-
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)	-

Table 9 ***Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 7 of 8)***

		AS Checks Supported (Minimum Agent Version Needed)[1]		
Product Name	**Product Version**	**Installation**	**Spyware Definition**	**Live Update[2]**
Sereniti, Inc.				
Sereniti Antispyware	1.x	yes (4.0.6.0)	-	yes
The River Home Network Security Suite Antispyware	1.x	yes (4.0.6.0)	-	yes
Sunbelt Software				
CounterSpy Enterprise Agent	1.8.x	yes (4.0.6.0)	-	-
CounterSpy Enterprise Agent	2.0.x	yes (4.1.3.0)	-	-
Sunbelt CounterSpy	1.x	yes (3.6.0.0)	-	yes
Sunbelt CounterSpy	2.x	yes (4.0.6.0)	-	yes
Symantec Corp.				
Norton 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

Table 9 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 78, 4.5.2.0 Agent, CAM/CAS Release 4.5(1) (Sheet 8 of 8)

		AS Checks Supported (Minimum Agent Version Needed)[1]		
Product Name	**Product Version**	**Installation**	**Spyware Definition**	**Live Update**[2]
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)	-
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 (Mac OS X)

Table 10 summarizes enhancements made for each version update of the Supported Antivirus/Antispyware Product List for the Mac OS X Clean Access Agent. See Clean Access AV Support Chart (Mac OS X), page 58 and Clean Access AS Support Chart (Mac OS X), page 59 for details.

Table 10 Supported AV /AS Product List Versions (Mac OS X)

Version	Enhancements
Release 4.5(1)/4.5(0)—4.5.0.0 Mac OS X Agent	
Versions 3, 2	Minor internally used data change
Version 1	**Added AV products**: • avast! Antivirus, 2.x • clamXav, 0.x • ClamXav, 1.x • eTrust Antivirus, 7.x • eTrust ITM Agent, 8.x • VirusBarrier X, 10.x • VirusBarrier X4, 10.4.x • VirusBarrier X5, 10.5.x • Virex 7.2, 7.2.x • Virex 7.5, 7.5.x • Virex 7.7, 7.7.x • VirusScan, 8.5.x • VirusScan, 8.6.x • Sophos Anti-Virus, 4.x • Norton AntiVirus, 10.x • Norton AntiVirus, 11.x • Norton AntiVirus, 8.x • Norton AntiVirus, 9.x • Trend Micro Security for Macintosh, 3.x **Added AS products**: • MacScan 2.x

Clean Access AV Support Chart (Mac OS X)

Table 11 lists Mac OS X Supported AV Products for release 4.5(1) of the Cisco NAC Appliance software.

Table 11 Clean Access Antivirus Product Support Chart (Mac OS X) Version 3, 4.5.0.0 Mac OS X Agent, CAM/CAS Release 4.5(1)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2,]
		Installation	Virus Definition	
ALWIL Software				
avast! Antivirus	2.x	yes (4.5.0.0)	yes (4.5.0.0)	-
ClamWin				
clamXav	0.x	yes (4.5.0.0)	yes (4.5.0.0)	yes
ClamXav	1.x	yes (4.5.0.0)	yes (4.5.0.0)	yes
Computer Associates International, Inc.				
eTrust Antivirus	7.x	yes (4.5.0.0)	yes (4.5.0.0)	-
eTrust ITM Agent	8.x	yes (4.5.0.0)	yes (4.5.0.0)	-
Intego				
VirusBarrier X	10.x	yes (4.5.0.0)	yes (4.5.0.0)	-
VirusBarrier X4	10.4.x	yes (4.5.0.0)	yes (4.5.0.0)	-
VirusBarrier X5	10.5.x	yes (4.5.0.0)	-	-
McAfee, Inc.				
Virex 7.2	7.2.x	yes (4.5.0.0)	yes (4.5.0.0)	-
Virex 7.5	7.5.x	yes (4.5.0.0)	yes (4.5.0.0)	-
Virex 7.7	7.7.x	yes (4.5.0.0)	yes (4.5.0.0)	-
VirusScan	8.5.x	yes (4.5.0.0)	yes (4.5.0.0)	-
VirusScan	8.6.x	yes (4.5.0.0)	yes (4.5.0.0)	-
Sophos Plc.				
Sophos Anti-Virus	4.x	yes (4.5.0.0)	yes (4.5.0.0)	-
Symantec Corp.				
Norton AntiVirus	10.x	yes (4.5.0.0)	yes (4.5.0.0)	-
Norton AntiVirus	11.x	yes (4.5.0.0)	yes (4.5.0.0)	-
Norton AntiVirus	8.x	yes (4.5.0.0)	yes (4.5.0.0)	-
Norton AntiVirus	9.x	yes (4.5.0.0)	yes (4.5.0.0)	-
Trend Micro, Inc.				
Trend Micro Security for Macintosh	3.x	yes (4.5.0.0)	yes (4.5.0.0)	-

[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 manual Agent **Remediate** 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 **Remediate** button is clicked. For products that do not support this feature, administrators can configure a different requirement type (such as "Local Check") to present alternate update instructions to the user.

Clean Access AS Support Chart (Mac OS X)

Table 12 lists Mac OS X Supported Antispyware Products for release 4.5(1) of the Cisco NAC Appliance software.

Table 12 Clean Access Antispyware Product Support Chart (Mac OS X) Version 3, 4.5.0.0 Mac OS X Agent/CAM/CAS Release 4.5(1)

		AS Checks Supported (Minimum Agent Version Needed)[1]		
Product Name	**Product Version**	**Installation**	**Spyware Definition**	**Live Update**[2]
SecureMac.com, Inc.				
MacScan	2.x	yes (4.5.0.0)	yes (4.5.0.0)	-

1. "Yes" in the AS Checks Supported columns indicates the Agent supports the AS Rule check for the product starting from the version of the Agent listed in parentheses (CAM automatically determines whether to use Def Version or Def Date for the check).
2. The Live Update column indicates whether the Agent supports live update for the product via the manual Agent **Remediate** 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 **Remediate** button is clicked. For products that do not support this feature, administrators can configure a different requirement type (such as "Local Check") to present alternate update instructions to the user.

Caveats

This section describes the following caveats:

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

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

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

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

Open Caveats - Release 4.5(1)

Note For caveats related to Cisco NAC Profiler, refer to the applicable version of the *Release Notes for Cisco NAC Profiler*.

Table 13 List of Open Caveats (Sheet 1 of 21)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsd03509	No	The Time Servers setting is not updated in HA-Standby CAM web console After updating the “Time Servers” setting in HA-Primary CAM, the counterpart “Time Servers” setting for the HA-Standby CAM does not get updated in the web console even though the “Time Servers” setting is updated in the HA-Standby CAM database.

Table 13 List of Open Caveats (Sheet 2 of 21)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCse86581	No	Agent does not correctly recognize def versions on the following Trend AV products: • PC-cillin Internet Security 2005 • PC-cillin Internet Security 2006 • OfficeScan Client Tested Clients: • PC-cillin Internet Security 2006 (English) on US-English Windows 2000 SP4 • OfficeScan Client (English) on US-English Windows 2000 SP4 • VirusBaster 2006 Internet Security (Japanese) on Japanese Windows XP SP2 • VirusBaster Corporate Edition (Japanese) on Japanese Windows XP SP2
CSCsg07369	No	Incorrect "IP lease total" displayed on editing manually created subnets Steps to reproduce: 1. Add a Managed Subnet having at least 2500+ IP addresses (for example 10.101.0.1/255.255.240.0) using CAM web page **Device Management > Clean Access Servers > Manage [IP Address] > Advanced > Managed Subnet**. 2. Create a DHCP subnet with 2500+ hosts using CAM web page **Device Management > Clean Access Servers > Manage [IP Address] > Network > DHCP > Subnet List > New**. 3. Edit the newly created subnet using CAM web page **Device Management > Clean Access Servers > Manage [IP Address] > Network > DHCP > Subnet List > Edit**. 4. Click **Update**. The CAM displays a warning informing the administrator that the current IP Range brings IP lease total up to a number that is incorrect. The CAM counts the IP address in the subnet twice, creating the incorrect count. The issue is judged to be cosmetic and does not affect DHCP functionality.
CSCsg66511	No	Configuring HA-failover synchronization settings on Secondary CAS takes an extremely long time Once you have configured the Secondary CAS HA attributes and click **Update**, it can take around 3 minutes for the browser to get the response from the server. (Configuring HA-failover synchronization on the Primary CAS is nearly instantaneous.)

Table 13 List of Open Caveats (Sheet 3 of 21)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsh77730	No	Clean Access Agent locks up when greyed out **OK** button is pressed The Clean Access Agent locks up when the client machine refreshes its IP address. This only occurs when doing an IP release/renew, so the CAS must be in an OOB setup. If the **Automatically close login success screen after** <*x*> **secs** option is enabled and the duration set to 0 (instantaneous) in the **Clean Access > General Setup > Agent Login** page and the user clicks on the greyed out **OK** button while the IP address is refreshing, the Clean Access Agent locks up after refreshing the IP address. The IP address is refreshed and everything else on the client machine works, but the user cannot close the Clean Access Agent without exiting via the system tray icon, thus "killing" the Agent process. **Workaround** Either uncheck the box or set that timer to a non-zero value. If it is set to anything else, and the user hits the greyed out OK button while the IP is refreshing, then the Agent window closes successfully.
CSCsi07595	No	DST fix will not take effect if generic MST, EST, HST, etc. options are specified Due to a Java runtime implementation, the DST 2007 fix does not take effect for Cisco NAC Appliances that are using generic time zone options such as "EST," "HST," or "MST" on the CAM/CAS UI time settings. **Workaround** If your CAM/CAS machine time zone setting is currently specified via the UI using a generic option such as "EST," "HST," or "MST." change this to a location/city combination, such as "America/Denver." **Note** CAM/CAS machines using time zone settings specified by the "service perfigo config" script or specified as location/city combinations in the UI, such as "America/Denver" are not affected by this issue.

Table 13 List of Open Caveats (Sheet 4 of 21)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCsj16366	No	Time sync on CAS The CAS network module (NME-NAC-K9) appears as "not connected" in CAM web console after a router/rack power outage. 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: "AutoConnectManager failed relinking CAM with CAS-i.p.add.rs." **Note** The time on the CAS module goes back to some time in 2006. **Workaround** The administrator should manually reset the system time in the CAS web console.
CSCsk55292	No	Agent not added to system tray during boot up When the Agent is installed on a Windows client, the Start menu is updated and Windows tries to contact AD (in some cases where the AD credentials are expired) to refresh the Start menu. Due to the fact that the client machine is still in the Unauthenticated role, AD cannot be contacted and an approximately 60 second timeout ensues, during which the Windows taskbar elements (Start menu, System Tray, and Task Bar) are locked. As a result, the Agent displays a "Failed to add Clean Access Agent icon to taskbar status area" error message. **Workaround** There are two methods to work around this issue: • Allow AD traffic through the CAS for clients in the Unauthenticated role. • Try to start the Agent manually after the install and auto load process fails.
CSCsl13782	No	Microsoft Internet Explorer 7.0 browser pop-ups on Windows Vista launched from the Summary Report appear behind the Summary Report window This is also seen when you click on the Policy link in the Policy window. This issue appears on Vista Ultimate and Vista Home, but is not seen with Firefox or on Internet Explorer versions running in Windows 2000 or Windows XP. **Note** This problem only happens when a Google tool bar is installed and enabled in Internet Explorer.

Table 13 List of Open Caveats (Sheet 5 of 21)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCsl17379	No	Multiple Clean Access Agent pop-ups with Multi NIC in L2 VGW OOB role-based VLAN The user sees multiple Clean Access Agent login dialogs with two or more active NICs on the same client machine pointing to the Unauthenticated network access point (eth1 IP address). After the first Clean Access Agent pops up and the user logs in, a second Agent login dialog pops up. If the user logs in to this additional Agent instantiation there are now two entries for the same system with both MAC addresses in the CAM's Certified Device List and Online Users List. **Workaround** The user can manually Disable Agent login pop-up after authentication.
CSCsl40626	No	Cisco NAC Web Agent should handle certificate revocation dialogs similar to Clean Access Agent Upon logging in via the Cisco NAC Web Agent (with certificate revocation turned on or with Norton 360 installed), the user is presented with a "Revocation information for the security certificate for this site is not available. Do you want to proceed?" dialog box several times (approximately 40 to 50 times). If the user clicks **Yes** to proceed enough times, the Web Agent fails to login and reports "You will not be allowed to access the network due to internal error. Please contact your administrator." back to the user.
CSCsl40812	No	The **Refresh Windows domain group policy after login** option is not functioning for Cisco NAC Web Agent (It is working fine with the Clean Access Agent.) This scenario was tested configuring a GPO policy for a Microsoft Internet Explorer browser title. The browser was not refreshed as expected after login in using the Web Agent.

Table 13 List of Open Caveats (Sheet 6 of 21)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsl75403	No	MAC filter does not work for Macintosh client machines connected to the network in VPN environment Steps to reproduce: **1.** Setup a VPN environment. **2.** Get the MAC address of the en0 interface of Macintosh client machine. **3.** Put the MAC address in the CAM device filter list with "Deny" access type. **4.** Connect the Macintosh client machine to the VPN concentrator. **5.** Agent will be allowed to perform VPN SSO [or present login page if no VPN SSO is configured]. **6.** Traffic originating from the client machine on the untrusted network is allowed to go to the trusted network even though the MAC address of the client machine is denied in the device filter list.
CSCsl77701	No	Network Error dialog appears during CAS HA failover When a user is logged in as ADSSO user on CAS HA system and the CAS experiences a failover event, the user sees is a pop-up message reading, "Network Error! Detail: The network cannot be accessed because your machine cannot connect to the default gateway. Please release/renew IP address manually." This is not an error message and the user is still logged in to the system. The user simply needs to click on the **Close** button to continue normal operation.
CSCsl88429	No	User sees Invalid session after pressing [F5] following Temporary role time-out When a user presses [F5] or [Refresh] to refresh the web page after the Agent Temporary role access timer has expired, the user sees an "Invalid" session message. If the user then attempts to navigate to the originally requested web address, they are prompted with the web login page again and are able to log in.
CSCsl88627	No	Description of **removesubnet** has "updatesubnet" in op field The **removesubnet** API function description has "updatesubnet" listed in its operations field. The description should read "removesubnet."

