# Release Notes for Cisco NAC Appliance (Cisco Clean Access), Version 4.1(2)

**Revised: April 11, 2008, OL-13883-01**

## Contents

These release notes provide late-breaking and release information for Cisco® NAC Appliance, formerly known as Cisco Clean Access (CCA), release 4.1(2). This document describes new features, changes to existing features, limitations and restrictions ("caveats"), upgrade instructions, and related information. These release notes supplement the Cisco NAC Appliance documentation included with the distribution. Read these release notes carefully and refer to the upgrade instructions prior to installing the software.

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

# Cisco NAC Appliance Releases

| Cisco NAC Appliance Version | Availability |
|---|---|
| 4.1.2.2 (Agent only) | October 8, 2007 |
| 4.1.2.1 ED | September 10, 2007 |
| 4.1(2) ED | July 26, 2007 |

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

# Cisco NAC Appliance Service Contract/Licensing Support

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

# System and Hardware Requirements

This section describes the following:

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

## System Requirements

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

- Clean Access Manager (CAM) system requirements
- Clean Access Server (CAS) system requirements
- Clean Access Agent (CAA) system requirements
- CAS High Availability Requirements

# Hardware Supported

This section describes the following:

- Cisco NAC Network Module
- NAC-3300 Series Appliances
- Important Installation Information for NAC-3310
- Cisco NAC Appliance Integration with Cisco NAC Profiler
- Additional Hardware Support Information

## Cisco NAC Network Module

⚠ **Caution** **Release 4.1.2.1 is the minimum mandatory version for all appliances**, and is required to support HA-CAS pairs. Refer to CSCsk24551, page 46 for additional details. For compatibility with CAM/CAS appliances running 4.1.2.1, you must use the standard product upgrade file to upgrade the NAC network module to 4.1.2.1. Refer to Enhancements in Release 4.1.2.1, page 11 for further details.

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

For details on NAC network module support in Release 4.1(2), refer to Enhancements in Release 4.1(2), page 12.

For hardware installation instructions (how to install the NAC network module in an Integrated Service Router) refer to *Installing Cisco Network Modules in Cisco Access Routers*.

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

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

While upgrading to release 4.1.2.1 is not required to support Cisco NAC network modules, if you are supporting 64-bit Windows Vista or Windows XP client systems, you must upgrade your CAM, CAS, NAC network module, and Agent components from 4.1(2) to 4.1.2.1.

## NAC-3300 Series Appliances

⚠ **Caution** **Release 4.1.2.1 is the minimum mandatory version for all appliances**, and is required to support HA-CAS pairs. Refer to CSCsk24551, page 46 for additional details. For compatibility with CAM/CAS appliances running 4.1.2.1, you must use the standard product upgrade file to upgrade the NAC network module to 4.1.2.1. Refer to Enhancements in Release 4.1.2.1, page 11 for further details.

Release 4.1(2) and later support Cisco NAC Appliance 3300 Series platforms.

Customers have the option to upgrade NAC-3310, NAC-3350, or NAC-3390 MANAGER and SERVER appliances to release 4.1(2) and later using a single upgrade file, **cca_upgrade-4.1.2.x.tar.gz**.

CD installation of release 4.1(2) and later is also supported:

- For NAC-3310 and NAC-3350, the **cca-4.1_2_1-K9.iso** file is required for new CD installation of the Clean Access Server or Clean Access Manager.

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

- For NAC-3390, a separate ISO file, **supercam-cca-4.1_2_1-K9.iso**, is required for CD installation of the Clean Access Super Manager.

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

## Important Installation Information for NAC-3310

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

### NAC-3310 Required BIOS/Firmware Upgrade

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

### NAC-3310 Required DL140 or serial_DL140 CD Installation Directive

The NAC-3310 appliance (MANAGER and SERVER) requires you to enter the **DL140** or **serial_DL140** installation directive at the "boot:" prompt when you install new system software from a CD-ROM. For more information, refer ro Known Issue with NAC-3310 CD Installation, page 52.

## Cisco NAC Appliance Integration with Cisco NAC Profiler

You can integrate your Cisco NAC Appliance system with the Cisco NAC Profiler solution. Cisco NAC Profiler performs endpoint profiling and behavior monitoring. It enables you to automatically discover, categorize, and monitor hundreds or thousands of endpoints for which user authentication and/or posture assessment does not apply.

The Cisco NAC Profiler solution consists of two primary components:

- **Cisco NAC Profiler Server**—The Cisco NAC Profiler Server appliance manages the Cisco NAC Profiler Collector component enabled on each Clean Access Server. The Profiler Server populates entries on the CAM's global device filter list (**Device Management > Filters > Devices > List**) for the endpoints it profiles and monitors. Clicking the Description link for a Profiler entry brings up the Profiler Server's Endpoint Summary data directly inside the CAM web console. The Cisco NAC Profiler Server is configured and managed via its own web console interface, as described in the *Cisco NAC Profiler Installation and Configuration Guide*.

- **Cisco NAC Profiler Collector**—The Cisco NAC Profiler Collector is a service that can be enabled on a NAC-3310 or NAC-3350 Clean Access Server running Release 4.1(2) or later. You must purchase a Cisco NAC Profiler Server appliance and obtain and install Cisco NAC Profiler/Collector licenses on the Profiler Server to deploy the Cisco NAC Profiler solution. See the "CLI Commands for Cisco NAC Profiler" section of the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(2)* for details.

For additional information on Cisco NAC Profiler refer to the following documents:

- *Cisco NAC Profiler Data Sheet*
- *Cisco NAC Profiler Ordering Guide*
- *Cisco NAC Appliance Service Contract / Licensing Support*
- *Release Notes for Cisco NAC Profiler* (refer to applicable version)
- *Cisco NAC Profiler Installation and Configuration Guide*

### Additional Hardware Support Information

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

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

See Troubleshooting, page 82 for further details.

## Supported Switches for Cisco NAC Appliance

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

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

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

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

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

| Cisco NAC Appliance Version | VPN Concentrator/Wireless Controller | VPN Clients |
|---|---|---|
| 4.1.2.1 | 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 7.2(0)81 or later | • Cisco SSL VPN Client (Full Tunnel)<br>• Cisco VPN Client (IPSec) |
| | Cisco WebVPN Service Modules for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers | |
| | Cisco VPN 3000 Series Concentrators, Release 4.7 | |
| | Cisco PIX Firewall | |

[1] For additional details, see also Known Issue with Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs), page 53.

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

For further details, see the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(2)* and the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(2)*.

# Software Compatibility

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

- Software Compatibility Matrixes
- Determining the Software Version

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

- Clean Access Supported AV/AS Product List, page 16
- Clean Access Agent Version Summary, page 38

## Software Compatibility Matrixes

This section describes the following:

- Release 4.1(2) CAM/CAS-Agent Compatibility
- Release 4.1(2) Agent-CAM/CAS Compatibility

- Release 4.1(2) CAM/CAS Upgrade Compatibility Matrix

## Release 4.1(2) CAM/CAS-Agent Compatibility

Table 2 shows Clean Access Manager and Clean Access Server compatibility and the Agent versions supported with each CCA 4.1(2) release. CAM/CAS/Agent versions displayed in the same row are compatible; however, older Agents will not support additional features/functionality introduced with new versions of the Agent. Cisco recommends that you synchronize your software images to the latest shown as compatible in the table.

*Table 2 Release 4.1(2) CAM/CAS-Agent Compatibility Matrix* [1]

| Clean Access Manager | Clean Access Server | Windows Clean Access Agent [2,3] | Mac OS Clean Access Agent [3] |
|---|---|---|---|
| 4.1.2.1 [4, 5] | 4.1.2.1 [4,5] | 4.1.2.2 [5,6]<br>4.1.2.1 [5, 6]<br>4.1.2.0 [6]<br>4.1.1.0 [7]<br>4.1.0.x [7,8] | 4.1.2.0 [9]<br>4.1.1.0<br>4.1.0.0 |
| 4.1(2) [4] | 4.1(2) [4] | | |

1. 4.1.2+ CAM/CAS are compatible with 4.1.x.x Agents, and 4.1.x CAM/CAS are compatible with 4.1.2.x Agents, except where noted. See Clean Access Agent Version Summary, page 38 for details and caveats resolved for each 4.1.2.x Agent version.
2. For checks/rules/requirements, the Agent can detect "N" (European) versions of the Windows Vista operating system, but the CAM/CAS treat "N" versions of Vista as their US counterpart.
3. Agent versions are not supported across major releases. Do not use 4.1.x.x Agents with 4.0(x) or prior releases. However, auto-upgrade is supported from any 3.5.1 and later Agent directly to the latest 4.1.2.x Agent. See Clean Access Agent Version Summary, page 38 for further details.
4. **Release 4.1.2.1 is the minimum mandatory version for all appliances**, and is required to support HA-CAS pairs. Refer to CSCsk24551, page 46 for additional details. For compatibility with CAM/CAS appliances running 4.1.2.1, you must use the standard product upgrade file to upgrade the NAC network module to 4.1.2.1. See Enhancements in Release 4.1.2.1, page 11 for details.
5. The 4.1.2.1 and later Agents perform authentication only for 64-bit Windows Vista and Windows XP client operating systems. Once the user is authenticated, the Agent does not perform posture assessment or remediation. CAM/CAS/Agent must all run release 4.1.2.1 to support 64-bit Windows OS. Because Cisco NAC Appliance provides authentication-only support for 64-bit operating system Agents, nessus scanning via the Clean Access Agent does not perform remediation on the client machine.
6. 4.1.2.0, 4.1.2.1, and 4.1.2.2 Agent Stub installers are not supported on Windows Vista.
7. Cisco strongly recommends running the latest 4.1.2.x Clean Access Agent with the latest 4.1(2)+ CAM/CAS release. By default, 4.1.0.x Agents are not allowed to log into a 4.1(2) CCA system. However, administrators can optionally configure the 4.1(2)+ CAM/CAS to allow 4.1.0.x Agent authentication and posture assessment, if necessary. Agents upgraded to 4.1.2.0 and later can still log into a 4.1(1) or 4.1(0) CAM/CAS. See *4.1.0.x Agent Support on Release 4.1(1)* in the 4.1(1) release notes for details.
8. 4.1.0.0/4.1.0.2 Agents do not support Windows Vista. Windows Vista support starts from Agent version 4.1.1.0 and later.
9. Releases 4.1(1) and 4.1(2)+ do not support auto-upgrade for the Mac OS Agent. Users can upgrade client machines to the latest Mac OS Agent by downloading the Agent via web login and running the Agent installation.

**Note** Refer to the "Cisco NAC Appliance Agents System Requirements" section of *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* for additional compatibility details across versions of the Agent.

## Release 4.1(2) Agent-CAM/CAS Compatibility

Table 3 shows Clean Access Agent compatibility with 4.1.x versions of the Clean Access Manager and Clean Access Server. Agent/CAM/CAS versions displayed in the same row are compatible; however, newer Agent features/functionality may not be available with older CAM/CAS releases. Cisco recommends that you synchronize your software images to the latest shown as compatible in the table.

*Table 3 Release 4.1(2) Agent-CAM/CAS Compatibility Matrix* [1],

| Windows Clean Access Agent [2,3] | Mac OS Clean Access Agent [3] | Clean Access Manager | Clean Access Server |
|---|---|---|---|
| 4.1.2.2 [4]<br>4.1.2.1 [4]<br>4.1.2.0 | 4.1.2.0 [5] | 4.1.2.1 [4] | 4.1.2.1 [4] |
| | | 4.1(2) | 4.1(2) |
| | | 4.1(1) | 4.1(1) |
| | | 4.1.0.2 | 4.1.0.2 |
| | | 4.1.0.1<br>4.1(0) | 4.1(0) |

[1] 4.1.2+ CAM/CAS are compatible with 4.1.x.x Agents, and 4.1.x CAM/CAS are compatible with 4.1.2.x Agents, except where noted. See Clean Access Agent Version Summary, page 38 for details and caveats resolved for each 4.1.2.x Agent version.

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

[3] Agent versions are not supported across major releases. Do not use 4.1.x.x Agents with 4.0(x) or prior releases. However, auto-upgrade is supported from any 3.5.1 and later Agent directly to the latest 4.1.2.x Agent. See Clean Access Agent Version Summary, page 38 for further details.

[4] The 4.1.2.1 and later Agents perform authentication only for 64-bit Windows Vista and Windows XP client operating systems. Once the user is authenticated, the Agent does not perform posture assessment or remediation. CAM/CAS/Agent must all run release 4.1.2.1 or later to support 64-bit Windows OS. Because Cisco NAC Appliance provides authentication-only support for 64-bit operating system Agents, nessus scanning via the Clean Access Agent does not perform remediation on the client machine.

[5] Releases 4.1(1) and 4.1(2)+ do not support auto-upgrade for the Mac OS Agent. Users can upgrade client machines to the latest Mac OS Agent by downloading the Agent via web login and running the Agent installation.

## Release 4.1(2) CAM/CAS Upgrade Compatibility Matrix

Table 4 shows 4.1(2) 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. Refer to Upgrading to 4.1.2.1, page 56 for detailed instructions.

.

*Table 4 Release 4.1(2) CAM/CAS Upgrade Compatibility Matrix*

| Clean Access Manager | | Clean Access Server | |
|---|---|---|---|
| **Upgrade From:** | **To:** | **Upgrade From:** | **To:** |
| 4.1(2)<br>4.1(1)<br>4.1(0)+ [1]<br>4.0(x)<br>3.6(x)<br>3.5(7)+ [2] | 4.1.2.1 [3] | 4.1(2)<br>4.1(1)<br>4.1(0)+ [1]<br>4.0(x)<br>3.6(x)<br>3.5(7)+ [2] | 4.1.2.1 [3] |

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

2. To upgrade from 3.5(7) and later, you must use the In-Place Upgrade from 3.5(7)+ to 4.1.2.1—Standalone Machines, page 59 or In-Place Upgrade from 3.5(7)+ to 4.1.2.1—HA-Pairs, page 63 procedures, as appropriate.
3. **Release 4.1.2.1 is the minimum mandatory version for all appliances**, and is required to support HA-CAS pairs. Refer to CSCsk24551, page 46 for additional details. For compatibility with CAM/CAS appliances running 4.1.2.1, you must use the standard product upgrade file to upgrade the NAC network module to 4.1.2.1. See Enhancements in Release 4.1.2.1, page 11 for details.

# Determining the Software Version

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

- Clean Access Manager (CAM) Version, page 9
- Clean Access Server (CAS) Version, page 9
- Clean Access Agent Versioning, page 10
- Cisco Clean Access Updates Versioning, page 10

## Clean Access Manager (CAM) Version

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

The software version is also displayed as follows:

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

### CAM Lite, Standard, Super

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

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

Note the following:

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

## Clean Access Server (CAS) Version

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

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

**Note** If configuring High Availability CAM or CAS pairs, see also Access Web Consoles for High Availability, page 78 for additional information.

## Clean Access Agent Versioning

On the CAM web console, you can determine Clean Access Agent versioning from the following pages:

- **Monitoring > Summary** (Setup and Patch Version)
- **Device Management > Clean Access > Clean Access Agent > Distribution** (Setup and Patch Version)
- **Device Management > Clean Access > Clean Access Agent > Updates** (Patch Version; see also Cisco Clean Access Updates Versioning, page 10)
- **Device Management > Clean Access > Clean Access Agent > Reports | View** (individual report shows username, OS, Agent version, client AV/AS version)

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

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

## Cisco Clean Access Updates Versioning

To view the latest version of Updates downloaded to your CAM, including Cisco Checks & Rules, CCA Agent Upgrade Patch, Supported AV/AS Product List, go to **Device Management > Clean Access > Clean Access Agent > Updates** on the CAM web console. See Clean Access Supported AV/AS Product List, page 16 for additional details.

# New and Changed Information

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

- Enhancements in Release 4.1.2.1, page 11
- Enhancements in Release 4.1(2), page 12

For additional details, see also:

- Hardware Supported, page 3
- Clean Access Supported AV/AS Product List, page 16
- Clean Access Agent Version Summary, page 38
- Caveats, page 41
- Known Issues for Cisco NAC Appliance, page 52

## Enhancements in Release 4.1.2.1

**Caution** **Release 4.1.2.1 is the minimum mandatory version for all appliances**, and is required to support HA-CAS pairs. Refer to CSCsk24551, page 46 for additional details. For compatibility with CAM/CAS appliances running 4.1.2.1, you must use the standard product upgrade file to upgrade the NAC network module to 4.1.2.1.

Release 4.1.2.1 is a general and important bug fix release for the Clean Access Manager, Clean Access Server, and Clean Access Agent that addresses the caveats described in Resolved Caveats - Release 4.1.2.1, page 45 and provides the enhancements listed below. No new features are added.

- Clean Access Agent (4.1.2.2)
- Clean Access Agent (4.1.2.1)
- Supported AV/AS Product List Enhancements

Release 4.1.2.1 is provided as both an upgrade.tar.gz file and ISO file for new CD installations.

For upgrade instructions refer to Upgrading to 4.1.2.1, page 56.

### Clean Access Agent (4.1.2.2)

Release 4.1.2.2 is a bug fix release for the Clean Access Agent that addresses the caveats described in Resolved Caveats - Agent Version 4.1.2.2, page 45 and provides additional AV/AS product support as detailed in Supported AV/AS Product List Enhancements, page 12 and Clean Access Agent Version Summary, page 38.

**Note** The 4.1.2.2 Agent performs authentication only for 64-bit Windows Vista and Windows XP client operating systems. Once the user is authenticated, the Agent does not perform posture assessment or remediation. To support 64-bit operating system Agents, the CAM and CAS must also be running release 4.1.2.1. Because Cisco NAC Appliance provides authentication-only support for 64-bit operating system Agents, nessus scanning via the Clean Access Agent does not perform remediation on the client machine.

## Clean Access Agent (4.1.2.1)

Release 4.1.2.1 introduces a Clean Access Agent that performs authentication on 64-bit Windows Vista and Windows XP client operating systems and provides additional AV/AS product support as detailed in Supported AV/AS Product List Enhancements, page 12 and Clean Access Agent Version Summary, page 38.

