Release Notes for Cisco NAC Appliance (Cisco Clean Access) for Version 4.1(0)

Revised: January 30, 2008, OL-11384-01

Contents

These release notes provide late-breaking and release information for Cisco® NAC Appliance, formerly known as Cisco Clean Access (CCA), release 4.1(0). This document describes new features, changes to existing features, limitations a nd restrictions ("caveats"), upgrade instructions, and related information. These release notes supplement the Cisco NAC Appliance documentation included with the distribution. Read these release notes carefully and refer to the upgrade instructions prior to installing the software.

- Cisco NAC Appliance Releases, page 2
- Cisco NAC Appliance Service Contract/Licensing Support, page 2
- System and Hardware Requirements, page 2
- Software Compatibility, page 4
- New and Changed Information, page 9
- Clean Access Supported AV/AS Product List, page 21
- Clean Access Agent Version Summary, page 39
- Caveats, page 40
- Known Issues for Cisco NAC Appliance, page 53
- New Installation of Release 4.1(0), page 56
- Upgrading to 4.1(0), page 58
- Troubleshooting, page 83
- Documentation Updates, page 89
- Obtaining Documentation, Obtaining Support, and Security Guidelines, page 92

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

Cisco NAC Appliance Releases

Cisco NAC Appliance Version	Availability
4.1.0.2 ED	February 9, 2007
4.1.0.1 ED [obsoleted by 4.1.0.2]	December 4, 2006
4.1(0) ED [obsoleted by 4.1.0.2]	November 14, 2006

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 licensing, including service contract support, new licenses, evaluation licenses, legacy licenses and RMA, refer to the following web page:

http://www.cisco.com/en/US/products/ps6128/prod_pre_installation_guide09186a008073136b.html

System and Hardware Requirements

This section describes the following:

- System Requirements
- Hardware Supported
- Supported Switches for Cisco NAC Appliance
- VPN 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

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 83 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 Components Supported for Single Sign-On (SSO)

Table 1 lists VPN 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(0)	Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs)[1]	N/A
	Cisco ASA 5500 Series Adaptive Security Appliances, Version 7.2(0)81 or above	• Cisco SSL VPN Client (Full Tunnel) • Cisco VPN Client (IPSec)
	Cisco WebVPN Service Modules for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers	
	Cisco VPN 3000 Series Concentrators, Release 4.7	
	Cisco PIX Firewall	

[1] For additional details, see also Known Issue with Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs), page 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 Administration Guide* and the *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide* available at:

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

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 21
- Clean Access Agent Version Summary, page 39

Software Compatibility Matrixes

This section describes the following:

- Release 4.1(0) Compatibility Matrix
- Release 4.1(0) CAM/CAS Upgrade Compatibility Matrix
- Release 4.1(0) Agent Upgrade Compatibility Matrix

Release 4.1(0) Compatibility Matrix

Table 2 shows Clean Access Manager and Clean Access Server compatibility and the Agent version bundled with each CCA 4.1(0) release (if applicable). CAM/CAS/Agent versions displayed in the same row are compatible with one another. Cisco recommends synchronizing your software images to match those shown as compatible in the table.

Note For additional details on compatibility of later 4.1.x.x Agent releases with 4.1.x CAM/CAS servers, refer to the Release Notes applicable to the Agent release.

Table 2 Release 4.1(0) Compatibility Matrix [1,2]

Clean Access Manager	Clean Access Server	Clean Access Agent [3]
4.1.0.2 [4]	4.1.0.2 [4]	4.1.0.2 [5]
4.1.0.1 [6] [obsoleted by 4.1.0.2]	4.1(0) [obsoleted by 4.1.0.2]	4.1.0.0
4.1(0) [obsoleted by 4.1.0.2]		

[1] **Releases 4.1(0), 4.1.0.1, and 4.1.0.2 do not support Windows Vista.** Only 4.0(x) releases starting from 4.0(4) and 4.0.x.x Agent versions starting from 4.0.4.0 support Windows Vista. See the "Clean Access Agent System Requirements" section of the *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* Guide for details.

[2] **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.** You will be able to upgrade NAC 3300 Series appliances to upcoming release 4.1(1) (which includes Cavium SSL accelerator support). Refer to the *Release Notes for Cisco NAC Appliance (Cisco Clean Access) for Version 4.1(1)* for details.

[3] 4.1.0.x versions of the Clean Access Agent are compatible with the latest 4.1(0) CAM/CAS release, unless otherwise specified. See Clean Access Agent Version Summary, page 39 for details and caveats resolved for each Agent version.

[4] Release 4.1.0.2 obsoletes and replaces releases 4.1.0.1 and 4.1(0). If your system is running 4.0(x), 3.6(x) or 3.5(x), and you wish to upgrade to release 4.1(0), upgrade to release 4.1.0.2 directly. See Enhancements in Release 4.1.0.2, page 9.

[5] For CAM/CAS release 4.1.0.2, upgrade to 4.1.0.2 Agent only applies for Windows OS. The Mac OS version of the Agent remains at 4.1.0.0.