Table 13 List of Open Caveats (Sheet 7 of 21)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCsm20254	No	CAS duplicates HSRP packets with Cisco NAC Profiler Collector Modules enabled. **Symptom** HSRP duplicate frames are sent by CAS in Real-IP Gateway with Collector modules enabled. This causes HSRP issues and the default gateway to go down. **Conditions** Real-IP Gateway and Collector modules enabled on a CAS with ETH0 and or ETH1 configured for NetWatch. **Workaround** Do not configure the CAS' ETH0 trusted interface or ETH1 untrusted interface in the NetWatch configuration settings for the CAS Collector. It is not a supported configuration.
CSCsm20655	No	Can not do a minor upgrade for Clean Access Agent from MSI package. When CCAAgent.msi is used and the Clean Access Agent is upgraded to a minor version (e.g. 4.1.2.1 to 4.1.2.2) the following error message will be displayed: “Another version of this product is already installed. Installation of this version cannot continue. To configure or remove the existing version of this product, use Add/Remove Programs on the Control Panel.” 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 **Workaround** Uninstall the program from Add/Remove Programs before installing it. See also Known Issues with MSI Agent Installer, page 133.
CSCsm25788	No	Avast 4.7 showing as not up to date with Cisco NAC Appliance Release 4.1(3) User is told that Avast needs to be updated, but shows as up to date. This occurs when user is running Avast 4.7 and the Agent version is 4.1.3.0 or 4.1.3.1 **Workaround** Create a custom check for Avast that allows the users on without verifying the definition version.

Table 13 List of Open Caveats (Sheet 8 of 21)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsm53743	No	File ownership of Mac OS X Agent directory and related files should be corrected File ownership of Mac OS X Agent and related files should be "root:admin." Currently, the file ownership is with UID 505 and GID 505. Anyone able to assume this UID could potentially modify the Agent application files and introduce a security threat.
CSCsm61077	No	ActiveX fails to perform IP refresh on Windows Vista with User Account Control (UAC) turned on. 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. **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. Alternatively, the Cisco NAC Web Agent can be used with no posture requirements enabled. See also Known Issue for Windows Vista and IP Refresh/Renew, page 132.

Table 13 List of Open Caveats (Sheet 9 of 21)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCsm76779	No	CSRF tag is added to CAS specific MAC Device Filter description field upon edit Steps to reproduce: 1. Go to CAS-specific device filters in the CAM web console (**Device Management > Clean Access Servers > Manage [IP_Address] > Filter > Devices**). 2. Edit a device filter with the description field like "<a href='http://www.cisco.com'>Cisco</a>" 3. Click **Save**. A CSRF tag is appended to (and is visible in) the hypertext entry in the device filter description field. Subsequent entry updates also append the same CSRF tag each time the administrator edits the description. After editing the description 3 times, however, the entry can no longer be edited and the CAS returns an "Updating device MAC failed" error message. **Note** This issue only addresses CAS-specific device filters and not *global* device filters addressed with caveat CSCsm55679.
CSCsm79088	No	Mac OS X Agent reports "Unknown user" when sending the second logout request The Mac OS X Agent specifies an "Unknown user" when it sends a second logout request before receiving a response from the first logout request. Steps to reproduce: 1. Log into the network using the Mac OS X Agent. 2. Right-click on Agent icon and choose **Logout**. 3. Repeat step 2 before receiving a response for the first logout request. The Mac Agent displays a "Cisco Clean Access Agent is having a difficulty with the server. Unknown user." error message, resulting in a situation where the client machine no longer appears in the CAM's Online Users list even though the Agent indicates that the user is logged in. In this situation, the Mac Agent essentially "freezes" as the user is no longer able to log out, ether.

Table 13 List of Open Caveats (Sheet 10 of 21)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCso15754	No	The ClamXAV live update feature may not work the first time if a "failed" ClamXAV installation requirement immediately precedes the live update in the Mac OS X Assessment Report remediation window If both a ClamXAV Link Distribution and a ClamXAV live update requirement are configured for Mac OS X client remediation, and the installation requirement appears right before the live definition update, then the ClamXAV live update may fail because as the installation process completes, the live update process begins and does not have a chance to read the updated ClamXAV version before launching. Therefore, if the timing is not right, users may have already started the live update while the actual ClamXAV application update tool is still copying onto the client machine. **Workaround** The user needs to perform the remediation process again because it requires a little extra time for the live update tool to be ready following ClamXAV installation. If the user clicks the **Remediate** button again after seeing the requirement fail in the first round of remediation tasks, it works just fine.
CSCso41549	No	Administrator cannot delete the OUL manually if the In-Band CAS is not available to the CAM If an In-Band CAS fails for some reason (if the CAS suffers a hardware failure, for example), users stay in the Online Users List. **Workaround** Manually delete the entry from the "user_info" table in the CAM database.
CSCso49473	No	SEVERE: javax.naming.CommunicationException causes no provider list Configuration: ADSSO with LDAP Lookup If the LDAP connection to AD drops because the lookup takes a long time or the route is lost suddenly, the Agent does not receive the list of auth providers so the user is presented with a blank provider list. Symptom: The dropdown list of authentication providers is blank. Conditions: LDAP server fails to respond due to network connectivity failure or a long directory search. The failure must occur after communication to the LDAP server has begun. Workaround: None **Note** CSCso61317 is a duplicate of this bug.

Table 13 List of Open Caveats (Sheet 11 of 21)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCso50613	No	Mac OS X Agent DHCP refresh fails if **dhcp_refresh** file does not exist DHCP refresh will fail with no notice (to the user or to the logs) if the **dhcp_refresh** file does not exist. The **dhcp_refresh** tool is required for all versions of Mac OS X Agents, so it always fails if the **dhcp_refresh** tool is missing regardless the Mac OS version. **Workaround** There are three ways to work around this issue: **1.** Reinstalling the Mac OS X Agent automatically reinstalls the missing **dhcp_refresh** file. **2.** Users can sign on to Cisco NAC Appliance via web login. The Java applet installs the **dhcp_refresh** tool if the **Install DHCP Refresh tool into Linux/MacOS system directory** option is checked under **User Page > Login Page > Edit > General**. **3.** When using the Apple Migration Assistant, the user can try to include **/sbin/dhcp_refresh** in the migration list.
CSCso61317	No	When LDAP lookup fails for an AD SSO user, the Provider list in the Agent dialog is empty **Scenario 1** AD SSO configured with LDAP lookup When the LDAP lookup fails for the user (some misconfiguration or not able to reach the right server to find the user), the Agent displays a login window without a Provider list. This happens because the user has already passed the login stage, but has failed the lookup stage. **Scenario 2 (less common)** The user is logged in to a machine that is not part of the domain, but the user does have an AD account. Steps that occur: **1.** A TGT, obtained with the AD account, is granted. **2.** The ST for the CAS is granted. **3.** Agent passes the local account information since the user has logged in locally to the machine. **4.** Authorization fails which causes the blank provider list.
CSCsq94290	No	AV Def file update does not launch for TrendMicro 16.10.1079 When a user logs in from a client machine running Windows XP Media Center Edition and the client goes through auto-remediation, the AV Def file update does not launch for TrendMicro 16.10.1079. **Workaround** Manually update the AV def files.

Table 13 List of Open Caveats (Sheet 12 of 21)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCsr50995	No	Agent doesn't detect Zone Alarm Security definitions correctly Symptom: User fails posture assessment when checking for AV definitions for Zone Alarm Security Suite 7.0. Conditions: This occurs using either the Any AV check or the Checkpoint Any check. **Workaround** Create a custom check for Zone Alarm Security Suite definition.
CSCsr52953	No	RMI error messages periodically appear for deleted and/or unauthorized CASs in CAM event logs Clean Access Servers connected to a CAM can periodically appear as "deleted" or "unauthorized" in the CAM event logs even though the CAS is functioning properly and has not experienced any connection issues with the Clean Access Manager. Error message examples are: • "SSL Communication 2008-07-23 00:31:29 SSLManager:authorizing server failed CN=10.201.217.201, OU=Perfigo, O=Cisco Systems, L=San Jose, ST=California, C=US" • "SSL Communication 2008-07-23 00:31:29 RMISocketFactory:Creating RMI socket failed to host 10.201.217.201:java.security.cert.CertificateException: Unauthorized server CN=10.201.217.201, OU=Perfigo, O=Cisco Systems, L=San Jose, ST=California, C=US" **Workaround** • Reboot the CAS and wait for the CAM to re-establish connection. • Reboot the CAM after deleting and removing the CAS from the Authorized CCA Server list using the CAM **Device Management > CCA Servers > Authorization** admin web console page.

Table 13 List of Open Caveats (Sheet 13 of 21)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsr61106	No	Cannot upgrade CAS via CAM's web UI An HTTP status 500 error message occurs stating “java.lang.OutofMemoryError” when upgrading the CAS via the CAM's web user interface if the CAM’s memory is less than 1GB, or during CAS software upgrade via the CAM’s web user interface using the release 4.5 upgrade package. This problem is seen with non-Cisco hardware with only 512MB memory installed; i.e. Dell's 750, 850, or 860. With release 4.5, the problem is seen with all Cisco appliances including NAC-3140, NAC-3310, NAC-3350 & NAC-3390. **Workaround** Upgrade the CAS using the SSH method.
CSCsr90712	No	Symantec Antivirus delays Clean Access Agent startup The Agent takes a long time to pop up on a client machine with real-time antivirus scanning enabled and operating. **Workaround** Exclude the Clean Access Agent AV411 directory from Symantec Antivirus scanning. See http://service1.symantec.com/support/ent-security.nsf/docid/2002092413394848. **Note** The step to configure Extensions can be omitted. For Vista, refer to http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008111414031848.

Table 13 List of Open Caveats (Sheet 14 of 21)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**

CSCsr95757	No	CAM intermittently stops processing SNMP MAC notification traps from the switch
		This issue can occur on different edge switches. Once the problem is present, no further SNMP MAC notification traps are processed from the CAM for the switch in question.
		Note There is no **perfigo-log0.log.0** information, but a **tcpdump** from a CAM CLI session indicates that the CAM is receiving SNMP MAC notification traps.
		Workaround To re-establish correct SNMP trap handling on the CAM, open a CAM CLI session and enter the following commends:
		`service perfigo stop`
		`service perfigo start`
		The CAM immediately starts processing the SNMP MAC notification traps from the problem switch(es).
		Note After a period of time, however, this problem may appear again.

CSCsu47350	No	Invalid version number displayed in CAM backup snapshot web page When the administrator navigates to another page in the CAM web console during the backup snapshot process, the resulting snapshot version number is invalid.
CSCsu63247	No	DHCP IP refresh not working for some Fedora core 8 client machines DHCP IP refresh does not work on Fedora core 8 clients logging in to a Layer 3 Real-IP Gateway CAS using the current version of the Java applet. As a result, Fedora core8 clients must use web login to gain access to the Cisco NAC Appliance network. **Note** There is no known workaround for this issue

Table 13 List of Open Caveats (Sheet 15 of 21)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCsu63619	No	Out-of-Band switch port information from OUL/CDL missing upon login after upgrade OOB switch port information in Online Users List/Certified Devices List is missing upon login after upgrading to release 4.5. This issue occurs when the client machine has not been disconnected from the network (has not generated a MAC notification trap from the switch), and logs into the OOB network after upgrade. **Workaround** Disconnect the client machine from the switch and reconnect. This generates the MAC linkdown notification trap from the switch to the CAM updating the Discovered Clients list with the appropriate port information for this client machine. **Note** This issue is cosmetic and does not affect Cisco NAC Appliance functionality.
CSCsu69247	No	ERROR: File type requirements does not exist During CD installation of Cisco NAC Appliance Release 4.5, users can see the following error message in the nac_manager.log file: "2008-09-21 19:25:55.592 -0700 ERROR com.perfigo.wlan.web.admin.DMSoftwareManager - DMSM syncDMSoftware: Directory('/perfigo/control/tomcat/webapps/packages/') for file type requirements does not exist" This is a benign error message related to webapps packages that have been relocated in the installation script and has no impact on image installation.
CSCsu78379	No	Bandwidth settings for Receiver CAM roles should not change after Policy Sync Steps to reproduce: **1.** Create role on Master CAM, r1 **2.** Edit Upstream and Downstream Bandwidth fields of r1 to equal 1Kbps **3.** Create role on Receiver CAM, r2 **4.** Edit Upstream and Downstream Bandwidth fields of r2 to equal 2 Kbps **5.** Select role-based Master Policies to Export and perform manual sync **6.** Upstream and Downstream Bandwidth fields for role r1 on Receiver CAM are changed to -1 (not 2 Kbps and not 1 Kbps). **Note** Receiver's Up/Down Kbps, Mode, Burst should either not change or should be the same as the Master.

Table 13 List of Open Caveats (Sheet 16 of 21)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsu84848	No	CAM should set the switch port to Authentication VLAN before removing from OUL and DCL The CAM should set the switch port to the Authentication VLAN before removing the user from Online Users List and Discovered Client List when the Switch or WLC entry is deleted from the CAM. **Workaround** Bounce the switch port to clear the OUL and DCL.
CSCsu84977	No	CAS: ERROR /proc/click/intern_filter_group/failsafe The following error message can appear to users during CD installation of Cisco NAC Appliance release 4.5 in Clean ACcess Servers: "com.perfigo.wlan.jmx.Shell - /proc/click/intern_filter_group/failsafe (No such file or directory)" This error message is related to a recently-removed file failsafe and has no impact on CD installation.
CSCsu88594	No	Removal of www.perfigo.com Root CA from GUI The www.perfigo.com Root CA should be removed from the GUI. With the default configuration there is no CA certificate button to offer on the web (or user) login page. The Cisco NAC Appliance administrator must configure user page content and specify whether or not to offer the Root CA along with its content from the dropdown menu (either the www.perfigo.com CA certificate or an imported third-party CA certificate—the default choice is the www.perfigo.com CA). **Workaround** To change this behavior go to **Administration > User Pages > Login Page > Edit > Content** and deselect the **Root CA** table entry.
CSCsu88796	No	CAM upgrade: Error message in 4.1(3)-to-4.5 upgrade details log When upgrading the Clean Access Manager from release 4.1(3) to 4.5, users may see a benign "scriplet failed" error message listed in the upgrade details log file. This error message has no impact on upgrade to release 4.5.
CSCsu89385	No	"not a symbolic link" error message in 4.1(3)-to-4.5 CAS upgrade details log When administrators upgrade Clean Access Servers from release 4.1(3) to release 4.5, they may see a number of "not a symbolic link" error messages in the upgrade details log. These error messages have no effect on the CAS upgrade. **Note** You can run **./showstate.sh** in the CAS CLI to verify successful upgrade.