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

## Supported AV/AS Product List Enhancements

- Version 66 of the Supported AV/AS Product List and 4.1.2.2 Agent add AV/AS product support as described in Clean Access Supported AV/AS Product List, page 16.
- Version 64 of the Supported AV/AS Product List and 4.1.2.1 Agent added AV/AS product support as listed in Supported AV/AS Product List Version Summary, page 34.
- See Clean Access Supported AV/AS Product List, page 16 for the latest AV/AS product charts.

# Enhancements in Release 4.1(2)

This section details the enhancements delivered with Cisco NAC Appliance release 4.1(2) for the Clean Access Manager and Clean Access Server.

### General Enhancements

- Cisco NAC Appliance Integration with Cisco NAC Profiler/Collector Solution
- New Cisco NAC Network Module (NME-NAC-K9) Support
- NAC Appliance Platform Type Display
- Debug Log Download Enhancement
- Active VPN Client Status Page Enhancement
- WSUS Requirement Configuration Display Enhancement
- New “service perfigo platform” CLI Command
- Web Login Support Using Safari Browser for Mac OS
- Supported AV/AS Product List Enhancements (Version 61)

# General Enhancements

## Cisco NAC Appliance Integration with Cisco NAC Profiler/Collector Solution

With Release 4.1(2), you can integrate the Cisco NAC Appliance system with the Cisco NAC Profiler solution. The Cisco NAC Profiler system enables you to automatically discover, categorize, and monitor hundreds or thousands of endpoints for which user authentication and/or posture assessment does not apply. For component descriptions and hardware support information, see Cisco NAC Appliance Integration with Cisco NAC Profiler, page 4.

## New Cisco NAC Network Module (NME-NAC-K9) Support

Release 4.1(2) introduces support for the Cisco NAC Appliance network module (NME-NAC-K9) on the next generation service module for the Cisco 2811, 2821, 2851, 3825, and 3845 Integrated Services Routers (ISRs).

The Cisco NAC Network Module for Integrated Services Routers supports the same software features as the Clean Access Server (CAS) on a NAC Appliance, with the exception of high availability. NME-NAC-K9 does not support failover from one module to another. The integration of CAS capabilities into a network module for ISRs allows network administrators to manage a single device in the branch office for data, voice, and security requirements. The NME-NAC-K9 network module is available as a single hardware module with 50-user and 100-user license options, and supports a maximum of 100 online, concurrent users.

Once initially installed, the Cisco NAC network module is managed in the CAM web console like any other Clean Access Server, and a single CAM can manage both CAS appliances and NAC network modules. To add the Cisco NAC network module to your network, at least one Clean Access Manager appliance (Lite, Standard or Super) must be already installed and configured.

Cisco ISR platforms need to run Cisco ISO software Release 12.4(11)T or later (IP Base image or above) in order to support the Cisco NAC network module.

If introducing the Cisco NME-NAC-K9 network module to an existing Cisco NAC Appliance network, you must upgrade all CAM/CAS appliances to release 4.1(2) or later for compatibility.

**Note** The Cisco NAC Network Module (NME-NAC-K9) is supported starting from Cisco NAC Appliance Release 4.1(2) and later only.

**Caution** **Release 4.1.2.1 is the minimum mandatory version for all appliances**, and is required to support HA-CAS pairs. Refer to CSCsk24551, page 46 for additional details. For compatibility with CAM/CAS appliances running 4.1.2.1, you must use the standard product upgrade file to upgrade the NAC network module to 4.1.2.1.

For hardware installation instruction (how to install the NAC network module in an Integrated Service Router) refer to *Installing Cisco Network Modules in Cisco Access Routers*.

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

## NAC Appliance Platform Type Display

To support the new Cisco NAC network module, release 4.1(2) features a new **Platform** field in the top-level **IP** settings screens for both the CAM and CAS that tells the administrator whether the CAS is a standard Clean Access Server appliance or a new Cisco NAC network module installed in a Cisco ISR router chassis.

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

- **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP** | new **Platform** field featuring either "APPLIANCE" or "NME-NAC"

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

- **Administration > Network Settings > IP** | new **Platform** field featuring either "APPLIANCE" or "NME-NAC"

You can also use the CAS CLI to view the platform type. See New "service perfigo platform" CLI Command, page 15 for details.

## Debug Log Download Enhancement

Beginning with release 4.1(2), you can now specify the number of days of collected debug logs to download in order to aid troubleshooting efforts when working with Cisco technical support. Previously, debug logs compiled to download to technical support included all recorded log entries in the CAM/CAS database. The default setting is one week (7 days).

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

- **Administration > Clean Access Manager > Support Logs** | new field allowing you to specify the number of days for debug log download to technical support

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

- **Monitoring > Support Logs** | new field allowing you to specify the number of days for debug log download to technical support

## Active VPN Client Status Page Enhancement

Beginning with release 4.1(2), the **Active Clients** page in the CAM web console displays the time a client logged in to the network along with the client IP address, client name, and access server IP address.

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

- **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > VPN Auth > Active Clients** | new "Login Time" column

## WSUS Requirement Configuration Display Enhancement

New Help text has been added to the Windows Server Update Service Requirement configuration page describing the configuration dependencies related to the **Severity** setting.

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

- **Device Management > Clean Access > Clean Access Agent > Requirement > New Requirement** | **Windows Server Update Service** requirement type

## New "service perfigo platform" CLI Command

The CAS CLI includes the new **`service perfigo platform`** command in release 4.1(2). The command allows you to determine whether the CAS is a standard Clean Access Server appliance or a new Cisco NME-NAC-K9 network module installed in a Cisco ISR router chassis. The command output includes either "APPLIANCE" or "NME-NAC" as the platform setting.

You can also use the web console to view the platform type. See NAC Appliance Platform Type Display, page 14 for details.

## Web Login Support Using Safari Browser for Mac OS

Beginning with release 4.1(2), users running Mac OS X on client machines can connect to the NAC Appliance via web login from a Safari web browser. To support this enhancement, Mac users must be running Safari browser version 2.0.4 or later.

## Supported AV/AS Product List Enhancements (Version 61)

- See Clean Access Supported AV/AS Product List, page 16 for the latest AV/AS product charts.
- See Supported AV/AS Product List Version Summary, page 34 for details on each update to the list.

# Clean Access Supported AV/AS Product List

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

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

**Note** Cisco recommends keeping your Supported AV/AS Product List up-to-date on your CAM by configuring the **Update Settings** under **Device Management > Clean Access > Clean Access Agent > Updates** to "Automatically check for updates every 1 hour."

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

- Clean Access AV Support Chart (Windows Vista/XP/2000), page 17
- Clean Access AV Support Chart (Windows ME/98), page 27
- Clean Access AS Support Chart (Windows Vista/XP/2000), page 29

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

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

- Supported AV/AS Product List Version Summary, page 34
- Clean Access Agent Version Summary, page 38

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

**Note** Where possible, Cisco recommends using AV Rules mapped to AV Definition Update Requirements when checking antivirus software on clients, and AS Rules mapped to AS Definition Update Requirements when checking anti-spyware software on clients. In the case of non-supported AV or AS products, or if an AV/AS product/version is not available through AV Rules/AS Rules, administrators always have the option of creating their own custom checks, rules, and requirements for the AV/AS vendor (and/or using Cisco provided pc_ checks and pr_rules) through **Device Management > Clean Access > Clean Access Agent** (use New Check, New Rule, and New File/Link/Local Check Requirement). See the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(2)* for configuration details.

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

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

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

*Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 1 of 10)*

| Product Name | Product Version | AV Checks Supported (Minimum Agent Version Needed)[1] | | Live Update [2, 3] |
|---|---|---|---|---|
| | | Installation | Virus Definition | |
| **AEC, spol. s r.o.** | | | | |
| TrustPort Antivirus | 2.x | yes (4.0.6.0) | - | yes |
| **AhnLab, Inc.** | | | | |
| AhnLab Security Pack | 2.x | yes (3.5.10.1) | yes (3.5.10.1) | yes |
| AhnLab V3 Internet Security 2007 Platinum | 7.x | yes (3.6.5.0) | yes (3.6.5.0) | yes |
| AhnLab V3 Internet Security 7.0 Platinum Enterprise | 7.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| V3Pro 2004 | 6.x | yes (3.5.10.1) | yes (3.5.12) | yes |
| V3 VirusBlock 2005 | 6.x | yes (4.1.2.0) | yes (4.1.2.0) | - |
| **ALWIL Software** | | | | |
| avast! Antivirus | 4.x | yes (3.5.10.1) | yes (3.5.10.1) | yes |
| avast! Antivirus (managed) | 4.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| avast! Antivirus Professional | 4.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| **America Online, Inc.** | | | | |
| Active Virus Shield | 6.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| AOL Safety and Security Center Virus Protection | 102.x | yes (4.0.4.0) | yes (4.0.4.0) | - |
| AOL Safety and Security Center Virus Protection | 1.x | yes (3.5.11.1) | yes (3.5.11.1) | - |
| AOL Safety and Security Center Virus Protection | 210.x | yes (4.0.4.0) | yes (4.0.4.0) | - |
| AOL Safety and Security Center Virus Protection | 2.x | yes (4.1.0.0) | yes (4.1.0.0) | - |
| **Authentium, Inc.** | | | | |
| Command Anti-Virus Enterprise | 4.x | yes (3.5.0) | yes (3.5.0) | yes |
| Command AntiVirus for Windows | 4.x | yes (3.5.0) | yes (3.5.0) | yes |
| Command AntiVirus for Windows Enterprise | 4.x | yes (3.5.2) | yes (3.5.2) | yes |
| Cox High Speed Internet Security Suite | 3.x | yes (4.0.4.0) | yes (4.0.4.0) | yes |

*Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 2 of 10)*

| Product Name | Product Version | AV Checks Supported (Minimum Agent Version Needed)[1] | | Live Update [2, 3] |
|---|---|---|---|---|
| | | Installation | Virus Definition | |
| **Avira GmbH** | | | | |
| Avira AntiVir Windows Workstation | 7.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Avira Premium Security Suite | 7.x | yes (3.6.5.0) | yes (3.6.5.0) | yes |
| **Beijing Rising Technology Corp. Ltd.** | | | | |
| Rising Antivirus Software AV | 17.x | yes (3.5.11.1) | yes (3.5.11.1) | yes |
| Rising Antivirus Software AV | 18.x | yes (3.5.11.1) | yes (3.5.11.1) | yes |
| Rising Antivirus Software AV | 19.x | yes (4.0.5.0) | yes (4.0.5.0) | yes |
| **BellSouth** | | | | |
| BellSouth Internet Security Anti-Virus | 5.x | yes (4.0.5.1) | yes (4.0.5.1) | - |
| **BullGuard Ltd.** | | | | |
| BullGuard 7.0 | 7.x | yes (4.1.2.0) | yes (4.1.2.0) | - |
| **Check Point, Inc** | | | | |
| ZoneAlarm Anti-virus | 7.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| ZoneAlarm (AntiVirus) | 7.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| ZoneAlarm Security Suite Antivirus | 7.x | yes (4.0.5.0) | yes (4.0.5.0) | yes |
| **ClamAV** | | | | |
| ClamAV | devel-x | yes (4.0.6.0) | yes (4.0.6.0) | yes |
| **ClamWin** | | | | |
| ClamWin Antivirus | 0.x | yes (3.5.2) | yes (3.5.2) | yes |
| ClamWin Free Antivirus | 0.x | yes (3.5.4) | yes (3.5.4) | yes |
| **Computer Associates International, Inc.** | | | | |
| CA Anti-Virus | 8.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| CA 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 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 |

*Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 3 of 10)*

| Product Name | Product Version | AV Checks Supported (Minimum Agent Version Needed)[1] | | Live Update [2, 3] |
|---|---|---|---|---|
| | | Installation | Virus Definition | |
| **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) | - |
| **eEye Digital Security** | | | | |
| eEye Digital Security Blink Personal | 3.x | yes (4.0.6.0) | yes (4.0.6.0) | yes |
| eEye Digital Security Blink Professional | 3.x | yes (4.0.6.0) | yes (4.0.6.0) | - |
| **Eset Software** | | | | |
| NOD32 antivirus system | 2.x | yes (3.5.5) | yes (3.5.5) | yes |
| **Fortinet Inc.** | | | | |
| FortiClient Consumer Edition | 3.x | yes (4.0.6.0) | yes (4.0.6.0) | yes |
| **Frisk Software International** | | | | |
| F-PROT Antivirus for Windows | 6.0.x | yes (4.0.5.1) | yes (4.0.5.1) | - |
| F-Prot for Windows | 3.14e | yes (3.5.0) | yes (3.5.0) | yes |
| F-Prot for Windows | 3.15 | yes (3.5.0) | yes (3.5.0) | yes |
| F-Prot for Windows | 3.16c | yes (3.5.11) | yes (3.5.11) | yes |
| F-Prot for Windows | 3.16d | yes (3.5.11) | yes (3.5.11) | yes |
| F-Prot for Windows | 3.16x | yes (3.5.11.1) | yes (3.5.11.1) | yes |
| **F-Secure Corp.** | | | | |
| F-Secure Anti-Virus | 5.x | yes (3.5.0) | yes (3.5.0) | yes |
| F-Secure Anti-Virus | 6.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| F-Secure Anti-Virus | 7.x | yes (4.0.4.0) | yes (4.0.4.0) | - |
| F-Secure Anti-Virus 2005 | 5.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| F-Secure Anti-Virus Client Security | 6.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| F-Secure 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 2006 Beta | 6.x | yes (3.5.8) | yes (3.5.8) | yes |
| **GData Software AG** | | | | |
| AntiVirusKit 2006 | 2006.x | yes (4.1.0.0) | yes (4.1.0.0) | - |
| **Grisoft, Inc.** | | | | |
| Antivirussystem AVG 6.0 | 6.x | yes (3.5.0) | yes (3.5.0) | - |
| AVG 6.0 Anti-Virus - FREE Edition | 6.x | yes (3.5.0) | yes (3.5.0) | - |
| AVG 6.0 Anti-Virus System | 6.x | yes (3.5.0) | yes (3.5.0) | - |

*Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 4 of 10)*

| Product Name | Product Version | AV Checks Supported (Minimum Agent Version Needed)[1] | | Live Update [2, 3] |
|---|---|---|---|---|
| | | Installation | Virus Definition | |
| AVG 7.5 | 7.x | yes (4.0.4.0) | yes (4.0.4.0) | yes |
| AVG Antivirensystem 7.0 | 7.x | yes (3.5.0) | yes (3.5.0) | yes |
| AVG Anti-Virus 7.0 | 7.x | yes (3.5.0) | yes (3.5.0) | yes |
| AVG Anti-Virus 7.1 | 7.1.x | yes (3.6.3.0) | yes (3.6.3.0) | yes |
| AVG Free Edition | 7.x | yes (3.5.0) | yes (3.5.0) | yes |
| **HAURI, Inc.** | | | | |
| ViRobot Desktop | 5.0.x | yes (4.0.5.1) | yes (4.0.5.1) | - |
| **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 |
| Avira AntiVir PersonalEdition Premium | 7.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| **IKARUS Software GmbH** | | | | |
| IKARUS Guard NT | 2.x | yes (4.0.6.0) | yes (4.0.6.0) | - |
| IKARUS virus utilities | 5.x | yes (4.0.6.0) | yes (4.0.6.0) | - |
| **Internet Security Systems, Inc.** | | | | |
| Proventia Desktop | 8.x | yes (4.0.6.0) | - | - |
| Proventia Desktop | 9.x | yes (4.0.6.0) | yes (4.0.6.0) | - |
| **Kaspersky Labs** | | | | |
| Kaspersky Anti-Virus 2006 Beta | 6.0.x | yes (3.5.8) | yes (3.5.8) | - |
| Kaspersky Anti-Virus 6.0 | 6.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Kaspersky Anti-Virus 6.0 Beta | 6.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Kaspersky Anti-Virus for Windows File Servers | 5.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| Kaspersky Anti-Virus for Windows Workstations | 5.0.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| Kaspersky Anti-Virus for Windows Workstations | 6.x | yes (4.0.6.0) | yes (4.0.6.0) | yes |
| Kaspersky Anti-Virus for Workstation | 5.0.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| Kaspersky Anti-Virus Personal | 4.5.x | yes (3.5.0) | yes (3.5.0) | yes |
| Kaspersky Anti-Virus Personal | 5.0.x | yes (3.5.0) | yes (3.5.0) | yes |
| Kaspersky Anti-Virus Personal Pro | 5.0.x | yes (3.5.11) | yes (3.5.11) | yes |
| Kaspersky Internet Security | 6.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Kaspersky(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.** | | | | |

*Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 5 of 10)*

| Product Name | Product Version | AV Checks Supported (Minimum Agent Version Needed)[1] | | Live Update [2, 3] |
|---|---|---|---|---|
| | | Installation | Virus Definition | |
| Kingsoft AntiVirus 2004 | 2004.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Kingsoft Internet Security | 7.x | yes (3.6.5.0) | yes (3.6.5.0) | yes |
| Kingsoft Internet Security 2006 + | 2006.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| **McAfee, Inc.** | | | | |
| McAfee 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 | 4.5.x | yes (3.5.0) | yes (3.5.0) | yes |
| McAfee VirusScan | 8.x | yes (3.5.1) | yes (3.5.1) | yes |
| McAfee VirusScan | 8xxx | yes (3.5.0) | yes (3.5.0) | yes |
| McAfee VirusScan | 9.x | yes (3.5.1) | yes (3.5.1) | yes |
| McAfee VirusScan | 9xxx | yes (3.5.0) | yes (3.5.0) | yes |
| McAfee VirusScan Enterprise | 7.0.x | yes (3.5.0) | yes (3.5.0) | yes |
| McAfee VirusScan Enterprise | 7.1.x | yes (3.5.0) | yes (3.5.0) | yes |
| McAfee VirusScan Enterprise | 7.5.x | yes (3.5.0) | yes (3.5.0) | yes |
| McAfee VirusScan Enterprise | 8.0.x | yes (3.5.0) | yes (3.5.0) | yes |
| McAfee VirusScan Enterprise | 8.x | yes (3.6.5.0) | yes (3.6.5.0) | yes |
| McAfee VirusScan Home Edition | 7.x | yes (4.0.6.1) | yes (4.0.6.1) | yes |
| McAfee VirusScan Professional | 8.x | yes (3.5.1) | yes (3.5.1) | yes |
| McAfee VirusScan Professional | 8xxx | yes (3.5.0) | yes (3.5.0) | yes |
| McAfee VirusScan Professional | 9.x | yes (3.5.1) | yes (3.5.1) | yes |
| McAfee VirusScan Professional Edition | 7.x | yes (3.5.0) | yes (3.5.0) | yes |
| Total Protection for Small Business | 4.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| **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 OneCare Live | 0.8.x | yes (3.5.11.1) | - | - |
| **MicroWorld** | | | | |
| eScan Anti-Virus (AV) for Windows | 8.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| eScan Corporate for Windows | 8.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| eScan Internet Security for Windows | 8.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| eScan Professional for Windows | 8.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |

*Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 6 of 10)*

| Product Name | Product Version | AV Checks Supported (Minimum Agent Version Needed)[1] | | Live Update [2, 3] |
|---|---|---|---|---|
| | | Installation | Virus Definition | |
| eScan Virus Control (VC) for Windows | 8.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| **Norman ASA** | | | | |
| Norman Virus Control | 5.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| **Panda Software** | | | | |
| Panda Antivirus 2007 | 2.x | yes (4.0.4.0) | yes (4.0.4.0) | - |
| Panda Antivirus 2008 | 3.x | yes (4.0.6.1) | yes (4.0.6.1) | - |
| Panda Antivirus 6.0 Platinum | 6 | yes (3.5.0) | yes (3.5.0) | yes |
| Panda Antivirus + Firewall 2007 | 6.x | yes (4.0.4.0) | yes (4.0.4.0) | yes |
| Panda Antivirus Lite | 1.x | yes (3.5.0) | yes (3.5.0) | - |
| Panda Antivirus Lite | 3.x | yes (3.5.9) | yes (3.5.9) | - |
| Panda Antivirus Platinum | 7.04.x | yes (3.5.0) | yes (3.5.0) | yes |
| Panda Antivirus Platinum | 7.05.x | yes (3.5.0) | yes (3.5.0) | yes |
| Panda Antivirus Platinum | 7.06.x | yes (3.5.0) | yes (3.5.0) | yes |
| Panda Client Shield | 4.x | yes (4.0.4.0) | yes (4.0.4.0) | - |
| Panda Internet Security 2007 | 11.x | yes (4.0.4.0) | yes (4.0.4.0) | yes |
| Panda Internet Security 2008 | 12.x | yes (4.0.6.1) | yes (4.0.6.1) | yes |
| Panda Platinum 2005 Internet Security | 9.x | yes (3.5.3) | yes (3.5.3) | yes |
| Panda Platinum 2006 Internet Security | 10.x | yes (4.0.4.0) | yes (4.0.4.0) | yes |
| Panda Platinum Internet Security | 8.03.x | yes (3.5.0) | yes (3.5.0) | yes |
| Panda Titanium 2006 Antivirus + Antispyware | 5.x | yes (3.5.10.1) | yes (3.5.10.1) | yes |
| Panda Titanium Antivirus 2004 | 3.00.00 | yes (3.5.0) | yes (3.5.0) | yes |
| Panda Titanium Antivirus 2004 | 3.01.x | yes (3.5.0) | yes (3.5.0) | yes |
| Panda Titanium Antivirus 2004 | 3.02.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Panda Titanium Antivirus 2005 | 4.x | yes (3.5.1) | yes (3.5.1) | yes |
| Panda TruPrevent Personal 2005 | 2.x | yes (3.5.3) | yes (3.5.3) | yes |
| Panda TruPrevent Personal 2006 | 3.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| WebAdmin Client Antivirus | 3.x | yes (3.5.11) | yes (3.5.11) | - |
| **Radialpoint Inc.** | | | | |
| 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 |
| **SalD Ltd.** | | | | |
| Dr.Web | 4.32.x | yes (3.5.0) | yes (3.5.0) | yes |

*Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 7 of 10)*

| Product Name | Product Version | AV Checks Supported (Minimum Agent Version Needed)[1] | | Live Update [2, 3] |
|---|---|---|---|---|
| | | Installation | Virus Definition | |
| Dr.Web | 4.33.x | yes (3.5.11.1) | yes (3.5.11.1) | yes |
| **Sereniti, Inc.** | | | | |
| Sereniti Antivirus | 1.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| The River Home Network Security Suite | 1.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| **SOFTWIN** | | | | |
| BitDefender 8 Free Edition | 8.x | yes (3.5.8) | yes (3.5.8) | - |
| BitDefender 8 Professional Plus | 8.x | yes (3.5.0) | yes (3.5.0) | - |
| BitDefender 8 Standard | 8.x | yes (3.5.0) | yes (3.5.0) | - |
| BitDefender 9 Internet Security AntiVirus | 9.x | yes (3.5.11.1) | yes (3.5.11.1) | - |
| BitDefender 9 Professional Plus | 9.x | yes (3.5.8) | yes (3.5.8) | yes |
| BitDefender 9 Standard | 9.x | yes (3.5.8) | yes (3.5.8) | yes |
| BitDefender Antivirus 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 Free Edition | 7.x | yes (3.5.0) | yes (3.5.0) | - |
| 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) | - |
| **Sophos Plc.** | | | | |
| Sophos Anti-Virus | 3.x | yes (3.5.3) | yes (3.5.3) | - |
| Sophos Anti-Virus | 4.x | yes (3.6.3.0) | yes (3.6.3.0) | - |
| Sophos Anti-Virus | 5.x | yes (3.5.3) | yes (3.5.3) | yes |
| Sophos Anti-Virus | 6.x | yes (4.0.1.0) | yes (4.0.1.0) | yes |
| Sophos Anti-Virus | 7.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| Sophos Anti-Virus version 3.80 | 3.8 | yes (3.5.0) | yes (3.5.0) | - |
| **Symantec Corp.** | | | | |
| Norton 360 (Symantec Corporation) | 1.x | yes (4.1.1.0) | yes (4.1.1.0) | yes |
| Norton AntiVirus | 10.x | yes (3.5.0) | yes (3.5.0) | yes |
| Norton AntiVirus | 14.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Norton AntiVirus | 15.x | yes (4.0.6.1) | yes (4.0.6.1) | yes |
| Norton AntiVirus 2002 | 8.00.x | yes (3.5.0) | yes (3.5.0) | yes |
| Norton AntiVirus 2002 | 8.x | yes (3.5.1) | yes (3.5.1) | yes |
| Norton AntiVirus 2002 Professional | 8.x | yes (3.5.0) | yes (3.5.0) | yes |
| Norton AntiVirus 2002 Professional Edition | 8.x | yes (3.5.0) | yes (3.5.0) | yes |
| Norton AntiVirus 2003 | 9.x | yes (3.5.0) | yes (3.5.0) | yes |

*Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 8 of 10)*

| Product Name | Product Version | AV Checks Supported (Minimum Agent Version Needed)[1] | | Live Update [2, 3] |
|---|---|---|---|---|
| | | **Installation** | **Virus Definition** | |
| Norton AntiVirus 2003 Professional | 9.x | yes (3.5.0) | yes (3.5.0) | yes |
| Norton AntiVirus 2003 Professional Edition | 9.x | yes (3.5.0) | yes (3.5.0) | yes |
| Norton AntiVirus 2004 | 10.x | yes (3.5.0) | yes (3.5.0) | yes |
| Norton AntiVirus 2004 Professional | 10.x | yes (3.5.0) | yes (3.5.0) | yes |
| Norton AntiVirus 2004 Professional Edition | 10.x | yes (3.5.0) | yes (3.5.0) | yes |
| Norton AntiVirus 2004 (Symantec Corporation) | 10.x | yes (3.5.0) | yes (3.5.0) | yes |
| Norton AntiVirus 2005 | 11.0.x | yes (3.5.0) | yes (3.5.0) | yes |
| Norton AntiVirus 2006 | 12.0.x | yes (3.5.5) | yes (3.5.5) | yes |
| Norton AntiVirus 2006 | 12.x | yes (3.5.5) | yes (3.5.5) | yes |
| Norton AntiVirus Corporate Edition | 7.x | yes (3.5.1) | yes (3.5.1) | yes |
| Norton Internet Security | 7.x | yes (3.5.0) | yes (3.5.0) | yes |
| Norton Internet Security | 8.0.x | yes (3.5.0) | yes (3.5.0) | yes |
| Norton Internet Security | 8.2.x | yes (3.5.1) | yes (3.5.1) | yes |
| Norton Internet Security | 8.x | yes (3.5.1) | yes (3.5.1) | yes |
| Norton Internet Security | 9.x | yes (3.5.10.1) | yes (3.5.10.1) | yes |
| Norton Internet Security (Symantec Corporation) | 10.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Norton SystemWorks 2003 | 6.x | yes (3.5.3) | yes (3.5.3) | yes |
| Norton SystemWorks 2004 Professional | 7.x | yes (3.5.4) | yes (3.5.4) | yes |
| Norton SystemWorks 2005 | 8.x | yes (3.5.3) | yes (3.5.3) | yes |
| Norton SystemWorks 2005 Premier | 8.x | yes (3.5.3) | yes (3.5.3) | yes |
| Norton SystemWorks 2006 Premier | 12.0.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Symantec AntiVirus | 10.x | yes (3.5.3) | yes (3.5.3) | yes |
| Symantec AntiVirus | 9.x | yes (3.5.0) | yes (3.5.0) | yes |
| Symantec AntiVirus Client | 8.x | yes (3.5.0) | yes (3.5.0) | yes |
| Symantec AntiVirus Server | 8.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Symantec AntiVirus Win64 | 10.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| Symantec Client Security | 10.x | yes (3.5.3) | yes (3.5.3) | yes |
| Symantec Client Security | 9.x | yes (3.5.0) | yes (3.5.0) | yes |
| Symantec Endpoint Protection | 11.x | yes (4.0.6.1) | yes (4.0.6.1) | yes |
| Symantec Scan Engine | 5.x | yes (4.0.5.1) | yes (4.0.5.1) | - |
| **Trend Micro, Inc.** | | | | |
| PC-cillin 2002 | 9.x | yes (3.5.1) | yes (3.5.1) | - |

*Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 9 of 10)*

| Product Name | Product Version | AV Checks Supported (Minimum Agent Version Needed)[1] | | Live Update [2, 3] |
|---|---|---|---|---|
| | | Installation | Virus Definition | |
| PC-cillin 2003 | 10.x | yes (3.5.0) | yes (3.5.0) | - |
| ServerProtect | 5.x | yes (4.1.0.0) | yes (3.6.5.0) | - |
| Trend Micro Antivirus | 11.x | yes (3.5.0) | yes (3.5.0) | yes |
| Trend Micro AntiVirus | 15.x | yes (3.6.5.0) | yes (3.6.5.0) | - |
| Trend Micro Client/Server Security | 6.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Trend Micro Client/Server Security Agent | 7.x | yes (3.5.12) | yes (3.5.12) | yes |
| Trend Micro HouseCall | 1.x | yes (4.0.1.0) | yes (4.0.1.0) | - |
| Trend Micro Internet Security | 11.x | yes (3.5.0) | yes (3.5.0) | yes |
| Trend Micro Internet Security | 12.x | yes (3.5.0) | yes (3.5.0) | - |
| Trend Micro OfficeScan Client | 5.x | yes (3.5.1) | yes (3.5.1) | yes |
| Trend Micro OfficeScan Client | 6.x | yes (3.5.1) | yes (3.5.1) | yes |
| Trend Micro OfficeScan Client | 7.x | yes (3.5.3) | yes (3.5.3) | yes |
| Trend Micro OfficeScan Client | 8.x | yes (4.0.5.0) | yes (4.0.5.0) | yes |
| Trend Micro PC-cillin 2004 | 11.x | yes (3.5.0) | yes (3.5.0) | yes |
| Trend Micro PC-cillin Internet Security 12 | 12.x | yes (4.0.1.0) | yes (4.0.1.0) | - |
| Trend Micro PC-cillin Internet Security 14 | 14.x | yes (4.0.1.0) | yes (4.0.1.0) | yes |
| Trend Micro PC-cillin Internet Security 2005 | 12.x | yes (3.5.3) | yes (3.5.3) | yes |
| Trend Micro PC-cillin Internet Security 2006 | 14.x | yes (3.5.8) | yes (3.5.8) | yes |
| Trend Micro PC-cillin Internet Security 2007 | 15.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| **VCOM** | | | | |
| Fix-It Utilities 7 Professional [AntiVirus] | 7.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| SystemSuite 7 Professional [AntiVirus] | 7.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| VCOM Fix-It Utilities Professional 6 [AntiVirus] | 6.x | yes (4.0.6.1) | yes (4.0.6.1) | yes |
| **Verizon** | | | | |
| Verizon Internet Security Suite Anti-Virus | 5.x | yes (4.0.5.1) | yes (4.0.5.1) | - |
| **Yahoo!, Inc.** | | | | |
| AT&T Yahoo! Online Protection [AntiVirus] | 7.x | yes (4.0.6.1) | yes (4.0.6.1) | yes |
| SBC Yahoo! Anti-Virus | 7.x | yes (3.5.10.1) | yes (3.5.10.1) | yes |
| Verizon Yahoo! Online Protection [AntiVirus] | 7.x | yes (4.0.6.1) | yes (4.0.6.1) | yes |
| **Zone Labs LLC** | | | | |
| ZoneAlarm Anti-virus | 6.x | yes (3.5.5) | yes (3.5.5) | - |
| ZoneAlarm Security Suite | 5.x | yes (3.5.0) | yes (3.5.0) | - |

*Table 5 Clean Access Antivirus Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 10 of 10)*

| Product Name | Product Version | AV Checks Supported (Minimum Agent Version Needed)[1] | | Live Update [2, 3] |
|---|---|---|---|---|
| | | Installation | Virus Definition | |
| ZoneAlarm Security Suite | 6.x | yes (3.5.5) | yes (3.5.5) | - |
| ZoneAlarm with Antivirus | 5.x | yes (3.5.0) | yes (3.5.0) | - |

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

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

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

# Clean Access AV Support Chart (Windows ME/98)

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

*Table 6 Clean Access Antivirus Product Support Chart (Windows ME/98) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 1 of 2)*

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

*Table 6 Clean Access Antivirus Product Support Chart (Windows ME/98) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 2 of 2)*

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

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

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

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

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

Table 7 lists Windows Vista/XP/2000 Supported Antispyware Products as of the latest release of the Cisco Clean Access software.

*Table 7 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 1 of 5)*

| | | AS Checks Supported (Minimum Agent Version Needed)[1] | | |
|---|---|---|---|---|
| **Product Name** | **Product Version** | **Installation** | **Spyware Definition** | **Live Update[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 7.0 Platinum Enterprise AntiSpyware | 7.x | yes (4.1.2.0) | yes (4.1.2.0) | yes |
| **America Online, Inc.** | | | | |
| AOL Safety and Security Center Spyware Protection | 2.0.x | yes (4.1.0.0) | - | - |
| AOL Safety and Security Center Spyware Protection | 2.1.x | yes (4.1.0.0) | yes (4.1.0.0) | - |
| AOL Safety and Security Center Spyware Protection | 2.2.x | yes (4.1.0.0) | yes (4.1.0.0) | - |
| AOL Safety and Security Center Spyware Protection | 2.3.x | yes (4.1.0.0) | yes (4.1.0.0) | - |
| AOL Safety and Security Center Spyware Protection | 2.x | yes (3.6.1.0) | yes (3.6.1.0) | - |
| AOL Spyware Protection | 1.x | yes (3.6.0.0) | yes (3.6.0.0) | - |
| AOL Spyware Protection | 2.x | yes (3.6.0.0) | - | - |
| **Anonymizer, Inc.** | | | | |
| Anonymizer Anti-Spyware | 1.x | yes (4.1.0.0) | yes (4.1.0.0) | - |
| Anonymizer Anti-Spyware | 3.x | yes (4.1.0.0) | yes (4.1.0.0) | - |
| **Authentium, Inc.** | | | | |
| Cox High Speed Internet Security Suite | 3.x | yes (4.0.4.0) | - | yes |
| **BellSouth** | | | | |
| BellSouth Internet Security Anti-Spyware | 5.x | yes (4.0.5.1) | yes (4.0.5.1) | - |
| **Bullet Proof Soft** | | | | |
| BPS Spyware & Adware Remover | 9.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| BPS Spyware-Adware Remover | 8.x | yes (3.6.0.0) | yes (3.6.0.0) | yes |
| BPS Spyware Remover | 9.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |

*Table 7 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 2 of 5)*

| | | AS Checks Supported (Minimum Agent Version Needed)[1] | | |
|---|---|---|---|---|
| **Product Name** | **Product Version** | **Installation** | **Spyware Definition** | **Live Update[2]** |
| **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 Security Suite Antispyware | 7.x | yes (4.0.5.0) | yes (4.0.5.0) | yes |
| **Computer Associates International, Inc.** | | | | |
| CA eTrust Internet Security Suite AntiSpyware | 5.x | yes (3.6.1.0) | yes (3.6.1.0) | yes |
| CA eTrust Internet Security Suite AntiSpyware | 8.x | yes (4.1.2.0) | yes (4.1.2.0) | yes |
| CA eTrust Internet Security Suite AntiSpyware | 9.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| CA eTrust PestPatrol | 5.x | yes (3.6.1.0) | yes (4.0.6.0) | yes |
| CA eTrust PestPatrol Anti-Spyware | 8.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| CA eTrust PestPatrol Anti-Spyware Corporate Edition | 5.x | yes (3.6.0.0) | yes (3.6.0.0) | yes |
| PestPatrol Corporate Edition | 4.x | yes (3.6.0.0) | yes (3.6.0.0) | yes |
| PestPatrol Standard Edition (Evaluation) | 4.x | yes (3.6.0.0) | yes (3.6.0.0) | yes |
| **EarthLink, Inc.** | | | | |
| Aluria Security Center AntiSpyware | 1.x | yes (4.1.0.0) | yes (4.1.0.0) | - |
| EarthLink Protection Control Center AntiSpyware | 1.x | yes (3.6.0.0) | yes (3.6.0.0) | - |
| EarthLink Protection Control Center AntiSpyware | 2.x | yes (4.0.6.0) | - | - |
| Primary Response SafeConnect | 2.x | yes (3.6.5.0) | - | - |
| **FaceTime Communications, Inc.** | | | | |
| X-Cleaner Deluxe | 4.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| **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** | | | | |
| 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 7 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 3 of 5)*

| Product Name | Product Version | AS Checks Supported (Minimum Agent Version Needed)[1] | | Live Update[2] |
|---|---|---|---|---|
| | | Installation | Spyware Definition | |
| SpywareBlaster v3.5.1 | 3.5.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| **Kingsoft Corp.** | | | | |
| Kingsoft Internet Security [AntiSpyware] | 7.x | yes (4.0.6.1) | yes (4.0.6.1) | yes |
| **Lavasoft, Inc.** | | | | |
| Ad-Aware 2007 Professional | 7.x | yes (4.0.6.1) | - | yes |
| Ad-aware 6 Professional | 6.x | yes (3.6.0.0) | yes (3.6.0.0) | - |
| Ad-Aware SE Personal | 1.x | yes (3.6.0.0) | yes (3.6.0.0) | - |
| Ad-Aware SE Professional | 1.x | yes (3.6.1.0) | yes (3.6.1.0) | yes |
| **McAfee, Inc.** | | | | |
| McAfee AntiSpyware | 1.5.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| McAfee AntiSpyware | 1.x | yes (3.6.0.0) | yes (4.1.0.0) | yes |
| McAfee AntiSpyware | 2.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| McAfee AntiSpyware Enterprise | 8.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| McAfee Anti-Spyware Enterprise Module | 8.0.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| McAfee VirusScan AS | 11.x | yes (4.0.6.1) | yes (4.0.6.1) | yes |
| **MicroSmarts LLC** | | | | |
| Spyware Begone | 4.x | yes (3.6.0.0) | - | - |
| Spyware Begone | 6.x | yes (4.1.0.0) | - | - |
| Spyware Begone | 8.x | yes (4.1.0.0) | - | - |
| Spyware Begone Free Scan | 7.x | yes (3.6.0.0) | - | - |
| Spyware Begone V7.30 | 7.30.x | yes (3.6.1.0) | - | - |
| Spyware Begone V7.40 | 7.40.x | yes (3.6.1.0) | - | - |
| Spyware Begone V7.95 | 7.95.x | yes (4.1.0.0) | - | - |
| Spyware Begone V8.20 | 8.20.x | yes (4.1.0.0) | - | - |
| Spyware Begone V8.25 | 8.25.x | yes (4.1.0.0) | - | - |
| **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 |
| **PC Tools Software** | | | | |
| Spyware Doctor | 4.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Spyware Doctor | 5.x | yes (4.0.6.0) | - | yes |
| Spyware Doctor 3.0 | 3.x | yes (3.6.0.0) | yes (3.6.0.0) | yes |

*Table 7 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 4 of 5)*

| | | AS Checks Supported (Minimum Agent Version Needed)[1] | | |
|---|---|---|---|---|
| **Product Name** | **Product Version** | **Installation** | **Spyware Definition** | **Live Update[2]** |
| 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 |
| **Prevx Ltd.** | | | | |
| Prevx1 | 1.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Prevx1 | 2.x | yes (4.1.0.0) | yes (4.1.0.0) | yes |
| Prevx Home | 2.x | yes (3.6.0.0) | yes (3.6.0.0) | - |
| **Radialpoint Inc.** | | | | |
| Radialpoint 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 |
| **Safer Networking Ltd.** | | | | |
| Spybot - Search & Destroy 1.3 | 1.3 | yes (3.6.0.0) | yes (3.6.0.0) | yes |
| Spybot - Search & Destroy 1.4 | 1.4 | yes (3.6.0.0) | yes (3.6.0.0) | yes |
| Spybot - Search & Destroy 1.5 | 1.x | yes (4.0.6.1) | yes (4.0.6.1) | - |
| **Sereniti, Inc.** | | | | |
| Sereniti Antispyware | 1.x | yes (4.0.6.0) | - | yes |
| The River Home Network Security Suite Antispyware | 1.x | yes (4.0.6.0) | - | yes |
| **SOFTWIN** | | | | |
| BitDefender 9 Antispyware | 9.x | yes (4.1.0.0) | yes (4.1.0.0) | - |
| **Sunbelt Software** | | | | |
| CounterSpy Enterprise Agent | 1.8.x | yes (4.0.6.0) | - | - |
| Sunbelt CounterSpy | 1.x | yes (3.6.0.0) | - | yes |
| Sunbelt CounterSpy | 2.x | yes (4.0.6.0) | - | yes |
| **Symantec Corp.** | | | | |
| Norton Spyware Scan | 2.x | yes (4.1.0.0) | yes (4.1.0.0) | - |
| **Trend Micro, Inc.** | | | | |
| Trend Micro Anti-Spyware | 3.5.x | yes (4.0.5.1) | yes (4.0.5.1) | - |
| Trend Micro Anti-Spyware | 3.x | yes (3.6.0.0) | - | - |
| Trend Micro PC-cillin Internet Security 2007 AntiSpyware | 15.x | yes (4.1.0.0) | - | yes |
| **VCOM** | | | | |

*Table 7 Clean Access Antispyware Product Support Chart (Windows Vista/XP/2000) Version 66, 4.1.2.2 Agent/Release 4.1.2.1 (Sheet 5 of 5)*

| | | **AS Checks Supported (Minimum Agent Version Needed)**[1] | | |
|---|---|---|---|---|
| **Product Name** | **Product Version** | **Installation** | **Spyware Definition** | **Live Update**[2] |
| Fix-It Utilities 7 Professional [AntiSpyware] | 7.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| SystemSuite 7 Professional [AntiSpyware] | 7.x | yes (4.0.5.1) | yes (4.0.5.1) | yes |
| VCOM Fix-It Utilities Professional 6 [AntiSpyware] | 6.x | yes (4.0.6.1) | yes (4.0.6.1) | yes |
| **Verizon** | | | | |
| Verizon Internet Security Suite Anti-Spyware | 5.x | yes (4.0.5.1) | yes (4.0.5.1) | - |
| **Webroot Software, Inc.** | | | | |
| Spy Sweeper | 3.x | yes (3.6.0.0) | - | - |
| Spy Sweeper | 4.x | yes (3.6.0.0) | - | - |
| Spy Sweeper | 5.x | yes (4.1.0.0) | - | - |
| Webroot Spy Sweeper Enterprise Client | 1.x | yes (3.6.0.0) | - | - |
| Webroot Spy Sweeper Enterprise Client | 2.x | yes (3.6.1.0) | - | - |
| Webroot Spy Sweeper Enterprise Client | 3.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 |
| SBC Yahoo! Applications | 2005.x | yes (3.6.0.0) | yes (3.6.0.0) | yes |
| Verizon Yahoo! Online Protection | 2005.x | yes (4.0.6.1) | yes (4.0.6.1) | yes |
| Yahoo! Anti-Spy | 1.x | yes (3.6.0.0) | yes (3.6.0.0) | - |
| **Zone Labs LLC** | | | | |
| Integrity Agent | 6.x | yes (4.1.2.0) | yes (4.1.2.0) | - |

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

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

# Supported AV/AS Product List Version Summary

Table 8 details enhancements made per version of the Supported Antivirus/Antispyware Product List. See Clean Access Supported AV/AS Product List, page 16 for the latest Supported AV list as of the latest release. See New and Changed Information, page 11 for the release feature list.

*Table 8 Supported AV /AS Product List Versions*

| Version | Enhancements |
|---|---|
| **Release 4.1.2.1—4.1.2.2 Agent** | |
| Version 66 | **AV Chart (Windows Vista/XP/2000)**—added live update support for new product:<br>• Trend Micro OfficeScan Client 8.x |
| Version 65 | Minor internally used data change |
| **Release 4.1.2.1—4.1.2.1 Agent** | |
| Version 64 | **Added New AV Products (Windows Vista/XP/2000):**<br>• eEye Digital Security Blink Personal, 3.x<br>• eEye Digital Security Blink Professional, 3.x<br>• FortiClient Consumer Edition, 3.x<br>• IKARUS Guard NT, 2.x<br>• IKARUS virus utilities, 5.x<br>• Kaspersky Anti-Virus for Windows Workstations, 6.x<br>• TrustPort Antivirus, 2.x<br>• Proventia Desktop, 8.x<br>• Proventia Desktop, 9.x<br>• ClamAV, devel-x<br>• McAfee VirusScan Home Edition, 7.x<br>• Panda Antivirus 2008, 3.x<br>• Panda Internet Security 2008, 12.x<br>• Norton AntiVirus, 15.x<br>• Symantec Endpoint Protection, 11.x<br>• VCOM Fix-It Utilities Professional 6 [AntiVirus], 6.x<br>• AT&T Yahoo! Online Protection [AntiVirus], 7.x<br>• Verizon Yahoo! Online Protection [AntiVirus], 7.x<br>**Added Live Update for the Following AV Products:**<br>• eEye Digital Security Blink Personal, 3.x |

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

| Version | Enhancements |
|---|---|
| Version 64 (continued) | **Added New AS Products (Windows Vista/XP/2000):**<br>• Spyware Doctor, 5.x<br>• EarthLink Protection Control Center AntiSpyware, 2.x<br>• Microsoft AntiSpyware, 1.x<br>• Sereniti Antispyware, 1.x<br>• The River Home Network Security Suite Antispyware, 1.x<br>• Zero-Knowledge Systems Radialpoint Security Services Spyware Protection, 6.x<br>• CounterSpy Enterprise Agent, 1.8.x<br>• Sunbelt CounterSpy, 2.x<br>• Kingsoft Internet Security [AntiSpyware], 7.x<br>• Ad-Aware 2007 Professional, 7.x<br>• McAfee VirusScan AS, 11.x<br>• Spybot - Search & Destroy 1.5, 1.x<br>• VCOM Fix-It Utilities Professional 6 [AntiSpyware], 6.x<br>• AT&T Yahoo! Online Protection, 2006.x<br>• Verizon Yahoo! Online Protection, 2005.x |
| Version 63 | **Added New AS Product (Windows Vista/XP/2000):**<br>• Webroot Spy Sweeper Enterprise Client, 3.x |
| Version 62 | Minor internally used data change |

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

| Version | Enhancements |
|---|---|
| **Release 4.1(2)—4.1.2.0 Agent** | |
| Version 61 | **Added New AV Products (Windows Vista/XP/2000):**<br>• AhnLab V3 Internet Security 7.0 Platinum Enterprise, 7.x<br>• BellSouth Internet Security Anti-Virus, 5.x<br>• ZoneAlarm Anti-virus, 7.x<br>• ZoneAlarm (AntiVirus), 7.x<br>• ClamAV, devel-x<br>• EarthLink Protection Control Center AntiVirus, 2.x<br>• F-PROT Antivirus for Windows, 6.0.x<br>• ViRobot Desktop, 5.0.x<br>• Kaspersky Anti-Virus for Windows File Servers, 5.x<br>• Kaspersky Anti-Virus for Windows Workstations, 5.0.x<br>• Kaspersky Anti-Virus for Workstation, 5.0.x<br>• Total Protection for Small Business, 4.x<br>• Radialpoint Virus Protection, 5.x<br>• Zero-Knowledge Systems Radialpoint Security Services Virus Protection, 6.x<br>• Sereniti Antivirus, 1.x<br>• The River Home Network Security Suite, 1.x<br>• Sophos Anti-Virus, 7.x<br>• Symantec AntiVirus Win64Symantec AntiVirus Win64, 10.x<br>• Symantec Scan Engine, 5.x<br>• Symantec AntiVirus Win64, 10.x<br>• Fix-It Utilities 7 Professional [AntiVirus], 7.x<br>• SystemSuite 7 Professional [AntiVirus], 7.x<br>• Verizon Internet Security Suite Anti-Virus, 5.x<br>• V3 VirusBlock 2005, 6.x<br>• BullGuard 7.0, 7.x<br>**Added Live Update for the Following AV Products:**<br>• ZoneAlarm Security Suite Antivirus, 7.x<br>• Panda Antivirus + Firewall 2007, 6.x |

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

| Version | Enhancements |
|---|---|
| Version 61 (continued) | **Added New AS products:**<br>• AhnLab V3 Internet Security 2007 Platinum AntiSpyware, 7.x<br>• BellSouth Internet Security Anti-Spyware, 5.x<br>• ZoneAlarm (AntiSpyware), 7.x<br>• AVG Anti-Spyware 7.5, 7.x<br>• McAfee Anti-Spyware Enterprise Module, 8.0.x<br>• ZoneAlarm Anti-Spyware, 7.x<br>• ZoneAlarm Pro Antispyware, 7.x<br>• Radialpoint Spyware Protection, 5.x<br>• Zero-Knowledge Systems Radialpoint Security Services Spyware Protection, 6.x<br>• Trend Micro Anti-Spyware, 3.5.x<br>• Fix-It Utilities 7 Professional [AntiSpyware], 7.x<br>• SystemSuite 7 Professional [AntiSpyware], 7.x<br>• Verizon Internet Security Suite Anti-Spyware, 5.x<br>• AhnLab V3 Internet Security 7.0 Platinum Enterprise AntiSpyware, 7.x<br>• CA eTrust Internet Security Suite AntiSpyware, 8.x<br>• AVG Anti-Malware [AntiSpyware], 7.x<br>• Integrity Agent, 6.x<br>**Added Live Update for the Following AS Products:**<br>• ZoneAlarm Security Suite Antispyware, 7.x |
| Version 60 | Minor internally used data change |

**Note** Cisco strongly recommends running version 4.1.2.2 of the Clean Access Agent with release 4.1(2) and later of the CAM/CAS. However, administrators can optionally configure the 4.1(2) CAM/CAS to allow login and posture assessment from 4.1.0.x Agents. Refer to the "Supported AV/AS Product List Version Summary" of the *Release Notes for Cisco NAC Appliance (Cisco Clean Access) Version 4.1(0)* for complete details on 4.1.0.x Agent AV/AS support.

# Clean Access Agent Version Summary

This section consolidates information for the Clean Access Agent client software. Table 9 lists the latest enhancements per version of the Clean Access Agent. Unless otherwise noted, enhancements are cumulative and apply both to the version introducing the feature and to subsequent later versions.

See Clean Access Supported AV/AS Product List, page 16 for details on related AV/AS support.

*Table 9 Clean Access Agent Versions*

| Agent Version [1] | Feature / Enhancement |
|---|---|
| 4.1.2.2 | • Version 4.1.2.2 of the Clean Access Agent includes fixes for the following caveats:<br>– CSCsk45258<br>– CSCsk68388<br>**Note** The 4.1.2.1 and later Agents perform authentication only for 64-bit client operating systems. Once the user is authenticated, the Agent does not perform posture assessment or remediation. To support 64-bit operating system Agents, the CAM and CAS must also be running release 4.1.2.1.<br>Because Cisco NAC Appliance provides authentication-only support for 64-bit operating system Agents, nessus scanning via the Clean Access Agent does not perform remediation on the client machine.<br>• Adds support as described in Supported AV/AS Product List Version Summary, page 34. See also Clean Access Agent (4.1.2.2), page 11. |

*Table 9 Clean Access Agent Versions*

| Agent Version [1] | Feature / Enhancement |
|---|---|
| 4.1.2.1 | • Release 4.1.2.1 introduces the 4.1.2.1 Clean Access Agent that performs authentication only on 64-bit Windows Vista and Windows XP client operating systems. The following 64-bit operating systems are supported:<br>– Windows XP Professional x64<br>– Windows Vista Home Basic x64<br>– Windows Vista Home Premium x64<br>– Windows Vista Business x64<br>– Windows Vista Ultimate x64<br>– Windows Vista Enterprise x64<br>• Once the user is authenticated, the Agent does not perform posture assessment or remediation. To support 64-bit operating system Agents, the CAM and CAS must also be running release 4.1.2.1. Because Cisco NAC Appliance provides authentication-only support for 64-bit operating system Agents, nessus scanning via the Clean Access Agent does not perform remediation on the client machine.<br>• Version 4.1.2.1 of the Clean Access Agent includes fixes for the following caveats:<br>– CSCsj28193<br>– CSCsj37496<br>– CSCsj49408<br>– CSCsj92822<br>– CSCsk01928<br>– CSCsk15081<br>– CSCsk20213<br>– CSCsk27579<br>• Adds support as described in Supported AV/AS Product List Version Summary, page 34. |
| 4.1.2.0 | **Windows Agent Enhancements (4.1.2.0)**<br>No new features or enhancements in Agent version 4.1.2.0—bug fixes only.<br>**Note** Clean Access Agent stub is not supported on Windows Vista.<br>For checks/rules/requirements, the Agent can detect "N" (European) versions of the Windows Vista operating system, but the CAM/CAS treat "N" versions of Vista as their US counterpart.<br>**Mac OS Agent Enhancements (4.1.2.0)**<br>No new features or enhancements in Agent version 4.1.2.0—bug fixes only.<br>**Note** Release 4.1(2) does not support auto-upgrade for the Mac OS Agent. Users can upgrade client machines to the latest Mac OS Agent by downloading the Agent via web login and running the Agent installation. |

*Table 9 Clean Access Agent Versions*

| Agent Version [1] | Feature / Enhancement |
|---|---|
| 4.1.1.0 | See the "Clean Access Agent Version Summary" section in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access) Version 4.1(1)* for details on the 4.1.1.0 Agent. |
| 4.1.0.x | See the "Clean Access Agent Version Summary" section in the *Release Notes for Cisco NAC Appliance (Cisco Clean Access) Version 4.1(0)* for details on the 4.1.0.x Agent. |

[1] See Release 4.1(2) CAM/CAS-Agent Compatibility, page 7 for upgrade compatibility details.