Table 13 List of Open Caveats (Sheet 17 of 21)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCsv18261	No	HA Failover database sync times out in event log after reboot In Cisco NAC Appliance release 4.5, the CAM HA database copy function times out when the active CAM fails over and becomes the standby CAM. (Event log entries show that the database copy function times out.) This situation arises when the inactive CAM comes up and attempts to copy the database from the active CAM, but the database is still locked by the [now standby] CAM. This issue is not seen during normal operation and database sync because the entries are copied in real time. **Note** In Cisco NAC Appliance releases prior to 4.5, there is no timeout function, and the database sync takes less time to complete because the CAM does not lock the database or verify the copy function.
CSCsv18995	No	Three requirement types allow administrators to select single Windows XP/Vista operating systems when "All" is checked When creating a new Windows Update, Launch programs, and/or Windows Server Update Services (WSUS) requirement type, and checking the "Windows XP (All)" or "Windows Vista (All)" options, the individual OS options are also still selectable (although they should not be). **Note** This issue is not seen on the other requirement types. There is no known workaround for this issue
CSCsv20270	No	Conflicting CAM's eth1 HA heartbeat address with release 4.5 after upgrade The perfigo service cannot be started on the standby CAM because both the eth1 interface of HA CAMs have the same IP address: either 192.168.0.253 or 192.168.0.254. This happens in an HA setup when one of the CAMs is upgraded from release 4.0(x) to 4.5 and the other CAM is fresh CD installed. **Workaround** Change to use the manual setting for eth1 on the fresh CD installed node or re-apply the HA config on the upgraded node.

Table 13 List of Open Caveats (Sheet 18 of 21)

DDTS Number	**Software Release 4.5(1)** **Corrected**	**Caveat**
CSCsv22418	No	CAS service IP not reachable after standby reboot due to race condition The Active CAS's service IP become unreachable after standby CAS reboot. In a rare race condition, the standby CAS temporarily becomes active for very short period of time after reboot. **Workaround** **1.** Increase the "Heartbeat Timeout" value from the recommended 15 seconds to 30 seconds. **2.** Or, run the heartbeat interface on Interface 3 (eth2 or eth3).
CSCsv78301	No	VPN SSO login does not work with VPN in managed subnet after upgrade to Cisco NAC Appliance release 4.5 Prior to release 4.5, the Clean Access Server associates the client with the VPN IP address and VPN Concentrator's MAC address after the first login. From there, the SWISS protocol only checks the IP address from the Agent and reports back to the Agent that the client is logged in (regardless of whether the client is connected via Layer 2 or Layer 3). In release 4.5, the SWISS protocol checks the MAC address for Layer 2 clients, but the MAC address reported by the Agent (which is the real client MAC address) is different from the one the CAS gets for the client (the VPN concentrator MAC address). As a result, the SWISS protocol tells the Agent that the client machine is not logged in (due to the different MAC addresses recorded) and the Agent launches the login dialog repeatedly, never able to complete login. **Workaround** Remove the subnet making up the client machine address pool from the collection of managed subnets and create a Layer 3 static route on the CAS untrusted interface (eth1) with VPN concentrator's IP address as the gateway for the VPN subnet using the CAM web console **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Static Routes** page.
CSCsx05054	No	DHCP does not work with IGNORE fallback policy and CAS Failover 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. **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.

Table 13 List of Open Caveats (Sheet 19 of 21)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsx05141	No	Clients cannot get IP addresses from CAS DHCP relay agent in CAS fail-open with CAS fallback scenario Steps to reproduce this issue: **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 dhcprelay starts on the CAS if you enter netstat. Even though the administrator can see dhcrelay functioning, clients are now unable to get IP addresses through new Active CAS.
CSCsx25557	No	NOD32 3.x Def date is not recognized by Clean Access Agent **Note** The support chart incorrectly showed that this version can be updated. Version 3.x is not able to be updated by the Agent. The update will have to be performed manually from the NOD32 console. **Note** There is no known workaround for this issue.
CSCsx35438	No	Clean Access Manager read timeout reached when deleting many DHCP IPs at once 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. **Workaround** Please see Known Issue with Mass DHCP Address Deletion, page 124.

Table 13 List of Open Caveats (Sheet 20 of 21)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsx45051	No	Agent may proceed with AV/AS auto remediation while it's not supported For an AV/AS Definition Update Requirement Type with Automatic Remediation Type and Antivirus/Anti-Spyware Vendor Name configured as ANY, when the client fails the requirement, the Agent should automatically launch the AV (or AS) update on the AV product for which the Agent supports live update. If live update is not supported, the Agent should prompt the user to perform manual remediation. With this issue, the Agent may proceed with auto remediation on a product for which the Agent does not support live update. As a result, auto remediation will fail, and the agent will prompt user to do manual remediation. **Note** This issue is observed with MS Live One 2.x. Auto Remediation fails when configured for MS Live One 2.x. **Workaround** Remediate AV manually while in the temporary role.
CSCsx78577	No	ClamAV not showing def date ClamAV does not provide the definition date to the Agent. **Workaround** There is no workaround at this time. This is a known issue.

CSCsx80459	No	JAVA_OPTS_TO of "" seen in CAM upgrade details
		When upgrading the Clean Access Manage to release 4.5(1), the additional message “`Ended up with JAVA_OPTS_TO of “”` may be seen in the upgrade details text displayed under Administration > CCA Manager > Software Upload. This message does not affect upgrade and is safe to ignore.
		`Welcome to the CCA Manager migration utility.`
		
		`...Upgrading to newer rpms of 4.5.1...done.`
		`...Upgrading CCA files...Ended up with JAVA_OPTS_TO of “”`
		`Preparing...`
		`##################################################`
		`nac_manager`
		`##################################################`

CSCsx81395	No	Sophos AV Definition rule fails even if Mac OS Agent has the latest definition The remediation window pops up for updating the Sophos definition files on the Mac OS Agent even though Sophos is updated. This occurs if Sophos is installed on the Mac OS client and an AV definition check for Sophos is configured on the CAM. **Workaround** There is no workaround at this time.

Table 13 List of Open Caveats (Sheet 21 of 21)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCsx95230	No	Length of token is not printed in the ADSSO logs When ADSSO logging is changed to DEBUG for troubleshooting purposes, the ADSSO logs display the token but not the token size. **Workaround** None.
CSCsx52263	No	NAC Appliances always assume USA keyboard layout When connected via Keyboard and Monitor, if a keyboard with layout other than US layout is used, the Cisco NAC Appliances do not recognize the keyboard and it is possible to erroneously enter different characters. **Workaround** Use a US layout keyboard or ensure that you know the key mapping if you are connecting a keyboard of different layout.

Resolved Caveats - Release 4.5(1)

Note For caveats related to Cisco NAC Profiler, refer to the applicable version of the *Release Notes for Cisco NAC Profiler*.

Table 14 List of Resolved Caveats (Sheet 1 of 13)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCsd90433	Yes	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 14 List of Resolved Caveats (Sheet 2 of 13)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsl71585	Yes	DHCP status does not display non-restricted scope with Relay IP restriction When a DHCP range with no restrictions and a DHCP range with a Relay-IP restriction are created using the Clean Access Manager (CAM) GUI, the DHCP range with no restrictions does not display. Steps to reproduce: 1. Create a DHCP scope with no restriction, either VLAN ID or Relay-IP on the CAS using the CAM GUI. 2. Add a static route on the CAS using the CAM GUI. 3. Create another DHCP scope with a relay-IP restriction. 4. Go to the DHCP Status web page. The web page only displays the IPs for the relay-IP restriction and does not display the non-restricted IP scope. **Workaround** Avoid creating DHCP scopes having both no restrictions and Relay-IP restrictions. **Note** The issue is known to be cosmetic and does not affect functionality.
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. See also CSCsw35162, page 91.
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.

Table 14 List of Resolved Caveats (Sheet 3 of 13)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
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:
		`+       <!--`
		`        <filter-mapping>`
		`                <filter-name>CSRFFilter</filter-name>`
		`                <url-pattern>/*</url-pattern>`
		`        </filter-mapping>`
		`+       -->`

CSCso32106	Yes	Port list on CAM should be sortable by "Description" instead of index
		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:
		`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`
		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.
		Workaround None. All the ports show up in the CAM, they are just not in the expected order.

CSCso44904	Yes	CAM does not manage CAS via the **Manage** icon in web console 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. **Note** Although the CAS web console is unreachable, operations continue normally and users are able to authenticate via the Cisco NAC Appliance. **Workaround** Restarting services on the CAM can resolve this issue.

Table 14 List of Resolved Caveats (Sheet 4 of 13)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCso57843	Yes	Standby CAS sends improper ARP request after bootup This issue occurs in an HA pair environment using DHCP Synchronization. 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. 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.” **1.** Sender MAC: Untrust MAC of Standby CAS—Correct Info **2.** Sender IP: Untrust IP of Active CAS— Wrong Info **3.** Target MAC: 0000.0000.0000—Correct Info **4.** Target IP: Link Detect IP for Untrusted—Correct Info **Note** There is no known workaround for this issue.
CSCsq27411	Yes	Standby CAS responds to ARP with the wrong MAC address 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. 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. **Note** There is no known workaround for this issue.
CSCsq59801	Yes	Nessus plug-ins greater than 10 MB size limitation When uploading a NESSUS plug-in .tar file that is greater than 10MB, the CAM returns the following error: “Result: Error: Failed to upload file Content Length Error (18113815 > 10485760)” When the upload file is greater than 10MB, the upload fails. **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.

Table 14 List of Resolved Caveats (Sheet 5 of 13)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsr75123	Yes	Better handling for certificate chain in **chain.crt** file 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. **Workaround** Edit the **chain.crt** file to correct the sequence of elements in the chain.
CSCsr95218	Yes	CAM Filters page does not display properly with limited Admin privileges When bringing up the CAM web console Filters page, the administrator receives the following error: "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." **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. **Workaround** Set the Certified Devices page to **read only** under the Admin Group permissions setup (**Administration > Admin Users > Admin Groups > Edit**).

Table 14 List of Resolved Caveats (Sheet 6 of 13)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCsu02167	Yes	SSL fails when Netscape Cert Type field does not contain "SSL Client" As a result, the CAS and CAM disconnect from one another and users cannot authenticate. Report log entries show: "SEVERE: SSLManager: client's certificate chain verification failed CN=CAS, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US:Netscape cert type does not permit use for SSL client" If certificates contain a Netscape Cert Type field and are used in release 4.1(6), that field has to contain both "SSL Server" and "SSL Client." If the field does not contain "SSL Client," communication between the CAS and CAM fails. If the Netscape Cert Type field does not exist, then SSL succeeds. If the Netscape Cert Type field does exist, but does not contain both "SSL Server" and "SSL Client," authentication fails. **Note** This issue has been observed with Entrust certificates and another educational CA. **Workaround** There are two methods to work around this issue: • 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	CAM/CAS does not handle blank spaces in certificate 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. **Workaround** Ensure you remove all blank spaces from the certificate.
CSCsv10336	Yes	CAS does not accommodate RADIUS accounting packets greater than 8192 bytes 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. 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. **Workaround** Set a local authentication fallback.

Table 14 List of Resolved Caveats (Sheet 7 of 13)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCsv49225	Yes	Unable to create a VLAN Profile when the VLAN name contains a hyphen This problem only applies to creating a VLAN profile and not when using the name for VLAN mapping. **Note** There is no known workaround for this issue.
CSCsv52402	Yes	When upgrading a CCA-3140 to release 4.5, the NICs are not recognized After an upgrade to release 4.5, the NICs on the CCA-3140 hardware are no longer recognized. This occurs when an appliance that was originally installed with version 3.6.4.4 or earlier is upgraded to 4.1(6), and subsequently upgraded to release 4.5. **Note** This issue only applies to systems that have been upgraded to 4.1(6). Systems upgraded directly from 4.1(5) or earlier are not affected by this defect. **Workaround** Refer to Known Issue with Upgrading CCA-3140 Appliance from Release 4.1(6) to 4.5, page 130for detailed steps.
CSCsv61373	Yes	DHCP Option 78 (slp-directory-agent) is not offered to clients, even though it is a scope option on the server The behavior has been observed in 4.1.3.1 Real-IP CASs. **Workaround** Configure the CAS as DHCP Passthrough device.
CSCsv64925	Yes	SSL communication error with LDAP server while using non-standard CA 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.

Table 14 List of Resolved Caveats (Sheet 8 of 13)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsv71328	Yes	Start the DHCP server when CAM is not reachable 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. Under the following condition the issue will show up: • 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. **Note** DHCP lease/configuration information between the CAS HA pair appliance is assumed to be in sync. See DHCP Failover Behavior Enhancement, page 11 for more information.
CSCsv73765	Yes	File distribution stops working in release 4.5 Downloading the file in a File Distribution requirement fails with an error indicating that the URL is invalid. The file is uploaded to the CAM, and the agent is performing a GET request for the right location, but the CAM sends a redirect to the client causing the file download operation to fail. **Note** There is no known workaround for this issue.
CSCsv74447	Yes	CAS Link-detect to check interface health 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.) **Workaround** We provide an alternative for the Link-detect function in the CAS web console. Cisco NAC Appliance administrators must add the **/etc/ha.d/linkdetect.conf** file specifying CAS interface eth0, eth1, or both to be monitored locally for link healthiness. See CAS HA Pair Link-Detect Configuration Enhancement, page 10 for more information.

Table 14 List of Resolved Caveats (Sheet 9 of 13)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCsv84296	Yes	SNMPv3 traps from switch are not interpreted by CAM if authpriv is used **Symptom** A) Switch sends SNMPv3 TRAP with AuthNopriv, CAM can listen to the TRAP. B) Switch sends SNMPv3 TRAP with Authpriv (MD5-DES), CAM cannot listen to the TRAP. C) Switch sends SNMPv3 TRAP with Authpriv (MD5-DES) to a Software Trap receiver works fine. **Conditions** This condition arises when the Switch and the CAM are configured to use SNMPv3 along with authpriv. **Workaround** A temporary workaround is to use SNMPv3 with authnopriv OR use SNMPv2 altogether.

CSCsw16823	Yes	IP assignment fails for VLAN restricted clients via DHCP relay
		After an upgrade to release 4.5, previously working DHCP IP pools sometimes stop assigning IP addresses. The log file located at **/var/log/dhcplog** displays messages similar to the following:
		`dhcpd: DHCPDISCOVER from 00:aa:bb:cc:dd:ee via 192.168.0.2: unknown network segment`
		`dhcpd: DHCPDISCOVER from 00:aa:bb:cc:dd:ff via 192.168.0.4: network SecureSmart: no free leases`
		The Clean Access Server must be configured to act as a DHCP Server. Some DHCP client requests must be relayed to the Clean Access Server, usually through a wireless gateway or router. The DHCP IP pool must be configured with a VLAN restriction.
		Workaround Fore release 4.5 only, there is a patch you should apply to resolve this issue. See Known Issue for DHCP Address Assignments in Layer 2 and Layer 3 Following Upgrade to Release 4.5(0), page 125.
		Problem
		A defect existed in DHCP IP pool handling in versions prior to release 4.5, in which the DHCP server was unable to differentiate between L2 and L3 DHCP clients connecting with the same VLAN ID, and would hand out inappropriate IP leases as a result. To fix this, IP pools for L3 connected DHCP clients are now required to be properly configured with Relay-IP based restriction. This, unfortunately, requires some reconfiguration for customers who were using L2 restrictions for their L3 IP pools.

Table 14 List of Resolved Caveats (Sheet 10 of 13)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsw20607	Yes	CAS/CAM Disconnect 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. Cisco has addressed this issue by introducing socket timeouts that have been tested in LAN and WAN environments.
CSCsw22550	Yes	DHCPD service locks up after enabling global option After enabling global DHCP options on the CAS and turning on the "one-lease-per-client" global option, the DHCPD service on the CAS stops responding in release 4.5. As a result, administrators cannot edit any of the DHCP options through the web console and the CAS stops handing out DHCP addresses to client machines. The only way to reactivate the web console is by manually stopping the service on the CAS, which only lasts a brief period before the service locks up and renders the web console unusable again. **Note** This issue is for both installation of release 4.5 and upgrade to release 4.5. **Workaround** • For release 4.5 only, There is a patch you should apply to resolve this issue. See Known Issue with DHCPD Service When Global DHCP Option is Enabled in Release 4.5(0), page 126. • Remove the "one-lease-per-client" global option from the DHCP configuration on the CAS.
CSCsw22557	Yes	OS Fingerprint Update required for Blackberry Bold Cisco NAC Appliance is reading the Blackberry Bold OS identifier as a Windows OS. **Note** There is no known workaround for this issue.
CSCsw32990	Yes	Cisco NAC Web Agent version 4.1.6 not checking AVG 8.0 When the Cisco NAC Web Agent is performing posture assessment and verifying whether or not AVG 8 is installed on the client machine, the Web Agent does not correctly recognize AVG 8. **Note** There is no known workaround for this issue.
CSCsw33455	Yes	Improve CAM/CAS communication resiliency during network link failures Bad WANs can make AutoConnectManager hang and not service cases that should connect. 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.

Table 14 List of Resolved Caveats (Sheet 11 of 13)

DDTS Number	Software Release 4.5(1)	
	Corrected	**Caveat**
CSCsw35162	Yes	UI Forefront date-based checks support does not work 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. **Note** Date-based checks are not supported at this time. **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**. **Note** See also CSCsl94153, page 82.
CSCsw67822	Yes	Check and retrieve/delete MAC address from filter-list. An enhancement to the Cisco NAC Appliance API is requested to: 1. Be able to retrieve all MACs for the filters (filter-list) 2. Query the filters (filter-list) if a particular MAC already exists. 3. Delete the MAC entry from the filter-list. **Note** Two new APIs (checkmac/getmaclist) and related information have been added; removemac is already there. See Cisco NAC Appliance API Enhancement, page 11.
CSCsw86694	Yes	CAS/CAM references wrong network configuration file **Netstat -an** shows wrong local IP address for a socket. **Workaround** Delete **ifcfg-eth0/eth1.bak** files from the “networkscripts” directory on the appliance.
CSCsw97200	Yes	Upgrade does not preserve DB snapshot create date/time reported by CAM 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. **Note** There is no known workaround for this issue.
CSCsx02849	Yes	ADSSO can run into trouble if exception is thrown 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. **Workaround** Reboot the CAS.

Table 14 List of Resolved Caveats (Sheet 12 of 13)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsx05756	Yes	ADSSO fails if there is a delay in getting the Kerboros ticket from AD ADSSO fails intermittently when the user is coming out of standby. Packet captures shows there is a delay in refreshing the Kerberos ticket when ADSSO fails. **Workaround** Cancel the window. ADSSO will retry and pass. Reproduced ADSSO failing first time problem with 4.5.0.0 Agent with a 1500ms delay using WAN link simulator.
CSCsx10139	Yes	Upgrade should modify CAS Fallback old default settings to the new one If you upgrade the CAS to release 4.5(1) or 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. **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. **Note** The CAS Fallback default settings for Cisco NAC Appliance releases prior to 4.5(1)/4.1(8) are: – **Fallback Policy**: Ignore – **Detect Interval**: 60 seconds – **Detect Timeout**: 300 seconds The new CAS Fallback default settings with 4.1(8) are: – **Fallback Policy**: Ignore – **Detect Interval**: 20 seconds – **Detect Timeout**: 300 seconds – **Fail Percentage**: 30%

Table 14 List of Resolved Caveats (Sheet 13 of 13)

	Software Release 4.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsx67692	Yes	Apache on the CAS crashes if host polices contain more than 10 hosts Apache on the CAS crashes when publishing host policies if more than 10 policies have been enabled by administrators on the CAM. This is seen when multiple host polices are enabled/disabled under User Management > User Roles > Traffic Control > Host > Unauthenticated Role -> <xxx policy>, with “Parse Proxy Traffic” enabled under: Device Management-> CCA Servers > <one of the CAS> > Filter > Roles > Allowed Hosts. **Workaround** None. Fixed in later releases.

Resolved Caveats - Agent Version 4.5.2.0

Refer to Cisco NAC Appliance Agents, page 23 and Enhancements in Release 4.5(1), page 9 for additional information.

Table 15 List of Resolved Caveats

	Agent Version 4.5.2.0	
DDTS Number	**Corrected**	**Caveat**
CSCsr50995	Yes	Agent does not detect Zone Alarm Security definitions correctly Symptom: User fails posture assessment when checking for AV definitions for Zone Alarm Security Suite 7.0. Conditions: This occurs using either the Any AV check or the Checkpoint Any check. **Workaround** Create a custom check for Zone Alarm Security Suite definition.
CSCsx44947	Yes	Add support for Panda Managed Office Protection Clean Access Agent does not support Panda Managed Office Protection.
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 4.5.1.0

Refer to Cisco NAC Appliance Agents, page 23 and Enhancements in Release 4.5(1), page 9 for additional information.

Table 16 List of Resolved Caveats (Sheet 1 of 5)

	Agent Version 4.5.1.0	
DDTS Number	**Corrected**	**Caveat**
CSCsq70524	Yes	Winsock Error on agent after login is complete Steps to reproduce: 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. **Note** This does issue does not occur in a Layer 3 In-Band RIP setup.
CSCsr20126	Yes	Clean Access Agent does not notify user of need to reboot after WSUS remediation 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. 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. **Workaround** The only workaround is to educate users to use the details button in the agent and to restart after updating the operating system.
CSCsr63531	Yes	Cisco NAC Web Agent does not fully recognize Norton Corporate 10.1 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. **Workaround** Ensure users with Norton Corporate installed on the client machine use the persistent Clean Access Agent instead of the Cisco NAC Web Agent.

Table 16 List of Resolved Caveats (Sheet 2 of 5)

	Agent Version 4.5.1.0	
DDTS Number	**Corrected**	**Caveat**
CSCsr75771	Yes	Symantec AntiVirus 10.x not fully compatible with Clean Access Agent 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. **Note** Launching the update via the Symantec software successfully updates and the client machine, which then passes posture assessment. **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.)
CSCsr97355	Yes	AVG Anti-Virus Free 8.x support for Virus Definition check 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. **Workaround** Create custom checks and rules to detect virus definition update.
CSCsu30467	Yes	NIC must be present when using VPN over EVDO 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. **Workaround** Enable the wireless or wired adapter.
CSCsu45546	Yes	Winsock error 87 Upon resuming from hibernation, Clean Access Agent users will intermittently receive a “Winsock error 87" message. Agent reports following error: “An error occurred while calling the last Windows API function: Error Number = 87 Error Desc = The parameters are incorrect. “ **Workaround** Close the agent and attempt another login.

Table 16 List of Resolved Caveats (Sheet 3 of 5)

	Agent Version 4.5.1.0	
DDTS Number	**Corrected**	**Caveat**

CSCsu54170	Yes	Clean Access Agent does not properly detect McAfee Total Protection Service 4.7
		The Clean Access Agent does not detect McAfee Total Protection 4.7:
		`1. Product Type : AntiVirus (WmiAV)`
		`Product Name : McAfee unknown product`
		`Product Ver. : 4.7.0.566`
		`Def Ver. :`
		`Def Date :`
		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.
		Workaround Create a custom check to check with the following attributes:
		• 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	Clean Access Agent version 4.1.6.0 fails checks in Vista for Symantec Endpoint Protection 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: • 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). **Workaround** Install all Symantec Endpoint Protection components (including Proactive Threat Protection and Network Threat Protection).

Table 16 List of Resolved Caveats (Sheet 4 of 5)

	Agent Version 4.5.1.0	
DDTS Number	**Corrected**	**Caveat**
CSCsv05719	Yes	NOD32 is not detected as a valid AV solution but documented as supported In Cisco NAC Appliance release 4.1(6), Eset 3.x (3.x) passes the requirement but NOD32 (2.x) fails the requirement on a non-English XP installation. It is unconfirmed if this issue exists in versions earlier than 4.1.6. **Workaround** None.
CSCsv49290	Yes	BitDefender Total Security 2009 not detected in Cisco NAC Appliance release 4.1(6)
CSCsw22000	Yes	Intermediate issues detecting the AVG virus definition in Clean Access Agent 4.1.7.0 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. **Note** There is no known workaround for this issue.
CSCsw45111	Yes	Symantec Endpoint Protection version11MR3 can not identify the Def Version The Clean Access Agent cannot detect Symantec Endpoint protection Version 11 MR3 and reports “Error: -2147467259, CCA_Troubleshooting, Method '~' of object '~' failed” for definition version checking. This issue does not occur with Version 11MR2. **Workaround** Disable virus definition checking for version11MR3.
CSCsw47329	Yes	CCA Agent not detecting Trend 17.x Clean Access Agent Version 4.1.7.0 incorrectly detects Trend 17.x as “Trend Micro PC-cillin Internet Security Unknown Product” on clients with Trend Antivirus + Antispyware 17.x installed.
CSCsw52528	Yes	Disable Exit button in System Tray The Clean Access Agent Exit context menu in the system tray can be disabled if the user adds the following DWORD registry key to the client machine: DisableExit = 1 at HKLM\SOFTWARE\Cisco\Clean Access Agent\ See also Windows Clean Access Agent, page 23

Table 16 List of Resolved Caveats (Sheet 5 of 5)

	Agent Version 4.5.1.0	
DDTS Number	**Corrected**	**Caveat**
CSCsw86000	Yes	Clean Access Web Agent re-scan does not work after remediation The Cisco NAC Web Agent Re-Scan button does not work after having performed the AV definition remediation. The following occurs instead: • The Web agent is launched and it detects that the AV definition is not up-to-date. • Remediation is manually performed. • When clicking the Re-Scan button, nothing happens; the re-scan is simply not performed. • If the Web agent is restarted, it correctly detects that the AV definition is up-to-date. **Workaround** Either restart the Web agent, or use the Clean Access Agent.
CSCsw86119	Yes	Avast 4.x does not auto update When running Avast, installation and def checks work but auto update does not. Release notes state that live update is supported. **Workaround** None.

Resolved Caveats - Release 4.5(0)

Note For caveats related to Cisco NAC Profiler, refer to the applicable version of the *Release Notes for Cisco NAC Profiler*.

Note See Table 18 for details on Resolved Caveats - Agent Version 4.5.0.0.

Table 17 List of Closed Caveats (Sheet 1 of 8)

	Software Release 4.5(0)	
DDTS Number	**Corrected**	**Caveat**
CSCsd90433	Yes	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.”
CSCsk58244	Yes	Clean Access Report for WSUS shows failed This situation applies to Windows XP and Windows Vista client machines. The Agent report on the CAM does not show any on the updates required for the client.
CSCsl77438	Yes	CAM should delete obsolete OOB discovered clients There are obsolete OOB discovered clients, either left from deleted switches, or clients never come back. There should be a mechanism to delete these entries: 1. When switch is deleted from managed devices, delete related OOB online users and discovered clients. 2. Add a timers to check expired discovered clients, delete them and related OOB online users if they are not active. (with configurable expire time value). For more information, see Out-of-Band Discovered Clients Cleanup, page 20.
CSCsm24534	Yes	Online Users List/Certified Devices List problem This situation can occur if there are some online users without a Certified Devices List entry and the **Require user to be certified at every web login** option is checked. **Note** If there are two or more online users with the same MAC address and one of them logs out for whatever reason (logout, session timer, heartbeat timer), the MAC address is deleted from the Certified Devices List. This leaves other online users with the same MAC address without a certified device entry. **Workaround** Uncheck the **Require user to be certified at every web login** option.

Table 17 List of Closed Caveats (Sheet 2 of 8)

	Software Release 4.5(0)	
DDTS Number	**Corrected**	**Caveat**
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.
CSCsm42739	Yes	Delay in CAM availability on reboot with Multiple CASs over WAN link The CAM GUI takes a very long time to become available after rebooting when there are multiple CASs with large filter lists to publish. **Note** In some cases, you could have to wait for more than 20 minutes before the CAM GUI becomes available. There is no known workaround for this issue.
CSCsm51889	Yes	Server no longer listens on port 8910 on the trusted interface The Clean Access Server no longer listens on 8910 on the trusted interface. This is breaking Layer 3 Real-IP Out-of-Band deployments featuring ACL. In this deployment scenario, the Agent sends the traffic to the trusted interface because the certificate is generated with the trusted interface IP address (or the DNS resolves to the trusted IP address). **Workaround** Change the DNS resolution to the untrusted IP address.

Table 17 List of Closed Caveats (Sheet 3 of 8)

	Software Release 4.5(0)	
DDTS Number	**Corrected**	**Caveat**
CSCsm76779	Yes	CSRF tag is added to CAS specific MAC Device Filter description field upon edit Steps to reproduce: **1.** Go to CAS-specific device filters in the CAM web console (**Device Management > Clean Access Servers > Manage [IP_Address] > Filter > Devices**). **2.** Edit a device filter with the description field like “<a href=’http://www.cisco.com’>Cisco</a>” **3.** Click **Save**. A CSRF tag is appended to (and is visible in) the hypertext entry in the device filter description field. Subsequent entry updates also append the same CSRF tag each time the administrator edits the description. After editing the description 3 times, however, the entry can no longer be edited and the CAS returns an “Updating device MAC failed” error message. **Note** This issue only addresses CAS-specific device filters and not *global* device filters.
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.”
CSCsm95290	Yes	CAM does not send SNMP SETs to Switches in Out-of-Band The CAM does not send all required SNMP SETs to the switch upon successful user authentication in Out-of-Band environment. The missing SETs could be for VLAN assignment as well as for port bouncing.
CSCso33476	Yes	Blank space after IP address causes static route to fail When adding a static route to a CAS through the CAM GUI, when you enter a IP address and add a space at the end, the route appears to be added in the GUI. However, when you c heck of the routing table on the CAS, the route does not appear. **Workaround** Do not add a space after IP addresses in the CAM GUI.
CSCso41549	Yes	Administrator cannot delete the OUL manually if the In-Band CAS is not available to the CAM If an In-Band CAS fails for some reason (if the CAS suffers a hardware failure, for example), users stay in the Online Users List. **Workaround** Manually delete the entry from the “user_info” table in the CAM database.