# Caveats

This section describes the following caveats:

- Open Caveats - Release 4.1.2.1, page 41
- Resolved Caveats - Agent Version 4.1.2.2, page 45
- Resolved Caveats - Release 4.1.2.1, page 45
- Resolved Caveats - Release 4.1(2), page 47

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

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

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

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

## Open Caveats - Release 4.1.2.1

*Table 10 List of Open Caveats (Sheet 1 of 4)*

| | Software Release 4.1.2.1 | |
|---|---|---|
| **DDTS Number** | **Corrected** | **Caveat** |
| CSCsd90433 | No | Apache does not start on HA-Standby CAM after heartbeat link is restored.<br>Output from the fostate.sh command shows "My node is standby without web console, peer node is active." |
| CSCse86581 | No | Agent does not correctly recognize def versions on the following Trend AV products:<br>• PC-cillin Internet Security 2005<br>• PC-cillin Internet Security 2006<br>• OfficeScan Client<br>Tested Clients:<br>• PC-cillin Internet Security 2006 (English) on US-English Windows 2000 SP4<br>• OfficeScan Client (English) on US-English Windows 2000 SP4<br>• VirusBaster 2006 Internet Security (Japanese) on Japanese Windows XP SP2<br>• VirusBaster Corporate Edition (Japanese) on Japanese Windows XP SP2 |

*Table 10 List of Open Caveats (Sheet 2 of 4)*

| DDTS Number | Software Release 4.1.2.1 | |
|---|---|---|
| | **Corrected** | **Caveat** |
| CSCsg07369 | No | Incorrect "IP lease total" displayed on editing manually created subnets<br>Steps to reproduce:<br>1. Add a Managed Subnet having at least 2500+ IP addresses for e.g. 10.101.0.1 / 255.255.240.0 using CAM web page "Device Management > Clean Access Servers > Manage [IP Address] > Advanced > Managed Subnet"<br>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"<br>3. Edit the newly created subnet using CAM web page "Device Management > Clean Access Servers > Manage [IP Address] > Network > DHCP > Subnet List > Edit"<br>4. Click "Update". The CAM throws a warning announcing the current IP Range brings IP lease total up to a number that is not correct. The CAM counts the IP in the subnet twice which creates the discrepancy.<br>The issue does not affect DHCP functionality and is strictly known to be a cosmetic issue |
| CSCsg38702 | No | Agent cannot recognize Japanese Trend AV installation.<br>Agent properties shows "Product Name" garbled.<br>Client OS affected:<br>• Japanese Windows XP Professional SP2<br>• Japanese Windows 2000 Professional SP4<br>AV product affected:<br>• Japanese VirusBaster Corporate Edition 7.3 (US Product Name: Trend Micro OfficeScan Client)<br>Steps to reproduce:<br>Make a new AV rule:<br>- Type: Installation<br>- OS: Windows XP/2K<br>- Checks for Selected Operating Systems: Trend Micro OfficeScan Client 7.x |
| CSCsg57897 | No | Agent should not popup with client machine's IP address in Subnets device filter<br>Steps to reproduce:<br>1. Include the client's subnet or IP address in subnet based filter list using CAM web page "Device Management > Filters > Subnets"<br>2. Launch CCA Agent on the client machine (can be Windows or Mac OS |

*Table 10 List of Open Caveats (Sheet 3 of 4)*

| DDTS Number | Software Release 4.1.2.1 | |
|---|---|---|
| | **Corrected** | **Caveat** |
| CSCsg66511 | No | Configuring HA-failover synchronization settings on 1st CAS takes an extremely long time<br>The web page for HA-failover synchronization settings should not take so long upon configuring on the first CAS<br>Steps to reproduce:<br>1. Configure HA-Failover on both CAS, except failover synchronization settings<br>2. Go to HA-Secondary CAS web page “Administration > Network Settings > Failover > Synchronization”<br>3. Enter peer SSH Client & SSH Server key<br>4. Click “Update”. It will take around 3 minutes for the browser to get the response from the server. Configuring HA-failover synchronization on the second host (HA-Primary in this case) is done instantaneously and does not take that long |
| CSCsi07595 | No | DST fix will not take effect if generic MST, EST, HST, etc. options are specified<br>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.<br>**Workaround**<br>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.”<br>**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. |
| CSCsi47547 | No | AD SSO does not work if the CAS Account Password contains “()”<br>When CAS account password contains parentheses “()”, the AD SSO service does not start after entering the “Service perfigo restart” command. |
| CSCsi62063 | No | SSLVPN Single Sign On with ISR is unsuccessful<br>The user can log onto the SSLVPN gateway, but is then asked for logon credentials again when trying to access the trusted network. |

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

| | **Software Release 4.1.2.1** | |
|---|---|---|
| **DDTS Number** | **Corrected** | **Caveat** |
| CSCsj84398 | No | NAC-3310: "hda" error appears with specific Seagate hard drive model<br>An "hda" error message shows up on Cisco NAC-3310s with a specific Seagate hard drive model. (A known test issue was discovered and recorded with the Seagate hard drive model ST380815AS featuring "HPFO" firmware.)<br>As a result, the following error message appears on the user console and is logged in the /var/log/messages file:<br>`hda: status timeout: status=0xd0 { Busy }`<br>`ide: failed opcode was: unknown`<br>`hda: no DRQ after issuing MULTWRITE_EXT`<br>`ide0: reset: success` |
| CSCsk31476 | No | Windows Server Update Services Requirement "Show UI" option not working on Windows XP client machines<br>When you configure the Windows Server Update Services (WSUS) Requirement to show the update interface session to users with the "Show UI" **Installation Wizard Interface Setting**, Windows XP client machines install the latest windows update software (currently wuaueng.dll version 7.0.6000.381), but the Clean Access Agent only displays a grey window instead of the expected "Download and Install Updates" window.<br>**Workaround**<br>To avoid this issue, be sure to specify "No UI" for the **Installation Wizard Interface Setting** on your CAM's Windows Server Update Services Requirement configuration page (**Device Management > Clean Access > Clean Access Agent > Requirements > New/Edit**). |
| CSCsk73298 | No | Avira Antivirus PE Classic detected as unknown product on Agent<br>Clean Access Agent versions 4.1.2.1 and 4.1.2.2 detect Avira Antivirus Personal Edition Classic for Windows (7.06.00.270) as an unknown product on client machines running the Windows XP operating system. |

## Resolved Caveats - Agent Version 4.1.2.2

*Table 11 List of Closed Caveats*

| | Agent Version 4.1.2.2 | |
|---|---|---|
| DDTS Number | Corrected | Caveat |
| CSCsk45258 | Yes | Clean Access Agent freezes with Lavasoft Ad-Aware 2007 installed<br>If a client upgrades the Clean Access Agent to version 4.1.2.1 and the client has Lavasoft Ad-Aware 2007 installed, the Agent locks up and will not launch. |
| CSCsk68388 | Yes | Clean Access Agent may not work if Avira AntiVirus PE Classic 7.x is installed and updated<br>Updating the Avira AntiVirus Personal Edition Classic 7.x during a user session can lock up the Clean Access Agent. |

## Resolved Caveats - Release 4.1.2.1

*Table 12 List of Closed Caveats (Sheet 1 of 2)*

| | Software Release 4.1.2.1 | |
|---|---|---|
| DDTS Number | Corrected | Caveat |
| CSCsj28193 | Yes | Agent does not correctly detect Kaspersky 6.0 Antivirus<br>The Agent does not pass install checks for the Kaspersky 6.0 Antivirus application. |
| CSCsj37496 | Yes | Virus Definition File Version intermittently missing from Agent<br>Agent 4.0.5.1 on Windows Vista is intermittently missing the Virus Definition File Version, resulting in authentication failure. |
| CSCsj49408 | Yes | Clean Access Agent lists Microsoft Forefront Unknown Microsoft Product<br>Clean Access Agent 4.0.5.1 and 4.1.1.0 do not properly detect the Microsoft Forefront Client even though it is listed as a supported product for these platforms. |
| CSCsj92822 | Yes | McAfee Anti-Spyware Enterprise Module 8.0.0.989 is not detected by CCA Agent 4.1.2.0 |
| CSCsk01928 | Yes | Norton Antivirus on Windows 98/ME no longer detected by 4.0.6.0 agent<br>Windows 98 Agent login fails when Norton AntiVirus 2005 is the only AV application installed on the client. (No AV is present in the Agent Report Log and the Agent Properties dialog does not display any AV application.) |
| CSCsk05330 | Yes | Clean Access Agent does not work in 64-bit Windows operating systems |

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

| | Software Release 4.1.2.1 | |
|---|---|---|
| **DDTS Number** | **Corrected** | **Caveat** |
| CSCsk15081 | Yes | Apple iPhone should not be categorized as Mac OS X<br>Right now, iPhone users are categorized as Mac OS X users (in the online user list, for example). Because the Mac Agent does not support iPhone, we should not categorize iPhone users as Mac OS X. |
| CSCsk20213 | Yes | The Windows Vista Agent fails Windows Update check in the Korean time zone<br>The Clean Access Agent for clients running the Windows Vista operating system fail the Windows Update check because the Agent and operating system use different delimiters for date formats. (The Windows Vista operating system uses a (yyyy-mm-dd) date format while the Clean Access Agent uses (yyyy/mm/dd). |
| CSCsk24551 | Yes | e1000 network card stops working after upgrading to 4.1.2<br>Machines with Intel e1000 network card might not function correctly after upgrading to 4.1.2.<br>Conditions: Check /var/log/dmesg, e1000 driver version on machines other than ISR NME-NAC module should be 6.3.x, not 6.2.x.<br>Workaround:<br>`cp /lib/modules/2.6.11-perfigo/kernel/drivers/net/e1000/e1000.ko /lib/modules/2.6.11-perfigo/kernel/drivers/net/e1000_bryce/e1000_bryce.ko`<br>**Note** Release 4.1.2.1 is the minimum mandatory 4.1.2.x version for Cisco NAC Appliance. |
| CSCsk27579 | Yes | Agent on 64-bit operating system displays incorrect error message<br>After installing the Clean Access Agent on a Windows Vista/XP 64-bit operating system, users are presented a "The client version is old and not compatible. Please login from web browser to see the download link for the new version" Agent error message. |

## Resolved Caveats - Release 4.1(2)

*Table 13 List of Closed Caveats (Sheet 1 of 5)*

| | Software Release 4.1(2) | |
|---|---|---|
| **DDTS Number** | **Corrected** | **Caveat** |
| CSCsf98683 | Yes | CAM does not send Class attribute in RADIUS accounting<br>The CAM does not include the Class attribute when transmitting user login account information to a RADIUS server. |
| CSCsg98960 | Yes | 4.1(1) Installer does not recognize certain SCSI drives<br>When you install Cisco Clean Access Release 4.1(1) code (either Manager or Server) on certain hardware with SCSI Drives, the Installation process fails and displays the following message:<br>“An error has occurred - no valid devices were found on which to create new filesystems. Please check your hardware for the cause of the problem”<br>Upgrades to 4.1(1) from previous versions are not affected by this bug.<br>**Workaround**<br>At the boot prompt that appears during installation, enter “DL140” and then &lt;Enter&gt;.<br>`Cisco Clean Access Installer (C) 2006 Cisco Systems, Inc.`<br>`Welcome to the Cisco Clean Access Installer!`<br>`- To install a Cisco Clean Access device, press the <ENTER> key.`<br>`- To install a Cisco Clean Access device over a serial console, enter serial at the boot prompt and press the <ENTER> key.`<br>`boot:` **`DL140`** |
| CSCsh55834 | Yes | Sophos AntiVirus definition is failing<br>Recently, Sophos released a Virus Definition update. After enabling the update, users report that the Sophos software fails Cisco Clean Access authentication. |
| CSCsh84260 | Yes | User gets redirected to CAS after successful web login using a Safari browser in Mac OS<br>When functioning normally, a Mac OS client browser opens another window that displays the original URL requested at login following successful authentication. The issue in this case, however, is that the Safari 2.0.3 browser on the client opens another window displaying the CAS web login form over again. |
| CSCsi33630 | Yes | CAM/CAS should not pull all old logs when getting support logs<br>When the option to download the support logs from the Clean Access Manager and/or Clean Access Server is used download a .tar archive of the logs, the entire history of that CAM or CAS is downloaded resulting in massive log files with very little relevant content which are downloaded by the customer and sent to Cisco TAC to troubleshoot the Clean Access system. |

*Table 13 List of Closed Caveats (Sheet 2 of 5)*

| DDTS Number | Software Release 4.1(2) | |
|---|---|---|
| | **Corrected** | **Caveat** |
| CSCsi74978 | Yes | Symantec AntiVirus 10.x not recognized by CCA 4.1.0.2 for Windows XP (German localization) |
| CSCsi75692 | Yes | HTTP 500 error when attempting to upload a file to CAS<br>When the administrator tries to upload a file to the CAS via the CAM web console, the CAM returns an HTTP 500 error message. This error appears when the admin chooses **Authentication > Login Page** and clicks **File Upload** when managing the CAS from the CAM web console.<br>**Note** In addition to the HTTP 500 error message, the actual file upload function fails, as well. |
| CSCsi77900 | Yes | Uploaded Logo does not show up during preview<br>After uploading a logo to the CAM via **User Pages > File Upload**, if you add that logo to the Web Login page and do a preview, the preview page does not show the logo even though the logo *does appear* when the end user is redirected to the login page during Web Login. |
| CSCsi78024 | Yes | Guest Access option fails if the provider option is not Local DB<br>Under Web Login page, the Guest Access option does not work if the Provider is anything other than the local database. To enable the Guest option, change the Provider to “Local DB” and click the Guest Access button. |
| CSCsi79315 | Yes | Nessus Scanner: unable to update “SMB domain (optional)” value<br>Administrators cannot update or remove the preference value for the SMB domain specified under **Device Management > Clean Access > Network Scanner > Options > “Login Configurations” Category > Preference Name** SMB. |
| CSCsi83381 | Yes | Clean Access presents an erroneous popup window when case-insensitive is enabled<br>When the Case-Insensitive option under a user role is enabled, the Clean Access system returns a popup window for users after they log in through the web interface. |
| CSCsi86205 | Yes | A kernel error results when a user manages a CAS with the “ifconfig eth1 down” command<br>The *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(1)* instructs users to enter the “ifconfig eth1 down” command before managing a CAS operating in Virtual Gateway mode. Cisco recommends physically disconnecting the CAS eth1 interface before adding the CAS to the CAM.<br>**Note** As of release 4.1(2), Cisco Clean Access system software addresses the “ifconfig eth1 down” command issue. |

*Table 13 List of Closed Caveats (Sheet 3 of 5)*

| | Software Release 4.1(2) | |
|---|---|---|
| **DDTS Number** | **Corrected** | **Caveat** |
| CSCsi90893 | Yes | No message goes to perfigo-log when user cannot add CAS to CAM<br>When a user exceeds the maximum number of CAS licenses or there is no CAS license present, the Clean Access system logs an entry in the event log, but not in the perfigo-log. For consistency and ease of troubleshooting, both logs should feature the event as most other CAS/CAM issues are already logged in both places. |
| CSCsi94224 | Yes | When setting up mapping rules for AD SSO where multiple VLANs are also added to the rule, the Clean Access system returns an Internal Server Error. |
| CSCsi96567 | Yes | Clean Access Agent will not recognize def date for Lavasoft Ad-aware<br>When using Clean Access to posture assess end clients for Lavasoft Ad-aware Personal SE 1.0.6, the Agent does not recognize the definition date of the anti-spyware definitions, and the requirement fails. |
| CSCsj00939 | Yes | Non-URL right frame content not displayed to end users in 4.1(1)<br>When using a Frame-based design for the login page, the content on the right frame is not displayed to the end user when the content is HTML or text entered in the CAM web console page. Although the preview displays correctly (as preview is from the CAM), the end user does not see the content on the right frame when it is presented from the CAS.<br>**Workaround options**<br>**1.** Use a URL on the right frame instead of HTML or text content.<br>**Note** You will need to open access to URL in the Unauthenticated role as documented.<br>**2.** Use a frameless approach. |
| CSCsj02240 | Yes | Windows Vista machines with a UK time zone designation fail the Windows Update check because of a different date format. |
| CSCsj05741 | Yes | Spaces in Distinguished Name (DN) cause LDAP authentication failure<br>When attempting an auth test with an LDAP provider, if the DN contains a space, the auth fails and returns a "LDAP: error code 49" message. The space can be anywhere in the DN, and is represented with the %20 escape character found in the perfigo-log.<br>**Note** There could also be a "," or other special character in the DN. For example, "CN= Doe, Jane". |
| CSCsj08474 | Yes | Release 4.0(x) does not allow same default gateway for multiple subnets<br>A check was added in release 4.0(x) to prevent administrators from specifying the same default gateway for more than one IP subnet range in the DHCP subnet list. This check can prove problematic for customers upgrading to 4.0(x) from 3.5.7 out of necessity to support Windows Vista because they must modify the setup to have a separate default gateway/VLAN for every /24 network, which can place additional routing burden on CAS. |