Table 17 List of Closed Caveats (Sheet 4 of 8)

	Software Release 4.5(0)	
DDTS Number	**Corrected**	**Caveat**

CSCso47880	Yes	DHCP: wrong default gateway IP address being given out for scope/pool
		When a customer has multiple managed subnets on the same VLAN and has multiple non-continuous scopes on the same VLAN, the default gateway being handed out for the scope is incorrect.
		For example, suppose we have multiple managed subnets on the same VLAN and multiple scopes defined on the same VLAN:
		`10.10.10.0/24 vlan 20`
		`10.52.52.0/24 vlan 20`
		Note This is an administrator initiated issue for which there is no known workaround.

CSCso51899	Yes	HA failover detection not robust enough to detect hard drive failure In some circumstances, an HA standby device can fail to properly detect failure of the active device, resulting in a down/standby state that persists until the failed CAM is manually shut down. One condition that can lead to these issues is failure of the hard drive on the active CAM. The device still responds to heartbeats from the standby, so the standby CAM does not initiate failover. However, attempts to manage the CAM result in HTTP 500 errors and the CAM is unable to authenticate users. **Workaround** To address this issue, you can manually shut down and restart the failed CAM, but HA does not detect and resolve the problem on its own. For more information, see CAM/CAS High Availability Configuration Able to Detect Hard-Drive Failure, page 16.
CSCso57843	Yes	Standby CAS sends improper ARP request after bootup This issue occurs in an HA pair environment using DHCP Synchronization. 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. 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." **1.** Sender MAC: Untrust MAC of Standby CAS—Correct Info **2.** Sender IP: Untrust IP of Active CAS— Wrong Info **3.** Target MAC: 0000.0000.0000—Correct Info **4.** Target IP: Link Detect IP for Untrusted—Correct Info There is no known workaround for this issue.

Table 17 List of Closed Caveats (Sheet 5 of 8)

	Software Release 4.5(0)	
DDTS Number	**Corrected**	**Caveat**

CSCso63083	Yes	LDAP Authentication Fails if DN has a double quotation mark
		When authenticating to an LDAP server from Clean Access (including an Auth Test), authentication fails if the Distinguished Name attribute contains a double-quotation mark (“) character.
		The LDAP server responds to a search with
		`CN=\”Quote Test\”,CN=Users,DC=naaustin,DC=com`
		Then we bind to that user to check the password. But we send back:
		`CN=\\”Quote Test\\”,CN=Users,DC=naaustin,DC=com`
		An extra forward slash (\) is included in the return DN. This causes the bind and authentication to fail. If quote marks are removed from the user entry, authentication works as designed.
		Workaround Remove double-quotation marks from user account DNs.

CSCso76150	Yes	Need to make port VLAN assignments configurable When the user is removed from OUL (through linkdown or when the administrator removes a user from the Certified Devices List), the switch port is automatically moved to Authentication VLAN starting from release 4.1(3). Earlier the behavior was that the switch port VLAN assignment would remain unchanged until another user connected to Cisco NAC Appliance via the same port. Some customers want the earlier behavior preserved. Therefore, we need to make this a configurable option on port profile. For more information, see Assign Restricted VLAN for OOB Client Machines When Disconnected, page 18.
CSCsq27411	Yes	Standby CAS responds to ARP with the wrong MAC address 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. 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. There is no known workaround for this issue.

Table 17 List of Closed Caveats (Sheet 6 of 8)

	Software Release 4.5(0)	
DDTS Number	**Corrected**	**Caveat**
CSCsq59801	Yes	Nessus plug-ins greater than 10 MB size limitation When uploading a NESSUS plug-in .tar file that is greater than 10MB, the CAM returns the following error: “Result: Error: Failed to upload file Content Length Error (18113815 > 10485760)” When the upload file is greater than 10MB, the upload fails. **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.
CSCsq61727	Yes	Adding more than one program to a Launch Program Requirement garbles parameters For a Launch Program requirement type, adding one program works correctly. After adding a second program, however, the first program's parameters become garbled. For example, the parameters change from the correct “config ntrscan start= auto” to “config+ntrscan+start%3d+auto.” This effects execution, as the first program cannot run with the correct parameters.
CSCsq75149	Yes	Shield enhancement for OOB management OOB switch management on the CAM has a limited number of threads set up to deal with incoming SNMP traps. If a switch configuration has gone bad or there is a broken network configuration, the CAM cannot read/write to switches, and the limited number of threads can be quickly consumed. We need a mechanism to isolate bad switches and check them periodically to see whether they become normal or not. For more information, see Out-of-Band Shield Enhancement, page 20.
CSCsr78936	Yes	Need a clearer log message when deleting CA certificates Suggest updating so that “Encountered error: Cannot remove server's CA certificates” to state “Cannot delete CA certificates. Certificates are currently in use.”

Table 17 List of Closed Caveats (Sheet 7 of 8)

	Software Release 4.5(0)	
DDTS Number	**Corrected**	**Caveat**
CSCsu02167	Yes	SSL fails when Netscape Cert Type field does not contain “SSL Client” As a result, the CAS and CAM disconnect from one another and users cannot authenticate. Report log entries show: “SEVERE: SSLManager: client's certificate chain verification failed CN=CAS, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US:Netscape cert type does not permit use for SSL client” If certificates contain a Netscape Cert Type field and are used in release 4.1(6), that field has to contain both “SSL Server” and “SSL Client.” If the field does not contain “SSL Client,” communication between the CAS and CAM fails. If the Netscape Cert Type field does not exist, then SSL succeeds. If the Netscape Cert Type field does exist, but does not contain both “SSL Server” and “SSL Client,” authentication fails. **Note** This issue has been observed with Entrust certificates and another educational CA. **Workaround** • Get certificate reissued by CA with no Netscape Cert Type field, or ensure the field contains both “SSL Server” and “SSL Client.” • Use temporary certs (**not recommended**).
CSCsu26775	Yes	Unable to upload 4.5 upgrade patch in 4.1(x) CAS web UI In Cisco NAC Appliance releases prior to 4.5, the CAS web console upload feature (Administration > Software Update) does not allow upgrade files larger than 200MB to be uploaded to CAS. Upload fails with the following error “Error: Failed to upload file Content Length. Error (260551527 > 209715200)” To address this issue, Cisco has increased the file size limit to 500MB in release 4.5. **Note** Using CAS UI to upgrade the CAS from 4.5 to 4.5+ will work fine, but 4.1(x) to 4.5 upgrades will fail because the 4.5 upgrade file is larger than 200MB. **Workaround** Use the Command-Line Interface for upgrade instead of web GUI. (See also Known Issues with Web Upgrade in Release 4.1(x) and Earlier, page 127.)

Table 17 List of Closed Caveats (Sheet 8 of 8)

	Software Release 4.5(0)	
DDTS Number	**Corrected**	**Caveat**

CSCsu43508	Yes	Cavium errors on NAC-3140 upon CAM/CAS startup upgraded from 4.1(0)/4.0(3)
		Cavium error messages are seen on CCA-3140 CAM (Clean Access Manager) / CAS (Clean Access Server) when upgraded from releases prior to 4.1.0 / 4.0.3. The following snippet shows part of the error message that gets displayed upon CAM/CAS startup:
		`Starting atd: [  OK  ]`
		`/etc/rc3.d/S99local: line 9: cd: /perfigo/cavium_sdk/bin/: No such file or directory`
		`/etc/rc3.d/S99local: line 9: ./init_nitrox: No such file or directory`
		`Starting perfigo:  click: starting router thread pid 2973 (f743bf00)`
		Customers upgrading whose initial installed version was old (4.0.0-4.0.3) could see the message "pkp_drv: module license 'CAVIUM' taints kernel." This message can be safely ignored.
		There is no known workaround for this issue.

CSCsu91017	Yes	GSSAPI authentication fails intermittently for child domain users LDAP GSSAPI authentication fails intermittently for users in child domain. **Note** This problem is not seen for root domain users. There is no known workaround for this issue.

Resolved Caveats - Agent Version 4.5.0.0

Note For caveats related to Cisco NAC Profiler, refer to the applicable version of the *Release Notes for Cisco NAC Profiler*.

Note See Table 17 for details on Resolved Caveats - Release 4.5(0).

Table 18 List of Closed Caveats (Sheet 1 of 3)

	Agent Version 4.5.0.0	
DDTS Number	**Corrected**	**Caveat**
CSCsk46850	Yes	Oldest Agent session fails with mixed SSO In a mixed login environment (authentication for both wired users and VPN SSO for wireless users with the same accounts) an issue occurs in which the combined total of wired and wireless login sessions is sufficient to exceed the maximum configured user session limit, but if the oldest session is wireless, attempting to "end the oldest session" from the client fails. **Workaround** The Cisco NAC Appliance administrator must manually purge the oldest login session(s).
CSCsm53743	Yes	File ownership of Mac OS X Agent directory and related files should be corrected File ownership of Mac OS X Agent and related files should be "root:admin." Currently, the file ownership is with UID 505 and GID 505. Anyone able to assume this UID could potentially modify the Agent application files and introduce a security threat.
CSCsm79088	Yes	Mac OS X Agent reports "Unknown user" when sending the second logout request The Mac OS X Agent specifies an "Unknown user" when it sends a second logout request before receiving a response from the first logout request. Steps to reproduce: **1.** Log into the network using the Mac OS X Agent. **2.** Right-click on Agent icon and choose **Logout**. **3.** Repeat step 2 before receiving a response for the first logout request. The Mac Agent displays a "Cisco Clean Access Agent is having a difficulty with the server. Unknown user." error message, resulting in a situation where the client machine no longer appears in the CAM's Online Users list even though the Agent indicates that the user is logged in. In this situation, the Mac Agent essentially "freezes" as the user is no longer able to log out, ether.

Table 18 List of Closed Caveats (Sheet 2 of 3)

	Agent Version 4.5.0.0	
DDTS Number	**Corrected**	**Caveat**
CSCso81146	Yes	The Mac OS X Agent does not perform posture assessment in L3 with Device Filters Role As a result, the user is assigned the Temporary role in L3 using the Device Filters Role requiring posture assessment. **Workaround** • If the user requires posture assessment, use Device Filters Check in L3. • If the user does not require posture assessment, use Device Filters Role with no requirement in L3.
CSCso90974	Yes	Auto-upgrade does not work for Mac OS X Agent with VPN SSO enabled No auto-upgrade message is shown using VPN SSO when the CAM has a new Mac OS X Agent available. The network settings leading to this circumstance are: • Client is running an old Mac OS X Agent (version 4.1.3.1 or earlier) • The CAM has a newer version of the Mac OS X Agent available (version 4.5.0.0 or later) • The CAS has VPN SSO enabled In this scenario, the Mac OS X Agent still logs the user in via VPN SSO, but does not automatically upgrade the Agent. Therefore, the same Agent (version 4.1.3.1 or later) remains on the client machine after the VPN SSO login. **Workaround** Customers have two choices: • The user can manually download the new Agent via the web login page. • Disable VPN SSO on the CAM.
CSCso91681	Yes	Mac Agent auto-upgrade fails on slow connections With slow connections, the Mac OS X Agent may not finish downloading via HTTP in time. If the Agent download does not complete within approximately 10 seconds, it can fail. This issue exists in 256 kbps and 512 kbps bandwidth conditions. **Workaround** Cisco recommends users open a browser window and perform Web Login. After login, click the **Download** button to manually download and install the new Agent.

Table 18 List of Closed Caveats (Sheet 3 of 3)

	Agent Version 4.5.0.0	
DDTS Number	**Corrected**	**Caveat**
CSCso91745	Yes	Mac OS X Agent may not pop-up or login may fail on networks with high latency Round-trip network latency between client machine and the CAS should be 1000 ms or higher. As SWISS response timeout is 1 second, the Mac OS X Agent does not appear to users where the round-trip latency between the client machine and the CAS is 1000 ms or more. **Note** There is no known workaround for this issue.

New Installation of Release 4.5

The following steps summarize how to perform new CD software installation of release 4.5 on supported Cisco NAC Appliance hardware platforms (see Release 4.5 and Hardware Platform Support, page 3 for additional support details).

To upgrade or re-image a Cisco NAC Network Module, refer to the instructions in *Getting Started with Cisco NAC Network Modules in Cisco Access Routers*.

To upgrade on an existing NAC Appliance, refer to the instructions in Upgrading to Release 4.5, page 111.

For New Installation:

With release 4.5, installation occurs in two phases:

1. The software is installed from the CD, and when complete, the CD is ejected from the appliance.
2. The admin logs in and performs the initial configuration.

Step 1 If you are going to perform a new installation but are running a previous version of Cisco Clean Access, Cisco recommends backing up your current Clean Access Manager installation and saving the snapshot on your local computer, as described in General Preparation for Upgrade, page 114.

Step 2 Follow the instructions on your welcome letter to obtain product license files for your installation. See Licensing, page 2 for details. (If you are evaluating Cisco Clean Access, visit http://www.cisco.com/go/license/public to obtain an evaluation license.)

Step 3 Install the latest version of 4.5 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 4.5.1 subdirectory, download the latest 4.5(1) .ISO image, (e.g. **nac-4.5_1-K9.iso**) and burn the image as a bootable disk to a CD-R.

Note Cisco recommends burning the .ISO image to a CD-R using speeds 10x or lower. Higher speeds can result in corrupted/unbootable installation CDs.

c. Insert the CD into the CD-ROM drive of each installation server, and follow the instructions in the auto-run installer.

Step 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.

Step 5 Install a valid FlexLM product license file for the Clean Access Manager (either evaluation, starter kit, or individual license).

Step 6 At the admin login prompt, login with the web console username and password you configured when you installed the Clean Access Manager.

Step 7 In the web console, navigate to **Administration > CCA Manager > Licensing** to install any additional license files for your CASs, CAM HA pairs or CAS HA pairs. You must install the CAS license to add the CASs to the CAM and an OOB CAS license to enable OOB features on the CAM.

Step 8 For detailed steps on initial configuration, refer to the *Cisco NAC Appliance Hardware Installation Quick Start Guide, Release 4.5*.

For additional information on configuring your deployment, including adding the CAS(s) to the CAM, refer to the following guides:

- *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5(1)*
- *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.5(1)*

Note Clean Access Manager 4.5(1) is bundled with version 4.5.1.0 of the Cisco NAC Appliance Agents.

Note Cisco NAC Appliances assume the keyboard connected to be of US layout for both direct and IP-KVM connections. Use a US layout keyboard or ensure that you know the key mapping if you are connecting a keyboard of different layout.

Upgrading to Release 4.5

This section provides instructions for how to upgrade your existing supported Cisco NAC Appliance platform to release 4.5. If you need to perform a CD software installation, refer instead to New Installation of Release 4.5, page 110.

Refer to the following information prior to upgrade:

- Changes for 4.5 Installation/Upgrade
- General Preparation for Upgrade
- Upgrade Instructions for Standalone Machines
- Upgrade Instructions for HA Pairs

Changes for 4.5 Installation/Upgrade

Cisco NAC Appliance (Cisco Clean Access) release 4.5 ED and later is a major software release with Early Deployment status. Cisco strongly recommends to test new releases on a pilot system prior to upgrading your production system.

If planning to upgrade to Cisco NAC Appliance 4.5 ED and later, note the following:

- Hardware Considerations
- Features That May Change With Upgrade
- Upgrade Changes
- Password Changes

Hardware Considerations

- **Release 4.5 and later only supports and can only be installed on Cisco NAC Appliance CCA-3140, NAC-3310, NAC-3350, NAC-3390, and NME-NAC-K9 (NAC network module) platforms.** You cannot upgrade to or install release 4.5 on any other platform. See Hardware Support, page 2 for additional details.
- With release 4.5, there is only one product installation CD (.ISO) for all appliance platforms. The installation package determines whether the Clean Access Server, Clean Access Manager, or Super Clean Access Manager was previously installed, as well as the previous software version.
- **Starting from Release 4.5, the DL140 and serial_DL140 boot installation directives are no longer required when installing the software on NAC-3310 appliances.**
- If performing CD software installation on a NAC-3310 based appliance which is not reading the software on the CD ROM drive, refer to Known Issue with NAC-3310 Based Appliances.
- If you are planning to upgrade the CCA-3140 appliance, a workaround is needed if upgrading from release 4.1.6 to release 4.5. Refer to Known Issue with Upgrading CCA-3140 Appliance from Release 4.1(6) to 4.5, page 130 for details.

Features That May Change With Upgrade

- For new installations of Cisco NAC Appliance Release 4.5(1), the CAS Fallback behavior enhancement introduces new default values for the **Detect Interval** and **Detect Timeout** settings (20 and 300 seconds, respectively) and requires that the **Detect Timeout** value be at least 15 times the specified **Detect Interval**. If you are upgrading to release 4.5(1), 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 4.5(1). For more information, see CAS Fallback Behavior Enhancement, page 10.
- When upgrading a VPN SSO Cisco NAC Appliance network to release 4.5, user login does not work properly **when the user VPN is part of a managed subnet on the CAS**. For more information, see Known Issue for VPN SSO Following Upgrade to Release 4.5, page 125.
- After upgrading to Cisco NAC Appliance release 4.5, DHCP IP address pools configured on the CAS that provided valid DHCP IP address assignments using the previous release can sometimes stop assigning IP addresses. For more information, see Known Issue for DHCP Address Assignments in Layer 2 and Layer 3 Following Upgrade to Release 4.5(0), page 125.

Note This known issue only applies to Cisco NAC Appliance release 4.5 and has been resolved as of release 4.5(1).

- In release 4.5, if you have enabled the "one-lease-per-client" global DHCP option and turned on global options (in the **Device Management > CCA Servers > Manage [CAS_IP] > Network > DHCP > Global Options** page, **Root Global Option List**), the DHCPD service on the CAS stops responding. There is a patch you should apply to resolve this issue. See Known Issue with DHCPD Service When Global DHCP Option is Enabled in Release 4.5(0), page 126.

Note This known issue only applies to Cisco NAC Appliance release 4.5 and has been resolved as of release 4.5(1).

Upgrade Changes

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 4.5 and later. You must correct your certificate chain to successfully upgrade to release 4.5 and later. For details on how to fix certificate errors on the CAM/CAS after upgrade to release 4.5 and later, refer to the *How to Fix Certificate Errors on the CAM/CAS After Upgrade* Troubleshooting Tech Note.**

Note **Web upgrade is no longer supported for upgrade to release 4.5**. To upgrade your CAM and CAS from 4.1(x) or 4.0(x) releases, you must copy the **cca_upgrade-4.5.1-NO-WEB.tar.gz** file to each CAM and CAS appliance and run the upgrade script via the command line. Refer to Known Issues with Web Upgrade in Release 4.1(x) and Earlier, page 127 for details.

- Starting from Cisco NAC Appliance release 4.1(6) and later, 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.
- When upgrading CAM/CAS software images prior to release 4.1(6), administrators may notice "4.1.6" upgrade messages during the release 4.5 upgrade process. These messages are part of a normal two-step upgrade process and do not have any impact on the release 4.5 upgrade.
- Upgrade file names are slightly different if you use the CAM/CAS web console to upload the upgrade file to the CAM/CAS instead of using WinSCP, SSH File Transfer, or PSCP to copy the upgrade file to your machines. The names of files uploaded via web console contain appended numeric codes that you must know in order to extract upgrade files and initiate the upgrade process. For more information, see Known Issues with Web Upgrade in Release 4.1(x) and Earlier, page 127.
- Release 4.5 includes version 2.1.8-37 of the Cisco NAC Profiler Collector component that resides on the CAS installations. When upgrading CAS appliances (standalone or HA) to release 4.5, the upgrade script will check the version of the Collector and only upgrade it if version 2.1.8-37 is not already installed. Refer to the *Release Notes for Cisco NAC Profiler* for software compatibility matrixes and additional upgrade and product information.

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.

Password Changes

- To offer increased security against potential unauthorized access to Cisco NAC Appliance, the CAM and CAS root admin password you specify during initial system configuration (when performing fresh install or release 4.5 or reconfiguring the appliance via **service perfigo config**) must now meet strong password standards, as described in Strong Password Support for Root Admin Users, page 21. However, any existing CAM/CAS root passwords are preserved during upgrade.
- For new installations of Cisco NAC Appliance, there is no longer a default **cisco123** CAM web console password. Administrators must specify a unique password for the CAM web console. However, any existing CAM web console passwords (including the old default **cisco123**) are preserved during upgrade.

For additional details, see also:

- Hardware Support, page 2
- Out-of-Band Enhancements, page 17
- Known Issues for Cisco NAC Appliance, page 124

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 4.5 software and some running 4.1(x) software).

- **Upgrade Downtime Window**

  Depending on the number of Clean Access Servers you have, the upgrade process should be scheduled as downtime. For minor release upgrades (e.g. 4.5 to 4.5(1)), 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 also Known Issues with NAC-3300 Series Appliances and Serial HA (Failover) Connection, page 131.

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

  Cisco recommends creating a manual backup snapshot before and after upgrade of your CAM database. The snapshot contains CAM database configuration and CAS configuration for all CASs added to the CAM's domain. Pre- and post-upgrade snapshots allow you to revert to your previous database should you encounter problems during upgrade and preserves your upgraded database as a baseline after upgrade. Make sure to download the snapshots to another machine for safekeeping. After upgrade, delete all earlier snapshots from the CAM web console as they are no longer compatible. See Copy the Upgrade File to the CAS/CAM, page 117.

Warning **You cannot restore a CAM database from a snapshot created using a different release. For example, you cannot restore a 4.1(x) or earlier database snapshot to a 4.5 CAM.**

- **Software Downgrade**

  Once you have upgraded your software to release 4.5(1), if you wish to revert to your previous version of software, you will need to reinstall the previous version from the CD and recover your configuration based on the backup you performed prior to upgrading to 4.5(1). See Upgrade Instructions for Standalone Machines, page 116 for additional details.

- **Passwords**

  For upgrade via console/SSH, you will need your CAM and CAS `root` user password. See Default CAM Web Console Password Removed, page 23 for additional details.

Upgrading from Customer-Supplied Hardware to Cisco NAC Appliance Hardware Platforms

If you are running the Cisco NAC Appliance software (release 4.1(x) or earlier) on a non-appliance platform, you will need to purchase Cisco NAC Appliance hardware before you can upgrade your system to Release 4.5. You may additionally need to obtain proper FlexLM product licenses. Once you obtain a Cisco NAC platform, Cisco recommends that you:

Step 1 Back up your current system and create a backup snapshot for the software version you are running (e.g. 4.1(x)).

Step 2 Download and install the same software version on your new Cisco NAC appliance platform (e.g. 4.1(x)).

Step 3 Restore the snapshot to your new Cisco NAC appliance.

Step 4 If necessary, upgrade your appliance to 4.0(x) or 4.1(x). Then follow the appropriate upgrade procedure to upgrade your Cisco NAC Appliance to release 4.5.

Step 5 Create a backup snapshot of your upgraded system.

Note If you need to upgrade from a much older version of Cisco Clean Access, you may need to perform an interim upgrade to a version that is supported for upgrade to 4.5 or later. In this case, refer to the applicable *Release Notes* for upgrade instructions for the interim release. Cisco recommends to always test new releases on a different system first before upgrading your production system.

Upgrade Instructions for Standalone Machines

Note **Web upgrade is no longer supported for upgrade to release 4.5**. To upgrade your CAM and CAS from 4.1(x) or 4.0(x) releases, you must copy the **cca_upgrade-4.5.1-NO-WEB.tar.gz** file to each CAM and CAS appliance and run the upgrade script via the command line. Refer to Known Issues with Web Upgrade in Release 4.1(x) and Earlier, page 127 for details.

This section describes how to upgrade standalone (i.e. non-HA) CAM/CAS machines from release 4.0(x)/4.1(x) to the latest 4.5 release.

Review Changes for 4.5 Installation/Upgrade, page 111 and General Preparation for Upgrade, page 114 before proceeding with these upgrade instructions.

After you have downloaded and copied the upgrade file to the CAM/CAS, you must use the CAM/CAS CLI to extract the upgrade image files and perform the upgrade procedure as described in Run Upgrade Script on the CAM/CAS, page 118.

Summary of Steps for Standalone Upgrade

The steps to upgrade standalone 4.0(x)/4.1(x) systems are as follows:

1. Create CAM DB Backup Snapshot, page 116
2. Download the Upgrade File, page 117
3. Copy the Upgrade File to the CAS/CAM, page 117
4. Run Upgrade Script on the CAM/CAS, page 118

Create CAM DB Backup Snapshot

This section describes how to back up your current system.

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. 01_08_09-15-47_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. **01_08_09-15-47_snapshot_VER_4_5_0.gz**).

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

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

Step 6 After upgrade, delete all earlier snapshots from the CAM web console as they will no longer be compatible.

Note Cisco NAC Appliance creates automatic snapshots before and after software upgrades and failover events, and preserves the last 5. For further details, see "Database Recovery Tool" in the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5*.

Download the Upgrade File

This section describes how to access and download the upgrade file to your local machine.

Note **Web upgrade is no longer supported for upgrade to release 4.5**. To upgrade your CAM and CAS from 4.1(x) or 4.0(x) releases, you must copy the **cca_upgrade-4.5.1-NO-WEB.tar.gz** file to each CAM and CAS appliance and run the upgrade script via the command line. Refer to Known Issues with Web Upgrade in Release 4.1(x) and Earlier, page 127 for details.

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 4.5.1 subdirectory, download the latest 4.5(1) 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.

Copy the Upgrade File to the CAS/CAM

This section describes how to 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.

Caution If upgrading from Release 4.1(6) or earlier, the upgrade file MUST be copied to the **/store** directory on the respective CAM or CAS machine before running upgrade from the command line as described in Run Upgrade Script on the CAM/CAS, page 118.

If using WinSCP or SSH File Transfer

Step 1 Access the CAM via WinSCP or SSH File Transfer.

Step 2 Copy the **cca_upgrade-4.5.1-NO-WEB.tar.gz** file from your local machine to the **/store** directory on the Clean Access Manager.

Step 3 Access each CAS via WinSCP or SSH File Transfer.

Step 4 Copy the **cca_upgrade-4.5.1-NO-WEB.tar.gz** file from your local machine to the **/store** directory on *each* Clean Access Server.

If using PSCP

Step 1 Open a command prompt on your Windows computer.

Step 2 Cd to the path where your PSCP resides (e.g, C:\Documents and Settings\desktop).

Step 3 Enter the following command to copy the file to the **/store** directory on the CAM:

```
pscp cca_upgrade-4.5.1-NO-WEB.tar.gz   root@<ipaddress_manager>:/store
```

Step 4 Enter the following command to copy the file to the **/store** directory on the CAS (copy to each CAS):

```
pscp cca_upgrade-4.5.1-NO-WEB.tar.gz   root@<ipaddress_server>:/store
```

Run Upgrade Script on the CAM/CAS

This section describes how to untar the upgrade file and run the script to upgrade standalone CAM/CAS machines from release 4.0(x)/4.1(x) to the latest 4.5 release. You will need to login with your CAM and CAS `root` user passwords and access the command line of the CAM or CAS machine using one of the following methods:

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

When run, the upgrade script automatically determines whether the machine is a Clean Access Manager (CAM) or Clean Access Server (CAS) and executes accordingly.

Note The 4.5 upgrade script only executes if the current system is a supported Cisco NAC Appliance platform. Otherwise, the script exits with message "Unable to upgrade, not a recommended hardware platform for 4.5.x".

Upgrade the CAM

Note If upgrading a CCA-3140 appliance from release 4.1(6) to release 4.5, refer to Known Issue with Upgrading CCA-3140 Appliance from Release 4.1(6) to 4.5, page 130 prior to upgrade.

Step 1 Connect to the Clean Access Manager to upgrade using a console connection, or Putty or SSH.

Step 2 Log in as user `root` with root password.

Step 3 Change directory to **/store**:

```
cd /store
```

Step 4 Locate the upgrade file. If you used WinSCP, SSH File Transfer, or PSCP, the upgrade filename is **cca_upgrade-4.5.1-NO-WEB.tar.gz**.

```
ls -l
```

Step 5 Extract the contents of the downloaded upgrade file:

```
tar xzvf cca_upgrade-4.5.1-NO-WEB.tar.gz
```

The extraction process automatically places the upgrade files and necessary upgrade script in the **/cca_upgrade-4.5.1** directory.

Step 6 Change to the **/cca_upgrade-4.5.1** directory and execute the upgrade process:

```
cd cca_upgrade-4.5.1
./UPGRADE.sh
```

Step 7 When prompted to update the Windows Agent and Agent Patch, specify **y** or **n** to upgrade the Agent and Agent patch or retain the current Agent and Agent patch versions, respectively.

```
Please choose whether to upgrade Windows Agent to 4.5.1.0 and Agent Patch to 4.5.1.0 (It's
highly recommended to upgrade) (y/n)? [y]
Please choose whether to upgrade Mac Agent to 4.5.0.0 (It's highly recommended to upgrade)
(y/n)? [y]
```

Step 8 Wait for the upgrade to complete. This will take several minutes

```
...stopping CCA Manager...

Welcome to the CCA Manager migration utility.

...Upgrading to newer rpms of 4.5.1...done.
...Upgrading CCA files...done
Windows Agent and Agent Patch were upgraded to 4.5.1.0 and 4.5.1.0 respectively.
Mac Agent was upgraded to versions 4.5.0.0.
Clearing Tomcat cache...checking ssl configuration...done.
[root@cam127 cca_upgrade-4.5.1]#
```

Step 9 When upgrade is done, reboot the machine at the prompt:

```
reboot
```

Tip You can run **cat /perfigo/build** to verify the software version before and after upgrade.