*Table 13 List of Closed Caveats (Sheet 4 of 5)*

| DDTS Number | Software Release 4.1(2) | |
|---|---|---|
| | **Corrected** | **Caveat** |
| CSCsj08522 | Yes | HA-CAM should check the database schema before sync to prevent corruption<br>When an administrator upgrades between various 4.x.x releases of CCA and leaves the secondary CAM up during upgrade, the database can become corrupted. |
| CSCsj09966 | Yes | Mac Agent displays "User Page is not configured" message if the CAS is unavailable<br>When using the Mac Agent, if you open the login window and then lose connectivity to the CAS, the Agent returns the following error if you click "Login" or "Cancel" before the status icon changes color:<br>"Cisco Clean Access Agent is not able to retrieve enough information to perform login. Please contact your network administrator to report this issue. [User Page is not configured]." |
| CSCsj10043 | Yes | The Mac Agent ignores the "Auto Popup Login Window" option when launched<br>When using the Mac OS Clean Access Agent with the "Auto Popup Login Window" option enabled on the CAM, the login window does not automatically appear the first time the user starts the Agent. The Agent login screen *does* appear as intended, however, in subsequent (re-connection) events or if the NIC interface goes down and then comes back up. |
| CSCsj13172 | Yes | CAS HA does not send link-detect ping from untrusted interface<br>After upgrading the CAM/CAS from 4.0(5) to 4.1(1), the secondary CAS no longer sends link-detect pings from the untrusted interface to support the high availability configuration. |
| CSCsj18047 | Yes | HTML tags entered in the text field for the "Blocked Access" page are not displayed. |
| CSCsj29701 | Yes | Agent may pop up again after login in OOB deployment<br>In an OOB deployment, the Agent login screen may pop up again after login when it gets a SWISS response between successful login and the CAMs authorization-to-access VLAN change. During this period, SWISS thinks Agent is not authenticated and continues sending UDP discovery packets while the CAM is about to set the access VLAN for the Agent. |
| CSCsj30409 | Yes | With VSClient (SSL VPN Client) the Clean Access Agent locks up when the connection is broken<br>With VSClient running and the physical connection fails or the client machine goes into hibernate mode and comes back up, the Clean Access Agent locks up until the connection is reset/reestablished. |

*Table 13 List of Closed Caveats (Sheet 5 of 5)*

| | Software Release 4.1(2) | |
|---|---|---|
| **DDTS Number** | **Corrected** | **Caveat** |
| CSCsj33552 | Yes | fostate.sh shows incorrect UI status<br>The fostate.sh command displays a result of "My node is standby without web console, peer node is active" when the web console is unavailable. This occurs after the standby CAM recovers from an active-active CAM HA status.<br>Steps to reproduce:<br>1. Unplug the heartbeat interface of the CAM HA pair.<br>2. Both CAMs become active.<br>3. Reconnect the heartbeat interface.<br>4. The new standby CAM will show "My node is standby without web console, peer node is active", but actually the web console is unavailable.<br>**Workaround**<br>Reboot the standby CAM to start the web console and correct the status. |
| CSCsj35621 | Yes | User SSO log-in process when booting up the client machine is much longer than subsequent (connection reestablishment) events<br>When a user starts a Windows client machine, the Clean Access Agent starts automatically, as it is already an item in the Windows startup folder. If SSO is enabled, the SSO process delays approximately 30 seconds before displaying remediation or successful login pages.<br>If the user becomes disconnected and reestablishes the connection without rebooting their machine, however, the same SSO login window delays only about 5 seconds before displaying subsequent screens. |
| CSCsj36082 | Yes | Device Filter assigns incorrect user role<br>With Device Filters configured for MAC addresses in the network, the Clean Access system assigns incorrect roles to user profiles. |
| CSCsj44812 | Yes | Frame-based login page re-display problem<br>When using frame-based login, if an error occurs (like invalid username or password), the page is re-displayed as a frameless, rather than frame-based, page. |
| CSCsj50387 | Yes | AD SSO service may stop on the CAS if the DC has dynamic IP<br>When the "Domain" option is selected for Windows Authentication, the CAS does not query DNS for the domain once the TGT is expired. If the DC IP address changes during this time, the ADSSO service fails because the CAS tries to connect using the old IP address. |
| CSCsj54337 | Yes | No guest access button for PocketPC devices using Clean Access<br>Clean Access (release 4.1(1)) displays the correct guest access web login page for PocketPC wireless users, but only text appears where the button to continue the authentication process should be, |

# Known Issues for Cisco NAC Appliance

This section describes known issues when integrating Cisco NAC Appliance:

- Known Issue with NAT/PAT Devices and L3 Deployments
- Known Issues with HP ProLiant DL140 G3 Servers
- Known Issue with NAC-3310 CD Installation
- Known Issues with NAC-3300 Series Appliances and Serial HA (Failover) Connection
- Known Issues with Switches
- Known Issue with Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs)
- Known Issues with Broadcom NIC 5702/5703/5704 Chipsets
- Known Issue with MSI Agent Installer File Name
- Known Issue with Windows 98/ME/2000 and Windows Script 5.6

## Known Issue with NAT/PAT Devices and L3 Deployments

Cisco NAC Appliance does not support the use of a NAT/PAT device, such as a Firewall/Router, placed between users and the Clean Access Server in Layer 3 deployments. In Layer 3 deployments, where users are multiple hops away from the Clean Access Server, the CAS needs a unique user IP address for each client on which NAC enforcement is performed.

If NAT/PAT is used between the users and the CAS, all users appear to originate from the same IP address (the NAT/PATed IP) from a CAS perspective. Hence, only the first user goes through NAC enforcement, and after this user is certified, all remaining users are exempted from NAC enforcement.

## Known Issues with HP ProLiant DL140 G3 Servers

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

## Known Issue with NAC-3310 CD Installation

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

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

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

The standard procedure asks you to press "Enter" or, if installing via serial console connection, enter **serial** at the "boot:" prompt, For release 4.1(2) and later, however, NAC-3310 customers are required enter one of the following, instead:

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

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

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

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

## Known Issues with Switches

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

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

Due to changes in DHCP server operation with Cisco NAC Appliance release 4.0(2) and above, 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 section "Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs) and DHCP" in *Switch Support for Cisco NAC Appliance* for detailed instructions.

**Note** For further details on configuring DHCP options, see the *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(2)*.

## Known Issues with Broadcom NIC 5702/5703/5704 Chipsets

Customers running Cisco NAC Appliance release 4.1(2) and later on servers with 5702/5703/5704 Broadcom NIC cards may be impacted by caveat CSCsd74376. Server models with Broadcom 5702/5703/5704 NIC cards may include: Dell PowerEdge 850, CCA-3140-H1, HP ProLiant DL140 G2/ DL360/DL380. This issue involves the repeated resetting of the Broadcom NIC cards. The NIC cards do not recover from some of the resets causing the machine to become unreachable via the network.

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

## Known Issue with MSI Agent Installer File Name

The Clean Access Agent stub installer (either MSI or EXE) allows administrators to install and update the Clean Access Agent on client machines for users without administrator privileges . The Clean Access Agent MSI (Microsoft Installer format) file can be obtained in one of the following ways:

- Download and unzip the Clean Access Agent MSI file (CCAAgentMSIStub.zip) from the Clean Access Manager by clicking the **CCAA MSI Stub** download button from the **Device Management > Clean Access > Clean Access Agent > Installation** page of the CAM web console.
- Download the Clean Access Agent MSI file (CCAAgent-<*version*>.msi) from the Cisco Software Download site at http://www.cisco.com/pcgi-bin/tablebuild.pl/cca-agent.

**Caution** **Make sure the .msi file is named "CCAAgent.msi" before installing it**, particularly if downloading the file from Cisco Secure Software (where the version is specified in the download filename). 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.

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

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

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

**Win 98, ME, NT 4.0:**

Filename: scr56en.exe

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

**Win 2000, XP:**

Filename: scripten.exe

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

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

# New Installation of Release 4.1.2.1

⚠ **Caution** **Release 4.1.2.1 is the minimum mandatory version for all appliances**, and is required to support HA-CAS pairs. Refer to CSCsk24551, page 46 for additional details. For compatibility with CAM/CAS appliances running 4.1.2.1, you must use the standard product upgrade file to upgrade the NAC network module to 4.1.2.1.

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

If performing upgrade, refer to the instructions in Upgrading to 4.1.2.1, page 56.

**For New Installation:**

1. If you are going to perform a new installation but are running a previous version of Cisco Clean Access, back up your current Clean Access Manager installation and save the snapshot on your local computer, as described in General Preparation for Upgrade, page 58.
2. Follow the instructions on your welcome letter to obtain a license file for your installation. See Cisco NAC Appliance Service Contract/Licensing Support, page 2 for details. (If you are evaluating Cisco Clean Access, visit http://www.cisco.com/go/license/public to obtain an evaluation license.)
3. Install the latest version of 4.1(2) (e.g., release 4.1.2.1) on each Clean Access Server and Clean Access Manager, as follows:
   - Log in to Cisco Secure Software and download the latest 4.1.2.x .ISO image from http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml and burn it as a bootable disk to a CD-R.
   - Insert the CD into the CD-ROM drive of each installation server and follow the instructions in the auto-run installer.

**Warning** **If you are installing new system software from a CD-ROM (rather than performing an upgrade) on a NAC-3310 (both MANAGER and SERVER), you must enter `DL140` or `serial_DL140` at the "boot:" prompt. For details, see Important Installation Information for NAC-3310, page 4.**

4. After software installation, access the Clean Access Manager web admin console by opening a web browser and typing the IP address of the CAM as the URL. The Clean Access Manager License Form will appear the first time you do this to prompt you to install your FlexLM license files.
5. Install a valid FlexLM license file for the Clean Access Manager (either evaluation, starter kit, or individual license). You should have already acquired license files as described in Cisco NAC Appliance Service Contract/Licensing Support, page 2.
6. At the admin login prompt, login with the default user name and password **`admin/cisco123`** or with the web console username and password you configured when you installed the Clean Access Manager.
7. In the web console, navigate to **Administration > CCA Manager > Licensing** if you need to install any additional FlexLM license files for your Clean Access Servers.
8. For detailed software installation steps and further steps for adding the Clean Access Server(s) to the Clean Access Manager and performing basic configuration, refer to the following guides:
   - *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(2)*

- *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(2)*

**Note** Clean Access Manager 4.1.2.1 is bundled with Clean Access Agent 4.1.2.1.

# Upgrading to 4.1.2.1

**Caution** **Release 4.1.2.1 is the minimum mandatory version for all appliances**, and is required to support HA-CAS pairs. Refer to CSCsk24551, page 46 for additional details. For compatibility with CAM/CAS appliances running 4.1.2.1, you must use the standard product upgrade file to upgrade the NAC network module to 4.1.2.1.

This section provides instructions for how to upgrade your existing Cisco Clean Access system to release 4.1.2.1.

Refer to the following general information prior to upgrade:

- Notes on 4.1.2.1 Upgrade
- Settings That May Change With Upgrade
- General Preparation for Upgrade

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

- In-Place Upgrade from 3.5(7)+ to 4.1.2.1—Standalone Machines
- In-Place Upgrade from 3.5(7)+ to 4.1.2.1—HA-Pairs
- Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+—Standalone Machines
- Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)—HA Pairs

If you need to perform a fresh installation of the software, refer instead to New Installation of Release 4.1.2.1, page 55.

If you need to upgrade from a much older version of Cisco Clean Access, you may need to perform an interim upgrade to a version that is supported for upgrade to 4.1.2.1. In this case, refer to the applicable Release Notes for upgrade instructions for the interim release. Cisco recommends always testing new releases on a different system first before upgrading your production system.

## Notes on 4.1.2.1 Upgrade

**Caution** **Release 4.1.2.1 is the minimum mandatory version for all appliances**, and is required to support HA-CAS pairs. Refer to CSCsk24551, page 46 for additional details. For compatibility with CAM/CAS appliances running 4.1.2.1, you must use the standard product upgrade file to upgrade the NAC network module to 4.1.2.1.

If planning to upgrade to Cisco NAC Appliance (Cisco Clean Access) 4.1.2.1 ED, note the following:

- Only releases 4.1(2)+ and 4.1(1)+ can be installed on Cisco NAC Appliance 3300 Series platforms.

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

- If you are deploying one or more Cisco NAC network modules in your network, you must upgrade existing CAM/CAS appliances to release 4.1(2) or later for compatibility.
- If you are supporting 64-bit Windows Vista or Windows XP client systems, you must upgrade your CAM, CAS, NAC network module, and Agent components from 4.1(2) to 4.1.2.1. Because Cisco NAC Appliance provides authentication-only support for 64-bit operating system Agents, nessus scanning via the Clean Access Agent does not perform remediation on the client machine.
- Windows Vista is supported starting from release 4.1(1) and version 4.1.1.0 of the Agent, with the exception of the 4.1.2.2, 4.1.2.1, 4.1.2.0, and 4.1.1.0 Agent Stub installers, which are not supported on Windows Vista.
- Cisco NAC Appliance (Cisco Clean Access) release 4.1.2.1 ED is a software upgrade release with Early Deployment status.
- Cisco recommends using the console/SSH upgrade procedure to upgrade from release 3.6(x), 4.0(x), or 4.1(0)+, or 4.1(2) to release 4.1.2.1. See Console/SSH Upgrade—Standalone Machines, page 74.
- When upgrading from 3.6(x)/4.0(x) to the latest 4.1(x) release:
  - You can only perform web console upgrade on standalone non-HA CAM machines if they have already been patched for caveat CSCsg24153.
  - If the system has not already been patched, upgrade all your machines via console/SSH.
  - Standalone CAS machines must still be upgraded using the console/SSH upgrade procedure.

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

**Warning** **Web upgrade is NOT supported for software upgrade of HA-CAM pairs. Upgrade of high availability Clean Access Manager pairs must always be performed via console as described in Console/SSH Instructions for Upgrading HA-CAM and HA-CAS Pairs, page 79.**

- To upgrade from release 3.5(x) to 4.1.2.1, use the in-place upgrade procedure, in which the installation CD is used to upgrade each machine in place. For standalone systems, refer to In-Place Upgrade from 3.5(7)+ to 4.1.2.1—Standalone Machines, page 59. For HA systems, refer to In-Place Upgrade from 3.5(7)+ to 4.1.2.1—HA-Pairs, page 63
- **Read and review the installation or upgrade instructions completely before starting. The 3.5(x)+ to 4.1.2.1 in-place upgrade procedure is different from minor release upgrades and requires physical CD installation.**
- **If you have existing users, test the ED release in your lab environment first and complete a pilot phase prior to production deployment.**

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

## Settings That May Change With Upgrade

- **5702/5703/5704 Broadcom NIC chipsets**: If your system uses 5702/5703/5704 Broadcom NIC chipsets, and you are upgrading from 4.1(1)+, 4.1(0)+, 4.0(x), or 3.6(x), or 3.5(x), you will need to perform a firmware upgrade from HP. See Known Issues with Broadcom NIC 5702/5703/5704 Chipsets, page 53 for details.
- **Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs)**: If using the CAS as a DHCP server in conjunction with Airespace WLCs, you may need to configure DHCP options as described in Known Issue with Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs), page 53.
- **OOB Deployments**: Because Cisco NAC Appliance can control switch trunk ports for OOB (starting from release 3.6(1) +), please ensure the uplink ports for controlled switches are configured as "uncontrolled" ports either before or after upgrade.

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

- **DHCP Options**: When upgrading from 3.5/3.6 to 4.1(2) and later, any existing DHCP options on the CAS are not retained. Administrators must re-enter any previously configured DHCP options using the newly-enhanced **Global Options** page.
- **SNMP Settings**: When upgrading from 3.5 to 4.1(2) and later, any existing SNMP traps configured on the CAM are not retained. Administrators must re-enter any previously configured SNMP settings using the newly-enhanced **SNMP** page.

## General Preparation for Upgrade

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

- **Homogenous Clean Access Server Software Support**

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

  Depending on the number of Clean Access Servers you have, the upgrade process should be scheduled as downtime. For minor release upgrades (e.g. 4.1(2) to 4.1.2.x), our estimates suggest that it takes approximately 15 minutes for the Clean Access Manager upgrade and 10 minutes for each Clean Access Server upgrade. Use this approximation to estimate your downtime window.

**Note** Allow more time for a major in-place upgrade procedure (3.5(x)+ to 4.1(2)+ for example), particularly for high-availability (failover) pairs of machines.

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

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

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

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

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

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

  For additional safekeeping, Cisco recommends manually backing up your current Clean Access Manager installation (using **Administration > Backup**) both before and after the upgrade and to save the snapshot on your local computer. Backing up prior to upgrade enables you to revert to your previous release database should you encounter problems during upgrade. Backing up immediately following upgrade preserves your upgraded tables and provides a baseline of your 4.1(2) and later database. After the migration is completed, go to the database backup page (**Administration > Backup**) in the CAM web console. Download and then delete all earlier snapshots from there as they are no longer compatible. See Create CAM DB Backup Snapshot, page 69 for details.

**Warning** **You cannot restore a CAM database from a snapshot created using a different release. For example, you cannot restore a 4.1(1) or earlier database snapshot to a 4.1(2) and later CAM.**

- **Software Downgrade**

  Once you have upgraded your software to 4.1.2.1, if you wish to revert to your previous version of CCA software, you will need to reinstall the previous CCA version from the CD and recover your configuration based on the backup you performed prior to upgrading to 4.1.2.1.

- **Passwords**

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

# In-Place Upgrade from 3.5(7)+ to 4.1.2.1—Standalone Machines

This section describes the in-place upgrade procedure for upgrading your standalone CAM/CAS from release 3.5(7)/3.5(8)/3.5(9)/3.5(10)/3.5(11)+ to the latest 4.1.2.1 release. If you have high-availability (HA) pairs of CAM or CAS servers, refer instead to In-Place Upgrade from 3.5(7)+ to 4.1.2.1—HA-Pairs, page 63.

**Note** Review the following sections before proceeding with the in-place upgrade instructions:

- Upgrading to 4.1.2.1, page 56
- Settings That May Change With Upgrade, page 58
- General Preparation for Upgrade, page 58

### In-Place Upgrade Summary

The Cisco Clean Access 4.1.2.1 upgrade will create a complete snapshot of the configuration of your existing deployment, including failover information.

The Cisco Clean Access 4.1.2.1 upgrade will not restore local user directories, log files, manually created database snapshots, or nightly database snapshots older than last nights. Any of the above files that are valuable must be backed up separately prior to upgrading.