Upgrade the CAS

Note If upgrading a CCA-3140 appliance from release 4.1(6) to release 4.5, refer to Known Issue with Upgrading CCA-3140 Appliance from Release 4.1(6) to 4.5, page 130 prior to upgrade.

Step 1 Connect to the Clean Access Server to upgrade using a console connection, or Putty or SSH.

Step 2 Log in as user **root** with root password.

Step 3 Change directory to **/store**:

```
cd /store
```

Step 4 Locate the upgrade file. If you used WinSCP, SSH File Transfer, or PSCP, the upgrade filename is **cca_upgrade-4.5.1-NO-WEB.tar.gz**.

```
ls -l
```

Step 5 Extract the contents of the downloaded upgrade file:

```
tar xzvf cca_upgrade-4.5.1-NO-WEB.tar.gz
```

The extraction process automatically places the upgrade files and necessary upgrade script in the **/cca_upgrade-4.5.1** directory.

Step 6 Change to the **/cca_upgrade-4.5.1** directory and execute the upgrade process:

```
cd cca_upgrade-4.5.1
./UPGRADE.sh
```

Step 7 Wait for the upgrade to complete. This will take several minutes

```
...stopping CCA Server...
BaseAgent process stopped!
Stopping DHCP...
In Maintenance Mode...

Welcome to the CCA Server migration utility.

...Upgrading to newer rpms of 4.5.1...done.
...Upgrading CCA files...done
Clearing Tomcat cache...checking ssl configuration...done.
[root@cas128 cca_upgrade-4.5.1]#
```

Step 8 When upgrade is done, reboot the machine at the prompt:

```
reboot
```

Step 9 Repeat steps 1 through 8 for each CAS managed by the CAM.

Tip You can run **`cat /perfigo/build`** to verify the software version before and after upgrade.

Upgrade Instructions for HA Pairs

This section describes how to upgrade high-availability (HA) pairs of CAM or CAS servers from release 4.0(x)/4.1(x) to the latest 4.5 release.

If you have standalone CAM/CAS servers, refer instead to Upgrade Instructions for Standalone Machines, page 116.

Review Changes for 4.5 Installation/Upgrade, page 111 and General Preparation for Upgrade, page 114 before proceeding with these upgrade instructions.

Note **Web upgrade is no longer supported for upgrade to release 4.5**. To upgrade your CAM and CAS from 4.1(x) or 4.0(x) releases, you must copy the **cca_upgrade-4.5.1-NO-WEB.tar.gz** file to each CAM and CAS appliance and run the upgrade script via the command line. Refer to Known Issues with Web Upgrade in Release 4.1(x) and Earlier, page 127 for details.

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 also Known Issues with NAC-3300 Series Appliances and Serial HA (Failover) Connection, page 131.

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

Upgrading HA-CAM and HA-CAS Pairs

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

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

Note If upgrading a CCA-3140 appliance from release 4.1(6) to release 4.5, refer to Known Issue with Upgrading CCA-3140 Appliance from Release 4.1(6) to 4.5, page 130 prior to upgrade.

Step 1 Download and save the upgrade file to your local PC, as described in Download the Upgrade File, page 117.

Step 2 From either a console connection (keyboard/monitor/KVM) or via SSH, connect to the individual IP address of each machine in the failover pair.

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

Step 3 Login as the `root` user with the root password.

Step 4 Copy the upgrade image to each CAM/CAS machines’ **/store** directory as described in Copy the Upgrade File to the CAS/CAM, page 117.

Step 5 Change directory to **/store**:

```
cd /store
```

Step 6 Locate the upgrade file. If you used WinSCP, SSH File Transfer, or PSCP, the upgrade filename is **cca_upgrade-4.5.1-NO-WEB.tar.gz**.

```
ls -l
```

Step 7 Extract the contents of the downloaded upgrade file:

```
tar xzvf cca_upgrade-4.5.1-NO-WEB.tar.gz
```

The extraction process automatically places the upgrade files and necessary upgrade script in the **/cca_upgrade-4.5.1** directory.

Step 8 Before proceeding, determine the failover state on each machine by changing directory and running the **fostate.sh** command on each machine:

```
cd /perfigo/common/bin/
./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 appliance 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 appliance is active or standby as follows:

- Access the web console as described in “Accessing Web Consoles in High Availability Pairs” sections of the “Configuring High Availability” chapters in both the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.5* and the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.5*.
- 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 9 Stop services on the standby appliance by entering the following command via the console/SSH terminal:

```
service perfigo stop
```

Step 10 Wait until the standby appliance has suspended services.

Step 11 Change directory and run the **fostate.sh** command on the active appliance:

```
cd /perfigo/common/bin/
./fostate.sh
```

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

Step 12 Upgrade the active appliance as follows:

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

b. From the untarred upgrade directory created on the active appliance (for example **cca_upgrade-4.5.1**), run the upgrade script on the active appliance:

```
./UPGRADE.sh
```

c. For the CAM, when prompted to update the Windows Agent and Agent Patch, specify **y** or **n** to upgrade the Agent and Agent patch or retain the current Agent and Agent patch versions, respectively.

```
Please choose whether to upgrade Windows Agent to 4.5.1.0 and Agent Patch to 4.5.1.0
(It's highly recommended to upgrade) (y/n)? [y]
Please choose whether to upgrade Mac Agent to 4.5.0.0 (It's highly recommended to
upgrade) (y/n)? [y]
```

Step 13 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 14 Restart services on the standby appliance by entering the following command via the console/SSH terminal:

```
service perfigo start
```

Step 15 Upgrade the standby appliance as follows:

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

b. Change to the untarred upgrade directory created on the standby appliance:

```
cd cca_upgrade-4.5.1
```

c. Run the upgrade script on the standby appliance:

```
./UPGRADE.sh
```

d. For the CAM, when prompted to update the Windows Agent and Agent Patch, specify `y` or `n` to upgrade the Agent and Agent patch or retain the current Agent and Agent patch versions, respectively.

```
Please choose whether to upgrade Windows Agent to 4.5.1.0 and Agent Patch to 4.5.1.0
(It's highly recommended to upgrade) (y/n)? [y]
Please choose whether to upgrade Mac Agent to 4.5.0.0 (It's highly recommended to
upgrade) (y/n)? [y]
```

Step 16 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 17 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 18 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 appliances reboot.

Known Issues for Cisco NAC Appliance

This section describes known issues when integrating Cisco NAC Appliance:

- Known Issue with Mass DHCP Address Deletion
- Known Issue for VPN SSO Following Upgrade to Release 4.5
- Known Issue for DHCP Address Assignments in Layer 2 and Layer 3 Following Upgrade to Release 4.5(0)
- Known Issue with DHCPD Service When Global DHCP Option is Enabled in Release 4.5(0)
- Known Issues with Web Upgrade in Release 4.1(x) and Earlier
- Known Issues with www.perfigo.com Root CA
- Known Issue with Active HA CAM Web Console Following Failover
- Known Issue with Upgrading CCA-3140 Appliance from Release 4.1(6) to 4.5
- Known Issue with NAC-3310 Based Appliances
- Known Issues with NAC-3300 Series Appliances and Serial HA (Failover) Connection
- Known Issues with Switches
- Known Issues with Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs)
- Known Issue for Windows Vista and IP Refresh/Renew
- Known Issues for Windows Vista and Agent Stub
- Known Issues with MSI Agent Installer
- Known Issue with Windows 2000 Clean Access Agent/Local DB Authentication
- Known Issue with Windows XP/2000 and Windows Script 5.6

Known Issue with Mass DHCP Address Deletion

An issue exists in release 4.5(1) 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 90.

Note In release 4.5(1), 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 79.

Known Issue for VPN SSO Following Upgrade to Release 4.5

When you upgrade your Cisco NAC Appliance network employing VPN SSO to release 4.5, user login does not work properly **when the user VPN is part of a managed subnet on the CAS**.

In release 4.5, the SWISS protocol checks the MAC address for Layer 2 clients, but the MAC address reported by the Agent (which is the real client MAC address) is different from the one the CAS gets for the client (the VPN concentrator MAC address). As a result, the SWISS protocol tells the Agent that the client machine is not logged in (due to the different MAC addresses recorded) and the Agent launches the login dialog repeatedly, never able to complete login. Prior to release 4.5, the Clean Access Server associates the client with the VPN IP address and VPN Concentrator's MAC address after the first login. From there, the SWISS protocol only checks the IP address from the Agent and reports back to the Agent that the client is logged in (regardless of whether the client is connected via Layer 2 or Layer 3).

To work around this issue, remove the subnet making up the client machine address pool from the collection of managed subnets and create a Layer 3 static route on the CAS untrusted interface (eth1) with VPN concentrator's IP address as the gateway for the VPN subnet using the CAM web console **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > Static Routes** page.

Known Issue for DHCP Address Assignments in Layer 2 and Layer 3 Following Upgrade to Release 4.5(0)

Note This known issue only applies to Cisco NAC Appliance release 4.5(0) and has been resolved as of release 4.5(1).

After upgrading to Cisco NAC Appliance release 4.5, DHCP IP address pools configured on the CAS that provided valid DHCP IP address assignments using the previous release can sometimes stop assigning IP addresses. (See also CSCsw16823, page 89) A defect existed in DHCP IP pool handling in Cisco NAC Appliance releases prior to 4.5, in which the DHCP server was unable to differentiate between Layer 2 and Layer 3 DHCP clients connecting with the same VLAN ID. As a result, the CAS would hand out inappropriate IP address leases to client machines. In order for this issue to appear, a few criteria must exist within the network configuration:

- The Clean Access Server must be configured and operating as a DHCP Server.

- Some DHCP client requests must be relayed to the Clean Access Server, usually through a wireless gateway or router.
- The DHCP IP pool must be configured with a VLAN restriction.

To verify whether or not this issue is present in your network, you can view the log file located at **/var/log/dhcplog** and see if it displays messages similar to the following:

```
dhcpd: DHCPDISCOVER from 00:aa:bb:cc:dd:ee via 192.168.0.2: unknown network segment
dhcpd: DHCPDISCOVER from 00:aa:bb:cc:dd:ff via 192.168.0.4: network SecureSmart: no free
leases
```

To address this issue, apply the **Patch-CSCsw16823.tar.gz** patch to the CAS:

Note Apply this patch to the CAS only.

Step 1 Go to the Cisco Security Software download site at http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml and download the **Patch-CSCsw16823.tar.gz** file to your local machine.

Step 2 Place the **Patch-CSCsw16823.tar.gz** file in the **/store** directory on the CAS.

Step 3 Navigate to **/store**: **`cd /store`**.

Step 4 Enter **`tar zxvf Patch-CSCsw16823.tar.gz`** to extract the patch files in the **Patch-CSCsw16823** directory.

Step 5 Navigate to **Patch-CSCsw16823**: **`cd Patch-CSCsw16823`**.

Step 6 Enter **`./apply.sh`** to patch the CAS perfigo.jar files on the CAS.

Note Make sure following file permissions are correct on your system:

```
PERM        OWNER GROUP SIZE FILE_PATH
-rwxr-xr-x  root  root  1883230 /perfigo/access/tomcat/shared/lib/perfigo.jar
-rwxr-xr-x  root  root  1883230 /perfigo/agent/lib/perfigo.jar
```

Known Issue with DHCPD Service When Global DHCP Option is Enabled in Release 4.5(0)

Note This known issue only applies to Cisco NAC Appliance release 4.5(0) and has been resolved as of release 4.5(1).

In release 4.5, if you have enabled global DHCP options and turned on the “one-lease-per-client” global option (in the **Device Management > CCA Servers > Manage [CAS_IP] > Network > DHCP > Global Options** page, **Root Global Option List**), the DHCPD service on the CAS stops responding. (See also CSCsw22550, page 90.) As a result, administrators cannot edit any of the DHCP options through the web console and the CAS stops handing out DHCP addresses to client machines. (This issue applies to new installations of release 4.5 as well as upgrades to release 4.5.)

The only known way to reactivate the web console is by manually stopping the service on the CAS, which only lasts a brief period before the service locks up and renders the web console unusable again.

To address this issue, apply the **Patch-CSCsw22550.tar.gz** patch to the CAS:

Note Apply this patch to the CAS only.

Step 1 Go to the Cisco Security Software download site at http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml and download the **Patch-CSCsw22550.tar.gz** file to your local machine.

Step 2 Place the **Patch-CSCsw22550.tar.gz** file in the **/store** directory on the CAS.

Step 3 Navigate to **/store**: `cd /store`.

Step 4 Enter `tar zxvf Patch-CSCsw22550.tar.gz` to extract the patch files in the **Patch-CSCsw22550** directory.

Step 5 Navigate to **Patch-CSCsw22550**: `cd Patch-CSCsw22550`.

Step 6 Enter `./apply.sh` to patch the CAS dhcpd file.

Note Make sure following file permissions are correct on your system:

```
PERM        OWNER GROUP SIZE FILE_PATH
-rwxr-xr-x  root  root  6758 /perfigo/dhcp/dhcpd
```

Known Issues with Web Upgrade in Release 4.1(x) and Earlier

Prior to Release 4.5, Cisco NAC Appliance provided a web upgrade feature where the product upgrade file for a new release could be uploaded and executed on the CAM and CAS machines via the CAM or CAS web console.

Starting from Release 4.5, web upgrade is no longer supported and cannot be used to upgrade NAC appliances on 4.1(x) and 4.0(x) releases to Release 4.5. To upgrade your Cisco NAC Appliances from 4.1(x) or 4.0(x) releases, you must copy the upgrade file to each appliance and run the upgrade script via the command line, as described in Upgrading to Release 4.5, page 111.

In the case that administrators attempt web upgrade from the 4.1(x) or 4.0(x) web consoles, the following known issues will occur:

- When attempting to upgrade the CAS by uploading the upgrade file to the CAM's **Device Management > CCA Servers > Manage [CAS IP] > Misc > Update** page and clicking the **Apply** button, an HTTP 500 error occurs ("java.lang.OutofMemoryError") (CSCsr61106, page 73).
- When attempting to upload the upgrade file to the CAS via the CAS **Administration > Software Update** page, an error results ("Error: Failed to upload file Content Length Error (260551527 > 209715200)") and the file is not uploaded (CSCsu26775, page 106).
- Web upgrade of the CAM via the CAM's **Administration > CCA Manager > System Upgrade** may still function but is not supported for upgrade to Release 4.5.

Note that the two CAS web upload/upgrade errors cause no impact to the CAM database.

Starting from Release 4.5:

- Web console pages are renamed and only the upload file and log viewing functions on them are preserved, as described in CAM/CAS Software Upload Page Enhancements, page 15.
- CAS upgrade log files are preserved on the CAM's **Device Management > CCA Servers > Manage [CAS_IP] > Misc** web console page for upgraded systems only.
- For the file upload function, the file size limit is increased to 500 MB as described in CSCsu26775, page 106.
- Web-uploaded upgrade files are automatically placed in the /store directory of the CAM of the CAS (see Table 19).
- The release 4.5 upgrade script will not run in any directory not under /store.

Caution If upgrading from Release 4.1(6) or earlier, the upgrade file MUST be run only from the **/store** directory on the respective CAM or CAS machine.

Upgrade files that are uploaded to the CAM and CAS via web console are located in different directories, depending on the software release, as listed in Table 19.

Table 19 Web-Upload Directory Locations for CAM/CAS Upgrade Files

Cisco NAC Appliance Release	Web Upload Method	Web Console Upload Page	Resulting Directory Location
4.5 and later	CAM via CAM	**Administration > CCA Manager > Software Upload**	/store/
	CAS via CAS	**Administration > Software Upload**	/store/
4.1(6) and earlier	CAM via CAM	**Administration > CCA Manager > System Upgrade**	/perfigo/control/tomcat/normal-webapps/upload/patches/
	CAS via CAM	**Device Management > CCA Servers > Manage [CAS IP] > Misc > Update**	/perfigo/control/tomcat/normal-webapps/upload/ss_patches/
	CAS via CAS	**Administration > Software Update**	/store/upload/

Note For all releases, upgrade files that are uploaded to the CAM or CAS via web console have randomly-generated numeric code appended to the **.tar.gz** file (e.g. **cca_upgrade-<*version*>.tar<*numeric code*>.gz**).

Known Issues with www.perfigo.com Root CA

The Perfigo certificate authority, "EMAILADDRESS=info@perfigo.com, CN=www.perfigo.com, OU=Product, O="Perfigo, Inc.", L=San Francisco, ST=California, C=US" is used to generate temporary certificates and required for initial installation of CAM and CAS machines.

However, if the Perfigo CA remains on the CAM, it can render your Cisco NAC Appliance system vulnerable to security attacks. Before deploying your CAM and CAS(s) in a production environment, you must remove this certificate authority from the CAM and CAS databases. Cisco recommends searching for the string "www.perfigo.com" using the **Filter** options in the **Administration > CCA Manager > SSL > Trusted Certificate Authorities** CAM web console page and **Administration > SSL > Trusted Certificate Authorities** CAS web console page to quickly locate and remove this certificate authority from your CAM/CAS(s).

Before you can remove this CA from your CAM/CAS, you must obtain a third-party CA-signed SSL certificate and import it to your machines in order for the CAM/CAS components to work and to provide a trusted CA-signed certificate to end users.

Additionally, for any new CAM/CAS machines that you add to an existing production deployment, you will also need to remove the www.perfigo.com CA after initial installation and import a trusted CA-signed certificate.

For more information and detailed instructions on how to manage your SSL certificates when moving from a lab deployment to production-environment, see the "Manage CAM SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide* and the "Manage CAS SSL Certificates" section of the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide*.

Cisco is working to further resolve this issue in the future by addressing the fact that currently there is no CA certificate button available on the web (or user) login page. By design, the Cisco NAC Appliance administrator must configure user page content and specify whether or not to offer the Root CA along with its content (either the www.perfigo.com CA certificate or an imported third-party CA certificate—in release 4.5, the default option is still the www.perfigo.com CA) from a dropdown menu in the CAM web console pages. As the issue exists now, the administrator must change this behavior in the **Administration > User Pages > Login Page > Edit > Content** CAM web console page and deselect the **Root CA** table entry.

Known Issue with Active HA CAM Web Console Following Failover

For a brief period following a failover event, the administrator web console for the newly "active" CAM retains the limited menu/submenu options previously available while the machine was still the "standby" CAM.

To manually reproduce this scenario:

1. Configure the HA-CAM failover pair.
2. Issue the **`service perfigo stop`** CLI command on both HA-CAMs to stop services.
3. Issue the **`service perfigo start`** CLI command on the HA-Standby CAM to restart services.
4. As soon as the **`service perfigo start`** command finishes, access the HA-Service IP address in a browser for the administrator web console, enter authentication credentials, and click **Login**.
5. The CAM HA-Service IP administrator web console displays the limited menu/submenu options previously available while the machine was still the "standby" CAM.

To get the administrator web console to display properly, simply reload (Ctrl-refresh) the CAM HA-Service IP/hostname web page to display the full GUI for the now “active” CAM.

Known Issue with Upgrading CCA-3140 Appliance from Release 4.1(6) to 4.5

If you are planning to upgrade the CCA-3140 appliance, a workaround is needed if upgrading from release 4.1(6) to release 4.5. After an upgrade to Cisco NAC Appliance release 4.5, the NICs on the CCA-3140 hardware are no longer recognized. This occurs when an appliance that was originally installed with version 3.6.4.4 or earlier is upgraded to 4.1.6, and subsequently upgraded to 4.5.

Note This defect only applies to systems that have been upgraded to 4.1.6. Systems upgraded directly from 4.1.5 or earlier are not affected by this defect.

The following descriptions —CSCsv52402 Workaround and Further Problem Description—describe the workaround steps available to resolve this issue.

See CSCsv52402, page 87 for additional information.

CSCsv52402 Workaround

Step 1 To find out if your 4.1.6 system might be affected, type:

```
% rpm -qa | grep “tg3”
```

If it returns nothing, then your system will not be affected.

Step 2 If your system is affected, simply remove a file from /boot before you run the upgrade to avoid this defect (or remove the file and re-run the upgrade):

```
% rm /boot/2.6.11-perfigo-sp9
% cd /store/cca_upgrade-4.5.x
% ./UPGRADE.sh
```

Further Problem Description

If there is a bad network driver, a problem may be seen where the 'service perfigo stop' command fails prior to running the upgrade, displaying the following output:

```
...stopping CCA Server...
BaseAgent process stopped!
click: stopping router thread pid 2918
click module exiting
click error: 93 elements still allocated
click error: 457 outstanding news
Unable to handle kernel paging request at virtual address f8c4cc50
 printing eip:
f8c4cc50
*pde = 32298067
Oops: 0000 [#2]
```

To resolve this issue:

Step 1 Run the following commands:

```
% chkconfig --del perfigo
% reboot
```

Step 2 Then perform the workaround. The kernel panic will not occur, as the perfigo service will not be running.

Step 3 After the upgrade, but before the post-upgrade reboot, run:

```
% chkconfig --add perfigo
```

Step 4 The system should run normally.

Known Issue with NAC-3310 Based Appliances

When performing CD software installation, if a NAC-3310 based appliance does not read the software on the CD ROM drive, and instead attempts to boot from the hard disk, you will need to configure the appliance BIOS settings to boot from CD ROM before attempting to re-image or upgrade the appliance from CD. For detailed steps, refer to the "Configuring Boot Settings on NAC-3310 Based Appliances "section of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide* and *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide*.

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 Issues 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*.

Note This known issue does not affect Wireless Out-of-Band deployments because CASs are only deployed in Virtual Gateway mode, thus the CAS is not configured to perform any DHCP functions.

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 68.

Known Issues for Windows Vista and Agent Stub

Use “No UI” or “Reduced UI” Installation Option

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

“Interactive Services Dialog Detection” and Uninstall

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

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

Known Issues with MSI Agent Installer

MSI File Name

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

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

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

Minor Version Updates

You cannot upgrade minor version (4th digit) updates of the Clean Access Agent from the MSI package directly. You must uninstall the program from Add/Remove programs first before installing the new version. Refer to CSCsm20655, page 67 for details.

See also Troubleshooting, page 134 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 XP/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 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:

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."

Troubleshooting

This section provides troubleshooting information for the following topics:

- Vista/IE 7 Certificate Revocation List
- Windows Vista Agent Stub Installer Error
- 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
- Creating CAM/CAS Support Logs
- Recovering Root Password for CAM/CAS
- Troubleshooting CAM/CAS Certificate Issues
- Troubleshooting Switch Support Issues
- Other Troubleshooting Information

Note For additional troubleshooting information, see also New Installation of Release 4.5, page 110.

Vista/IE 7 Certificate Revocation List

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

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

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

To resolve the error, perform the following actions:

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

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

- **a.** Import the certificate to the client system's trusted root store.
- **b.** Disable the "Check for server certificate revocation (requires restart)" checkbox under IE's Tools > Internet Options > Advanced | Security settings.

Windows Vista Agent Stub Installer Error

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

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

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

To solve the problem:

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

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

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

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

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

Agent Stub Upgrade and Uninstall Error

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

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

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

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

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

Clean Access Agent AV/AS Rule Troubleshooting

When troubleshooting AV/AS Rules:

- View administrator reports for the Clean Access Agent from **Device Management > Clean Access > Clean Access Agent > Reports**
- 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 9).
2. Version of client OS (e.g. Windows XP SP2).
3. Version of Cisco Updates ruleset
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 137.
9. If necessary, provide CAM support logs as described in Creating CAM/CAS Support Logs, page 139.

Generating Windows Installer Log Files for Agent Stub

Users can compile the Windows Installer logs generated by the Install Shield 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 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

You can enable debug logging on the Clean Access Agent by adding a LogLevel registry value on the client with value “debug.” For Windows Agents (see Cisco NAC Appliance Agents, page 23), the event log is created in the directory **%APPDATA%\CiscoCAA**, where %APPDATA% is the Windows environment variable.

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

To view and/or change the Agent LogLevel setting:

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

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

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

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

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

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

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

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

Step 8 Re-login to the Clean Access Agent.

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

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

a. Open **Start > Run**.

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

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

Note

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

Generate Mac OS X Agent Debug Log

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

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

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

To view and/or change the Agent LogLevel:

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

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

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

Step 4 Choose **setting.plist**.

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

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

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

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

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

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

You must be the root user to edit the file.

Creating CAM DB Snapshot

See the instructions in Copy the Upgrade File to the CAS/CAM, page 117 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. Refer to "Support Logs" sections of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide* or *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide*.

Recovering Root Password for CAM/CAS

Refer to the "Recovering Root Password" section of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide* or *Password Recovery Procedure for the Cisco NAC Appliance (Cisco Clean Access)*.

Troubleshooting CAM/CAS Certificate Issues

Refer to the "Troubleshooting Certificate Issues" sections of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide* or *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide*.

Troubleshooting Switch Support Issues

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

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 20 Updates to Release Notes for Cisco NAC Appliance, Release 4.5

Date	Description
6/17/10	Added Caveat CSCsx52263 to Open Caveats - Release 4.5(1), page 60
7/9/09	Clean Access Agent Version 4.5.2.0: • Updated Release 4.5 Compatibility Matrix, page 6 • Updated Release 4.5 Clean Access Agent Upgrade Compatibility Matrix, page 8 • Added Version 4.5.2.0, page 23 to Windows Clean Access Agent, page 23 • Updated Clean Access Supported AV/AS Product Lists, page 26 • Added Resolved Caveats - Agent Version 4.5.2.0, page 94
3/5/09	Updated the description of Database Snapshot Upgrade Enhancement, page 16 under New Features and Enhancements in Release 4.5(0), page 11 to clarify enhancement function and intent
3/2/09	Moved CSCsd90433 from Open Caveats - Release 4.5(1), page 60 to Resolved Caveats - Release 4.5(1), page 81

Table 20 Updates to Release Notes for Cisco NAC Appliance, Release 4.5

Date	Description
2/25/09	Updates for Release 4.5(1) • Software Compatibility, page 6 (Updated) • Enhancements in Release 4.5(1), page 9 (New) • Cisco NAC Appliance Agents, page 23 (Updated) • Supported AV/AS Product List Version Summary (Windows), page 27 (New) • Clean Access AV Support Chart (Windows Vista/XP/2000), page 34 (New) • Clean Access AS Support Chart (Windows Vista/XP/2000), page 49 (New) • Open Caveats - Release 4.5(1), page 60 (Updated) • Resolved Caveats - Release 4.5(1), page 81 (New) • Resolved Caveats - Agent Version 4.5.1.0, page 95 (New) • Upgrading to Release 4.5, page 111 (Updated) • Changes for 4.5 Installation/Upgrade, page 111 (Updated) • Known Issue with Mass DHCP Address Deletion, page 124 (New) • Known Issue with NAC-3310 Based Appliances, page 131 (New) • Known Issue for Windows Vista and IP Refresh/Renew, page 132 (New)
1/13/09	Added information for CSCsv52402: • Added CSCsv52402 to open caveats • Added Known Issue with Upgrading CCA-3140 Appliance from Release 4.1(6) to 4.5, page 130 • Added notes to upgrade sections.
12/18/08	• Updated CSCsw16823 to reflect need for patch • Updated Known Issue for DHCP Address Assignments in Layer 2 and Layer 3 Following Upgrade to Release 4.5(0), page 125 with patch download and application instructions
12/11/08	• Added caveat CSCsw22550 to Open Caveats - Release 4.5(1), page 60 • Added warning regarding DHCP IP address assignments in Layer 2 and Layer 3 and another warning regarding DHCPD service failure when global DHCP options are enabled to Changes for 4.5 Installation/Upgrade, page 111 • Added Known Issue for DHCP Address Assignments in Layer 2 and Layer 3 Following Upgrade to Release 4.5(0), page 125 • Added Known Issue with DHCPD Service When Global DHCP Option is Enabled in Release 4.5(0), page 126 to address need to apply **Patch-CSCsw22550.tar.gz** patch to CAS
12/1/08	• Added caveat CSCsw16823 to Open Caveats - Release 4.5(1), page 60
11/17/08	• Added caveat CSCsv78301 to Open Caveats - Release 4.5(1), page 60 • Added warning regarding VPN SSO in Changes for 4.5 Installation/Upgrade, page 111 • Added Known Issue for VPN SSO Following Upgrade to Release 4.5, page 125
11/7/08	• Updated Software Compatibility, page 6 tables for 4.1(x) Agent compatibility.

Table 20 Updates to Release Notes for Cisco NAC Appliance, Release 4.5

Date	Description
11/5/08	• Minor update to file name specification in New Installation of Release 4.5, page 110
11/3/08	• Added Known Issue with Active HA CAM Web Console Following Failover, page 129 section to Known Issues for Cisco NAC Appliance
10/23/08	• Updated feature description in Certified Device List/Online User List Enhancements, page 19 • Minor updates to feature description in Out-of-Band Discovered Clients Cleanup, page 20
10/21/08	Release 4.5

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 Manger Installation and Configuration Guide, Release 4.5*
- *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.5*
- *Getting Started with Cisco NAC Network Modules in Cisco Access Routers*
- *Connecting Cisco Network Admission Control Network Modules*
- Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)
- Switch Support for Cisco NAC Appliance
- *Cisco NAC Appliance Service Contract / Licensing Support*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

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