The upgrade automatically determines from the upgrade snapshot whether the machine is a CAS or a CAM as well as all normal configuration utility settings, such as IP address.

The upgrade will create a log of its activities in the usual upgrade.html and details.html files.

The upgrade will print a warning and exit if too many large files are stored in your Clean Access Manager database. The limit is currently 90 MB for machines with 256 MB of memory, or available memory/2 for machines with more than 256 MB of memory.

### Summary of Steps for In-Place Upgrade (Standalone Machines)

The sequence of steps for in-place upgrade is as follows:

1. Create the Installation CD
2. Mount the CD-ROM and Run the Upgrade File
3. Swap Ethernet Cables (if Necessary)
4. Complete the In-Place Upgrade

## Create the Installation CD

**Step 1** If you already have the 4.1.2.1 installation CD shipped with your deployment of Cisco NAC Appliance, continue to Mount the CD-ROM and Run the Upgrade File, page 60.

**Step 2** If the 4.1.2.1 installation CD is not shipped with your deployment of Cisco NAC Appliance, you can easily create your own installation CD by logging into Cisco Downloads (http://www.cisco.com/kobayashi/sw-center/sw-ciscosecure.shtml).

**Step 3** Click the link for Cisco NAC Appliance Software. On the Cisco Secure Software page for Cisco NAC Appliance, click the link for the appropriate release. Download the following file to a local computer (for example, **`cca-4.1_x_y-K9.iso`**):

**cca-4.1_2_1-K9.iso**

**Step 4** Use a CD burning tool on your local computer to burn this ISO file as a bootable CD-ROM.

## Mount the CD-ROM and Run the Upgrade File

Once you have a 4.1.2.1 product or installation CD, perform the following steps on each CAM and CAS to upgrade each machine from 3.5(7)/3.5(8)/3.5(9)/3.5(10)/3.5(11) to the latest 4.1.2.1 release.

⚠ **Caution** The Clean Access Manager and Server software is not intended to coexist with other software or data on the target machine. The installation process formats and partitions the target hard drive, destroying any data or software on the drive. Before starting the installation, make sure that the target computer does not contain any data or applications that you need to keep.

**Step 5** For each machine to upgrade (either Clean Access Manager or Clean Access Server), connect to the machine either via console or using Putty or SSH.

**a.** Connect to the machine.

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

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

**Step 6** **Insert the 4.1.2.1 installation CD into the CD-ROM drive of the machine to be upgraded.**

**Step 7** Mount the CD-ROM on the machine to be installed (use the command: `mount /dev/cdrom /<mountpoint directory>`), for example:

```
mount /dev/cdrom /mnt
```

**Step 8** Change to the mountpoint directory:

```
cd /mnt
```

**Step 9** Run the upgrade file:

```
./upgrade.sh
```

**Note** For in-place upgrade, the **`upgrade.sh`** command must be lower case.

You will see the following banner:

```
[root@<ccahostname> root]# /mnt/upgrade.sh
Upgrade works for 3.5.7-3.5.11, continuing
############################################################
#         Welcome to Cisco Clean Access 4.1 upgrade        #
############################################################
The Cisco Clean Access 4.1 upgrade.
The 4.1 upgrade is different from previous upgrades. Please
be sure to read the documentation before proceeding

The Cisco Clean Access 4.1 upgrade will create a complete
snapshot of the configuration of your existing deployment,
including failover information.

The Cisco Clean Access 4.1 upgrade will not restore local
user directories, log files, manually created database snapshots,
or nightly database snapshots older than last nights. Any of the above
files that are valuable must be backed up separately prior to upgrading.
```

**Step 10** At the following prompt, type **`y`** to continue with the upgrade:

```
Continue with upgrade? (y/n)? [y]
```

**Step 11** The upgrade proceeds and the system performs a reboot:

```
Upgrade continuing
Backing up <“Clean Access Manager” or “Clean Access Server IP”>
Backup complete, system will reboot in 5 seconds
```

**Step 12** The Cisco Clean Access Installer Welcome Screen then appears after the system restarts. At the `boot:` prompt, press Enter if connected directly to the server machine, or type **`serial`** and press Enter if connected serially to the machine:

```
Cisco Clean Access 4.1-2 Installer (C) 2007 Cisco Systems, Inc.
                Welcome to the Cisco Clean Access 4.1-2 Installer!

 - To install a Cisco Clean Access device, press the <ENTER> key.
 - To install a Cisco Clean Access device over a serial console,
 enter serial at the boot prompt and press the <ENTER> key.
boot:
```

**Step 13** The 4.1.2.1 upgrade then automatically proceeds for approximately 2-5 minutes and the system will reboot one or more times. The display will show the Cisco Clean Access System Installer formatting the hard drive and installing each package.

## Swap Ethernet Cables (if Necessary)

**Step 14** Before the next automatic reboot, a warning message may be displayed if the new kernel has detected that NIC cards have been re-ordered. If this occurs, the Ethernet cables for eth0 and eth1 must be swapped on the machine. After swapping cables, press the Enter key and proceed with the installation as usual. NIC card re-ordering only occurs when upgrading from previous 3.5 installations; it will only occur only once and only during this stage of the installation.

```
CCA has detected a change in your networking hardware configuration.
Please switch the network cables between eth0 and eth1.

Press [ENTER] to continue...
```

**Step 15** After pressing Enter on the previous step, the machine will reboot, then reboot again, then come up normally.

## Complete the In-Place Upgrade

**Step 16** The 4.1.2.1 upgrade is successfully installed when the installation CD is ejected from the machine and the login prompt appears:

```
<ccahostname> login:
```

**Step 17** If you want to verify the software version, machine (CAM or CAS), and version date, you can login as user **`root`** with root user password and type the following command:

```
[root@<ccahostname> ~]# cat /perfigo/build
```

**Step 18** This completes the 4.1.2.1 upgrade procedure. Repeat the procedure for each machine to be upgraded to 4.1.2.1.

**Note** After performing 3.5(x)-to-4.1.2.1 migration, the very first time you log into the 4.1.2.1 CAM web console, the CAM will attempt an automated Cisco Update to populate the AV/AS tables in the database. A popup dialog with following message will appear:

```
"The system detects that it has just been upgraded to a newer version. It is now trying to
connect to the Cisco server to get the checks/rules and AV/AS support list update. It
might take a few minutes."
```

If the automated update fails (for example, due to incorrect proxy settings on your CAM), you will be prompted to perform Cisco Updates manually from **Device Management > Clean Access > Clean Access Agent > Updates**. A Cisco Update must be performed (whether automated or manual) before any new AV/AS rules can be configured.

# In-Place Upgrade from 3.5(7)+ to 4.1.2.1—HA-Pairs

This section describes the in-place upgrade procedure for upgrading high-availability (HA) pairs of CAM or CAS servers from release 3.5(7)/3.5(8)/3.5(9)/3.5(10)/3.5(11)+ to the latest 4.1.2.1 release.

If you have standalone CAM/CAS servers, refer instead to In-Place Upgrade from 3.5(7)+ to 4.1.2.1—Standalone Machines, page 59.

**Note** Review the following sections before proceeding with the in-place HA upgrade instructions:

- Upgrading to 4.1.2.1, page 56
- Settings That May Change With Upgrade, page 58
- General Preparation for Upgrade, page 58
- Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)—HA Pairs, page 77 (general instructions)

### Summary of Steps for In-Place Upgrade (HA Pairs)

The sequence of steps for HA in-place upgrade is as follows:

1. Prepare for HA Upgrade
2. Determine Active and Standby Machines
3. Shut Down Standby Machine and Upgrade Active Machine In-Place
4. Shut Down Active Machine and Upgrade Standby Machine In-Place
5. Complete the HA In-Place Upgrade

**Warning** **Make sure to follow this procedure to prevent the database from getting out of sync.**

## Prepare for HA Upgrade

**Step 1** Ensure you already have the latest 4.1.2.1 product CD. If not, follow the steps to Create the Installation CD, page 60.

**Step 2** Connect to each machine in the failover pair. Login as the `root` user with the root password (default is `cisco123`).

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

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

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

## Determine Active and Standby Machines

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

**Note** The **`fostate.sh`** command (failover state) is part of the upgrade script (starting from 3.5(3)+), and is located under **`/perfigo/common/bin/fostate.sh`** (from 4.0.2+) and/or under each upgrade directory (i.e. **`/store/cca_upgrade-<version>/`**). If needed, you can use **`locate fostate.sh`** to find the exact path of the command (you may be prompted to run the **`updatedb`** command first).

**a.** Locate the failover state command (fostate.sh) by changing directory to **`/perfigo/common/bin/`** or **`/store/<any post-3.5.3 upgrade directory>`** on each machine, for example:

```
cd /store/cca_upgrade_3.5.x
```

**b.** Perform **ls** to verify fostate.sh is in the directory.

**c.** Run the command on each machine:

```
./fostate.sh
```

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

## Shut Down Standby Machine and Upgrade Active Machine In-Place

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

```
shutdown -h now
```

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

**Step 6** **Insert the 4.1.2.1 installation CD into the CD-ROM drive of the Active machine to be upgraded.**

**Step 7** Mount the CD-ROM on the Active machine (use the command: `mount /dev/cdrom /<mountpoint directory>`), for example:

```
mount /dev/cdrom /mnt
```

**Step 8** Change to the mountpoint directory:

```
cd /mnt
```

**Step 9** Run the upgrade file:

```
./upgrade.sh
```

**Note** For in-place upgrade, the **`upgrade.sh`** command must be lower case.

You will see the following banner:

```
[root@<ccahostname> root]# /mnt/upgrade.sh
Upgrade works for 3.5.7-3.5.11, continuing
############################################################
#         Welcome to Cisco Clean Access 4.1 upgrade        #
```

```
############################################################
The Cisco Clean Access 4.1 upgrade.
The 4.1 upgrade is different from previous upgrades. Please
be sure to read the documentation before proceeding

The Cisco Clean Access 4.1 upgrade will create a complete
snapshot of the configuration of your existing deployment,
including failover information.

The Cisco Clean Access 4.1 upgrade will not restore local
user directories, log files, manually created database snapshots,
or nightly database snapshots older than last nights. Any of the above
files that are valuable must be backed up separately prior to upgrading.
```

**Step 10** At the following prompt, type **y** to continue with the upgrade:

```
Continue with upgrade? (y/n)? [y]
```

**Step 11** The upgrade proceeds and the system performs a reboot. The upgrade script performs the backup then the regular install takes place.

```
Upgrade continuing
Backing up <"Clean Access Manager" or "Clean Access Server IP">
Backup complete, system will reboot in 5 seconds
```

**Step 12** The Cisco Clean Access Installer Welcome Screen then appears after the system restarts. At the "`boot`:" prompt, press Enter if connected directly to the server machine, or type **`serial`** and press Enter if connected serially to the machine:

```
Cisco Clean Access 4.1-2 Installer (C) 2007 Cisco Systems, Inc.
                Welcome to the Cisco Clean Access 4.1-2 Installer!

 - To install a Cisco Clean Access device, press the <ENTER> key.
 - To install a Cisco Clean Access device over a serial console,
 enter serial at the boot prompt and press the <ENTER> key.
boot:
```

**Step 13** The 4.1.2.1 upgrade then automatically proceeds for approximately 2-5 minutes and the system will reboot one or more times. The display will show the Cisco Clean Access System Installer formatting the hard drive and installing each package.

**Step 14** If a warning displays because NIC cards have been re-ordered, follow the instructions for Swap Ethernet Cables (if Necessary), page 62.

**Note** For CAM upgrade, the 4.1.2.1 upgrade script automatically upgrades the Clean Access Agent files inside the CAM to version 4.1.2.1.

**Step 15** After pressing Enter on the previous step, the machine will reboot, then reboot again, then come up normally with the following messages:

For an upgraded Active HA-CAM:

```
Starting perfigo: Starting High-Availability services:
[OK]
Please wait while bringing up service IP.
Heartbeat service is running.
Service IP is up on local node.
[OK]
Fedora Core release 4 (Stentz)
Kernel 2.6.11-perfigo on an i686
camanager1 login:
```

For an upgraded Active HA-CAS:

```
    Starting perfigo: Starting IPSec...
    click: starting router thread pid 2826 (f7576800)
    Starting High-Availability services:
    [OK]
    [OK]
    Fedora Core release 4 (Stentz)
    Kernel 2.6.11-perfigo on an i686
    caserver1 login:
```

**Step 16** At the next prompt, run the fostate.sh command again to verify that the failover state of the machine is "My node is active, peer node is dead":

```
[root@<ccahostname> ~]# /perfigo/common/bin/fostate.sh
My node is active, peer node is dead
```

## Shut Down Active Machine and Upgrade Standby Machine In-Place

**Step 17** After the upgrade is completed, shut down the active box (e.g. `camanager1` or `caserver1` in the example) by entering the following command via the console or SSH terminal:

```
    shutdown -h now
```

**Step 18** Wait until the active box is done shutting down:

```
Stopping High-Availability services:
[OK]
```

**Step 19** Power on the standby box and ensure it boots up and is operating normally.

**Step 20** **After you boot up the standby box, Insert the 4.1.2.1 installation CD into the CD-ROM drive of the standby machine to be upgraded.**

**Warning** **To ensure the standby box does not try to boot from the CD, do not insert the CD into the CD-ROM drive until the standby box has completely booted up.**

**Step 21** Mount the CD-ROM on the standby machine (use the command: `mount /dev/cdrom /<mountpoint directory>`), for example:

```
    mount /dev/cdrom /mnt
```

**Step 22** Change to the mountpoint directory:

```
    cd /mnt
```

**Step 23** Run the upgrade file:

```
    ./upgrade.sh
```

**Note** For in-place upgrade, the **`upgrade.sh`** command must be lower case.

You will see the following banner:

```
[root@<ccahostname> root]# /mnt/upgrade.sh
Upgrade works for 3.5.7-3.5.11, continuing
############################################################
#         Welcome to Cisco Clean Access 4.1 upgrade        #
############################################################
The Cisco Clean Access 4.1 upgrade.
The 4.1 upgrade is different from previous upgrades. Please
```

```
be sure to read the documentation before proceeding

The Cisco Clean Access 4.1 upgrade will create a complete
snapshot of the configuration of your existing deployment,
including failover information.

The Cisco Clean Access 4.1 upgrade will not restore local
user directories, log files, manually created database snapshots,
or nightly database snapshots older than last nights. Any of the above
files that are valuable must be backed up separately prior to upgrading.
```

**Step 24** At the following prompt, type **y** to continue with the upgrade:

```
Continue with upgrade? (y/n)? [y]
```

**Step 25** The upgrade proceeds and the system performs a reboot. The upgrade script performs the backup then the regular install takes place.

```
Upgrade continuing
Backing up <Clean Access Manager or Clean Access Server IP>
Backup complete, system will reboot in 5 seconds
```

**Step 26** The Cisco Clean Access Installer Welcome Screen then appears after the system restarts. At the "`boot`:" prompt, press Enter if connected directly to the server machine, or type **`serial`** and press Enter if connected serially to the machine:

```
Cisco Clean Access 4.1-2 Installer (C) 2007 Cisco Systems, Inc.
                Welcome to the Cisco Clean Access 4.1-2 Installer!

 - To install a Cisco Clean Access device, press the <ENTER> key.
 - To install a Cisco Clean Access device over a serial console,
 enter serial at the boot prompt and press the <ENTER> key.
boot:
```

**Step 27** The 4.1.2.1 upgrade then automatically proceeds for approximately 2-5 minutes and the system will reboot one or more times. The display will show the Cisco Clean Access System Installer formatting the hard drive and installing each package.

**Step 28** If a warning displays because NIC cards have been re-ordered, follow the instructions for Swap Ethernet Cables (if Necessary), page 62.

**Note** For CAM upgrade, the 4.1.2.1 upgrade script automatically upgrades the Clean Access Agent files inside the CAM to version 4.1.2.1.

**Step 29** The system then reboots. When the system restarts, you will see the following messages:

For an upgraded Standby HA-CAM:

```
Starting perfigo: Starting High-Availability services:
[OK]
Please wait while bringing up service IP.
Heartbeat service is running.
Service IP is up on local node.
[OK]
Fedora Core release 4 (Stentz)
Kernel 2.6.11-perfigo on an i686
camanager2 login:
```

For an upgraded Standby HA-CAS:

```
Starting perfigo: Starting IPSec...
click: starting router thread pid 2826 (f7576800)
```

```
    Starting High-Availability services:
    [OK]
    [OK]
    Fedora Core release 4 (Stentz)
    Kernel 2.6.11-perfigo on an i686
    caserver2 login:
```

**Step 30** At the next prompt, run the fostate command again to verify that the failover state of the machine is “My node is active, peer node is dead”:

```
[root@<ccahostname> ~]# /perfigo/common/bin/fostate.sh
My node is active, peer node is dead
```

## Complete the HA In-Place Upgrade

**Step 31** Shut down the standby box (e.g. `camanager2` or `caserver2` in the example) by entering the following command via the SSH terminal:

```
    shutdown -h now
```

**Step 32** Power up the active box. Wait until it is running normally and connection to the web console is possible.

**Step 33** Power up the standby box.

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

**Step 34** Login as the root user on the standby box and run the fostate command again to verify that the failover state of the machine is “My node is standby, peer node is active”:

```
[root@<ccahostname> ~]# /perfigo/common/bin/fostate.sh
My node is standby, peer node is active
```

**Note** After performing 3.5(x)-to-4.1.2.1 migration, the very first time you log into the 4.1.2.1 CAM web console, the CAM will attempt an automated Cisco Update to populate the AV/AS tables in the database. A popup dialog with following message will appear:

```
"The system detects that it has just been upgraded to a newer version. It is now trying to
connect to the Cisco server to get the checks/rules and AV/AS support list update. It
might take a few minutes."
```

If the automated update fails (for example, due to incorrect proxy settings on your CAM), you will be prompted to perform Cisco Updates manually from **Device Management > Clean Access > Clean Access Agent > Updates**. A Cisco Update must be performed (whether automated or manual) before any new AV/AS rules can be configured.

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

This section describes the upgrade procedure for upgrading your standalone CAM/CAS machine from release 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2) to the latest 4.1.2.1 release. You can upgrade 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2) standalone machines to the latest 4.1.2.1 release using one of the following two methods:

- Web Console Upgrade—Standalone Machines, page 71
- Console/SSH Upgrade—Standalone Machines, page 74

**Note**

- If upgrading high-availability (HA) pairs of CAM or CAS servers running 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2), refer instead to Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)—HA Pairs, page 77.
- If upgrading your system from release 3.5(x), refer instead to In-Place Upgrade from 3.5(7)+ to 4.1.2.1—Standalone Machines, page 59.

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

- Upgrading to 4.1.2.1, page 56
- Settings That May Change With Upgrade, page 58
- General Preparation for Upgrade, page 58

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

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

1. Create CAM DB Backup Snapshot, page 69
2. Download the Upgrade File, page 70
3. Web Console Upgrade—Standalone Machines or Console/SSH Upgrade—Standalone Machines, page 74

## Create CAM DB Backup Snapshot

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

Note that Cisco NAC Appliance automatically creates daily snapshots of the CAM database and preserves the most recent from the last 30 days (starting from release 3.5(3)). It also automatically creates snapshots before and after software upgrades and failover events. For upgrades and failovers, only the last 5 backup snapshots are kept. (For further details, see “Database Recovery Tool” in the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(2)*.

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

To create a manual backup snapshot:

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

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

**Step 3** Click **Create Snapshot**. The CAM generates a snapshot file and adds it to the snapshot list at the bottom of the page. The file physically resides on the CAM machine for archiving purposes. The Version field and the filename display the software version of the snapshot for convenience (e.g. 04_15_07-14-58_snapshot_**VER_4.1.2.0.**gz).

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

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

## Download the Upgrade File

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

**Step 1** Log into Cisco Downloads (http://www.cisco.com/kobayashi/sw-center/sw-ciscosecure.shtml), navigate to the Network Admission Control section of the page, and click the link for Cisco Clean Access Software.

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

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

**Note** For patch upgrades, replace the .x in the file name with the minor release version numbers to which you are upgrading, for example, cca_upgrade-4.1.2.1.tar.gz.

## Web Console Upgrade—Standalone Machines

**Note** Cisco recommends using console/SSH to upgrade your machines from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2) to 4.1.2.1. See Console/SSH Upgrade—Standalone Machines, page 74.

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

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

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

**Warning** **Web upgrade is NOT supported for software upgrade of HA-CAM pairs. Upgrade of high availability Clean Access Manager pairs must always be performed via console as described in Console/SSH Instructions for Upgrading HA-CAM and HA-CAS Pairs, page 79.**

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

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

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

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

**Note**

- For web upgrade, upgrade each CAS first, then the CAM.
- Release 3.6(0)/4.0(0)/4.1(0)/4.1(1)/4.1(2) or later must be installed and running on your CAM/CAS(es) before you can upgrade to release 4.1.2.1 via web console.
- Alternatively, you can always upgrade using the instructions in Console/SSH Upgrade—Standalone Machines, page 74.
- If upgrading failover pairs, refer to Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)—HA Pairs, page 77.

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

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

### Upgrade CAS from CAS Management Pages

You can upgrade your CAS from release 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2) to release 4.1.2.1 using web upgrade via the CAS management pages as described below or, if preferred, using the instructions for Upgrade CAS from CAS Direct Access Web Console, page 73.

**Step 1** Create CAM DB Backup Snapshot, page 69.

**Step 2** Download the Upgrade File, page 70.

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

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

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

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

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

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

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

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

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

**Step 8** Access the CAS management pages again and click the **Misc** tab. The new software version and date will be listed in the **Current Version** field. (See also Determining the Software Version, page 9.)

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

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

### Upgrade CAS from CAS Direct Access Web Console

You can upgrade the CAS from the CAS direct access web console using the following instructions. To upgrade the CASes from the CAM web console, see Upgrade CAS from CAS Management Pages, page 72.

**Step 1** Create CAM DB Backup Snapshot, page 69.

**Step 2** Download the Upgrade File, page 70.

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

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

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

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

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

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

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

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

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

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

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

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

### Upgrade CAM from CAM Web Console

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

**Warning** **Web upgrade is *not* supported for software upgrade of HA-CAM pairs. Upgrade of high availability Clean Access Manager pairs must always be performed via console as described in Console/SSH Instructions for Upgrading HA-CAM and HA-CAS Pairs, page 79.**

**Step 1** Create CAM DB Backup Snapshot, page 69.

**Step 2** Download the Upgrade File, page 70.

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

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

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

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

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

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

**Step 8** Access the CAM web console again. After login, you will see the new software version at the top right corner of the web console. (See also Determining the Software Version, page 9.)

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

## Console/SSH Upgrade—Standalone Machines

This section describes the standard console/SSH upgrade procedure when upgrading your standalone CAM/CAS from release 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2) to the latest 4.1.2.1 release. For this procedure, you need to access the command line of the CAM or CAS machine using one of the following methods:

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

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

**Note**

- If upgrading high-availability (HA) pairs of CAM or CAS servers running 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2), refer instead to Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)—HA Pairs, page 77.
- If upgrading your system from 3.5(x), refer instead to In-Place Upgrade from 3.5(7)+ to 4.1.2.1—Standalone Machines, page 59.

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

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

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

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

**Note** Review the following before proceeding with the 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2) to 4.1.2.1 console/SSH upgrade instructions:

- Upgrading to 4.1.2.1, page 56
- Settings That May Change With Upgrade, page 58
- General Preparation for Upgrade, page 58

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

Steps are as follows:

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

### Download the Upgrade File and Copy to CAM/CAS

**Step 1** Create CAM DB Backup Snapshot, page 69.

**Step 2** Download the Upgrade File, page 70.

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

**If using WinSCP or SSH File Transfer:**

a. Copy **cca_upgrade-4.1.2.1.tar.gz** to the /store directory on the Clean Access Manager.

b. Copy **cca_upgrade-4.1.2.1.tar.gz** to the /store directory on *each* Clean Access Server.

**If using PSCP:**

a. Open a command prompt on your Windows computer.

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

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

```
pscp cca_upgrade-4.1.2.1.tar.gz root@ipaddress_manager:/store
```

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

```
pscp cca_upgrade-4.1.2.1.tar.gz root@ipaddress_server:/store
```

### Perform Console/SSH Upgrade on the CAM

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

**a.** Connect to the Clean Access Manager.

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

**c.** Change directory to /store:

```
cd /store
```

**d.** Uncompress the downloaded file:

```
tar xzvf cca_upgrade-4.1.2.1.tar.gz
```

**4.** Execute the upgrade process:

```
cd cca_upgrade-4.1.2.1
./UPGRADE.sh
```

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

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

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

**Note** For CAM upgrade, the 4.1.2.1 upgrade script automatically upgrades the Clean Access Agent files inside the CAM to version 4.1.2.1.

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

```
reboot
```

### Perform Console/SSH Upgrade on the CAS

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

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

**a.** Connect to the Clean Access Server.

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

c. Change directory to /store:

```
cd /store
```

d. Uncompress the downloaded file:

```
tar xzvf cca_upgrade-4.1.2.1.tar.gz
```

5. Execute the upgrade process:

```
cd cca_upgrade-4.1.2.1
./UPGRADE.sh
```

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

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

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

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

```
reboot
```

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

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

This section describes the upgrade procedure for upgrading high-availability (HA) pairs of CAM or CAS servers from release 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2) to the latest 4.1.2.1 release.

If you have standalone CAM/CAS servers, refer instead to Upgrading from 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2)+—Standalone Machines, page 69.

**Note** Your system must be on 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2) to use the upgrade procedure described in this section. If your system is on 3.5(x), refer instead to the instructions in In-Place Upgrade from 3.5(7)+ to 4.1.2.1—HA-Pairs, page 63.

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

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

**If you are using serial connection for HA, BIOS redirection to the serial port must be disabled for**

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

**Warning** **Web upgrade is NOT supported for software upgrade of HA-CAM pairs. Upgrade of high availability Clean Access Manager pairs must always be performed via console as described in Console/SSH Instructions for Upgrading HA-CAM and HA-CAS Pairs, page 79.**

**Note** Review the following before proceeding with the 3.6(x)/4.0(x)/4.1(0)+/4.1(1)+/4.1(2) to 4.1.2.1 HA upgrade instructions:

- Upgrading to 4.1.2.1, page 56
- Settings That May Change With Upgrade, page 58
- General Preparation for Upgrade, page 58

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

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

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

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

## Access Web Consoles for High Availability

### Determining Active and Standby CAM

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

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

### Determining Primary and Secondary CAM

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

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

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

### Determining Active and Standby CAS

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

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

### Determining Primary and Secondary CAS

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

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

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

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

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

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

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

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

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

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

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

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

**Step 2** Verify that the upgrade package is present in the /store directory on each machine. (Refer to Download the Upgrade File and Copy to CAM/CAS, page 75 for instructions.)

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

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

```
tar xzvf cca_upgrade-4.1.2.1.tar.gz
```

**b.** CD into the created "cca_upgrade-4.1.2.1" directory on each machine.

**c.** Run the following command on each machine:

```
./fostate.sh
```

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

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

- Access the web console as described in Access Web Consoles for High Availability, page 78, or
- SSH to the Service IP of the CAM/CAS pair, and type `ifconfig eth0`. The Service IP will always access the active CAM or CAS, with the other pair member acting as standby.

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

```
shutdown -h now
```

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

**Step 6** CD into the created "cca_upgrade-4.1.2.1" directory on the active box.

```
cd cca_upgrade-4.1.2.1
```

**Step 7** Run the following command on the active box:

```
./fostate.sh
```

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

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

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

b. From the untarred upgrade directory created on the active box (for example "cca_upgrade-4.1.2.1"), run the upgrade script on the active box:

```
./UPGRADE.sh
```

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

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

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

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

**Note** For CAM upgrade, the 4.1.2.1 upgrade script automatically upgrades the Clean Access Agent files inside the CAM to version 4.1.2.1.

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

```
shutdown -h now
```

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

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

**Step 12** Perform the upgrade to the standby box:

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

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

```
cd cca_upgrade-4.1.2.1
```

c. Run the upgrade script on the standby box:

```
./UPGRADE.sh
```

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

```
shutdown -h now
```

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

**Step 15** Power up the standby box.

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

# Troubleshooting

This section discusses the following:

- Creating CAM DB Snapshot
- Creating CAM/CAS Support Logs
- Recovering Root Password for CAM/CAS (Release 4.1(x)/4.0(x)/3.6(x))
- No Web Login Redirect / CAS Cannot Establish Secure Connection to CAM
- Agent Error: "Network Error SSL Certificate Rev Failed 12057"
- Clean Access Agent AV/AS Rule Troubleshooting
- Enable Debug Logging on the Clean Access Agent
- Troubleshooting Switch Support Issues
- Troubleshooting Network Card Driver Support Issues
- Other Troubleshooting Information

## Creating CAM DB Snapshot

See the instructions in Create CAM DB Backup Snapshot, page 69 for details.

## Creating CAM/CAS Support Logs

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

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

**Note**

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

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

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

1. Power up the machine.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- Invalid domain name
- CAM is unreachable

To identify common issues:

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

To resolve these issues:

1. Set the time on the CAM and CAS correctly first.
2. Regenerate the certificate on the CAS using the correct IP address or domain.
3. Reboot the CAS.
4. Regenerate the certificate on the CAM using the correct IP address or domain.
5. Reboot the CAM.

## Agent Error: "Network Error SSL Certificate Rev Failed 12057"

The "Network error: SSL certificate rev failed 12057" error can occur and prevent login for 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). Note that 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.
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.

## Clean Access Agent AV/AS Rule Troubleshooting

When troubleshooting AV/AS Rules:

- View administrator reports for the Clean Access Agent from **Device Management > Clean Access > Clean Access Agent > Reports** (see Clean Access Agent Versioning, page 10)
- 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 (see Cisco Clean Access Updates Versioning, page 10.
4. Product name and version of AV/AS software from the Add/Remove Program dialog box.
5. What is failing—AV/AS installation check or AV/AS update checks? What is the error message?
6. What is the current value of the AV/AS def date/version on the failing client machine?
7. What is the corresponding value of the AV/AS def date/version being checked for on the CAM? (See **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info**.)
8. If necessary, provide Agent debug logs as described in Enable Debug Logging on the Clean Access Agent, page 85.
9. If necessary, provide CAM support logs as described in Creating CAM/CAS Support Logs, page 82.

## Enable Debug Logging on the Clean Access Agent

For 4.1.x.x versions of the Clean Access Agent (and 4.0.x.x/3.6.1.0+), you can enable debug logging on the Agent by adding a LogLevel registry value on the client with value "debug," as described in the following sections:

- Generate Windows Agent Debug Log
- Generate Mac OS Agent Debug Log

You can copy this event log to include it in a customer support case.

### Generate Windows Agent Debug Log

**Note** For Windows Agents, the event log is created in the directory **%APPDATA%\CiscoCAA**, where %APPDATA% is the Windows environment variable.

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

**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, type: `%APPDATA%/CiscoCAA`

c. You will find event.log file there.

**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 Agent Debug Log

For Mac OS Agents (4.1.2.0+, 4.1.1.0+, and 4.1.0.0+), the Agent **event.log** file and **setting.plist** user preferences file are available under <*username*> **> Library > Application Support > Cisco Systems > CCAAgent.app**.

To view and specify the Agent LogLevel, however, you must access a global **setting.plist** system preferences file (which is *different* from the user-level **setting.plist** file).

**Note** Although any user on the Mac may view the LogLevel setting in the **setting.plist file**, you must be a superuser or root user on the machine to change LogLevel settings for the Mac OS Agent.

To view and/or change the Agent LogLevel:

**Step 1** Open the navigator pane and navigate to <*local drive ID*> > **Library > Application Support > Cisco Systems**.

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

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

**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 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 circumstances. 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.

## Troubleshooting Switch Support Issues

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

## Troubleshooting Network Card Driver Support Issues

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

## Other Troubleshooting Information

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

http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html

# Documentation Updates

*Table 14 Updates to Release Notes for Cisco NAC Appliance, Release 4.1(2) and Later*

| Date | Description |
|---|---|
| 4/10/08 | • Added note to CSCsk24551, page 46<br>• Updated template and boilerplate. |
| 4/7/08 | • Added a caution/footnote for release 4.1.2.1 as the minimum mandatory version for all appliances under :<br>– Cisco NAC Network Module, page 3<br>– NAC-3300 Series Appliances, page 3<br>– Software Compatibility Matrixes, page 6<br>– Enhancements in Release 4.1.2.1, page 11<br>– New Cisco NAC Network Module (NME-NAC-K9) Support, page 13<br>– New Installation of Release 4.1.2.1, page 55<br>– Upgrading to 4.1.2.1, page 56, and Notes on 4.1.2.1 Upgrade, page 56<br>• Added CSCsk24551 to Resolved Caveats - Release 4.1.2.1, page 45<br>• Updated upgrade references from 4.1(2) to 4.1.2.1 throughout .<br>• Removed reference to NAC-3350 and 2.1.7 under Cisco NAC Appliance Integration with Cisco NAC Profiler, page 4<br>• Updated hypertext links, boilerplate, trademark. |
| 1/30/08 | Applied new template and updated trademark information |
| 1/11/08 | Added caveat CSCsk05330 to Resolved Caveats - Release 4.1.2.1, page 45 |
| 12/11/07 | Converted to latest template and republished |
| 10/8/07 | Updates for Agent version 4.1.2.2<br>• Updated Software Compatibility Matrixes, page 6<br>• Updated Enhancements in Release 4.1.2.1, page 11<br>• Updated Clean Access Supported AV/AS Product List, page 16<br>• Updated Supported AV/AS Product List Version Summary, page 34<br>• Updated Clean Access Agent Version Summary, page 38<br>• Updated Open Caveats - Release 4.1.2.1, page 41<br>• Added Resolved Caveats - Agent Version 4.1.2.2, page 45 |
| 9/20/07 | Updated Software Compatibility Matrixes, page 6 tables and footnotes. |
| 9/19/07 | Added caveat CSCsk31476 to Open Caveats - Release 4.1.2.1, page 41 |
| 9/11/07 | Added Known Issue with NAT/PAT Devices and L3 Deployments, page 52 |

*Table 14 Updates to Release Notes for Cisco NAC Appliance, Release 4.1(2) and Later*

| Date | Description |
|---|---|
| 9/10/07 | Updates for release 4.1.2.1<br>• Updated Software Compatibility Matrixes, page 6<br>• Added Enhancements in Release 4.1.2.1, page 11<br>• Added Clean Access Supported AV/AS Product List, page 16<br>• Updated Supported AV/AS Product List Version Summary, page 34<br>• Updated Clean Access Agent Version Summary, page 38<br>• Updated Open Caveats - Release 4.1.2.1<br>• Added Resolved Caveats - Release 4.1.2.1, page 45 |
| 8/31/07 | Updated Hardware Supported, page 3 to feature integration with Cisco NAC Profiler |
| 8/13/07 | Added Known Issue with MSI Agent Installer File Name, page 54 |
| 8/8/07 | Updated Known Issues for Cisco NAC Appliance, page 52 |
| 7/27/07 | • Added caveat CSCsj84398 to Open Caveats - Release 4.1(2)<br>• Updated NAC-3310 Required BIOS/Firmware Upgrade, page 4 and Known Issues with HP ProLiant DL140 G3 Servers, page 52 to point to *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* |
| 7/26/07 | Release 4.1(2) |

## Related Documentation

For the latest updates to Cisco NAC Appliance (Cisco Clean Access) documentation on Cisco.com see:

http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html

or simply http://www.cisco.com/go/cca

- *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(2)*
- *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(2)*
- *Getting Started with NAC Network Modules in Cisco Access Routers*
- *Installing Cisco Network Modules in Cisco Access Routers*
- *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.