6. 4.1.0.1 is a CAM-only patch release applied to 4.1(0) CAMs that resolves caveat CSCsg89516, page 48. See Enhancements in Release 4.1.0.1, page 10 for details.

For upgrade instructions, see Upgrading to 4.1(0), page 58.

Release 4.1(0) CAM/CAS Upgrade Compatibility Matrix

Table 3 shows 4.1(0) 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.

Table 3 Release 4.1(0) CAM/CAS Upgrade Compatibility Matrix [1,2]

Clean Access Manager		Clean Access Server	
Upgrade From:	**To:**	**Upgrade From:**	**To:**
4.1.0.1 4.1(0) [3] 4.0(x) [3] 3.6(x) [3] 3.5(7)+ [4]	4.1.0.2 [5]	4.1(0) 4.0(x) [3] 3.6(x) [3] 3.5(7)+ [4]	4.1.0.2 [5]
4.1(0)	4.1.0.1 [6]	4.0(x) [3] 3.6(x) 3.5(7)+ [4]	4.1(0)
4.0(x) [3] 3.6(x) 3.5(7)+	4.1(0)		

[1] **Releases 4.1(0), 4.1.0.1, and 4.1.0.2 do not support Windows Vista.** Only 4.0(x) releases starting from 4.0(4) and 4.0.x.x Agent versions starting from 4.0.4.0 support Windows Vista. See the "Clean Access Agent System Requirements" section of the *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* Guide for details.

[2] **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.** You will be able to upgrade NAC 3300 Series appliances to upcoming release 4.1(1) (which includes Cavium SSL accelerator support). Refer to the *Release Notes for Cisco NAC Appliance (Cisco Clean Access) for Version 4.1(1)* for details. .

[3] In order to use the web upgrade package on Clean Access Managers running 3.6.x and 4.0.x, it is necessary to first apply the patch for CSCsg24153. (Please visit http://www.cisco.com/cgi-bin/tablebuild.pl/cca-patches for more information regarding CCA patches). If you have not applied the patch, you can upgrade the CAM via console/SSH upgrade instead.
Web upgrade of Clean Access Servers running 3.6.x and 4.0.x to release 4.1(0) is not supported. Use console/SSH upgrade only to upgrade the CAS. (See Notes on 4.1(0) Upgrade, page 58.)

[4] To upgrade from release 3.5(7) and above, you must use the in-place upgrade procedure. See Upgrading to 4.1(0), page 58.

[5] Release 4.1.0.2 obsoletes and replaces releases 4.1.0.1 and 4.1(0). If your system is running 4.0(x), 3.6(x) or 3.5(x), and you wish to upgrade to release 4.1(0), upgrade to release 4.1.0.2 directly. See Enhancements in Release 4.1.0.2, page 9.

[6] 4.1.0.1 is a CAM-only patch release that resolves caveat CSCsg89516, page 48. See Enhancements in Release 4.1.0.1, page 10 for details.

For upgrade instructions, see Upgrading to 4.1(0), page 58.

Release 4.1(0) Agent Upgrade Compatibility Matrix

Table 4 shows Clean Access Agent upgrade compatibility when upgrading existing versions of the Agent after 4.1(0) CAM/CAS upgrade. Except where noted, you can auto-upgrade any 3.5.1+ Agent directly to the latest 4.1.0.x Agent.

Table 4 Release 4.1.0.x Agent Upgrade Compatibility Matrix [1]

Clean Access Manager	Clean Access Server	Clean Access Agent	
		Upgrade From:	**To Latest Compatible Version:** [2]
4.1.0.2	4.1.0.2	4.1.0.0	4.1.0.2 [3] (Windows OS only)
4.1.0.1	4.1(0)	4.0.x.x 3.6.x.x 3.5.1 and above	4.1.0.0
4.1(0)			

1. **Releases 4.1(0), 4.1.0.1, and 4.1.0.2 do not support Windows Vista.** Only 4.0(x) releases starting from 4.0(4) and 4.0.x.x Agent versions starting from 4.0.4.0 support Windows Vista. See the "Clean Access Agent System Requirements" section of the *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* Guide for details.
2. Agent versions are not supported across major releases. Do not use 4.1.0.x Agents with 4.0(x) or prior releases. However, auto-upgrade is supported from any 3.5.1 or above Agent directly to the latest 4.1.0.x Agent. See Clean Access Agent Version Summary, page 39 for further details.
3. For CAM/CAS release 4.1.0.2, upgrade to 4.1.0.2 Agent only applies for Windows OS. The Mac OS version of the Agent remains at 4.1.0.0.

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 7
- Clean Access Server (CAS) Version, page 8
- Clean Access Agent Versioning, page 8
- Cisco Clean Access Updates Versioning, page 8

Clean Access Manager (CAM) Version

The top of the CAM web console displays the software version installed. Starting from release 4.1(0), 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 Appliance 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

- From the CAM web console, go to **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Misc > Update | Current Version**
- Or, from CAS direct access console, go to: **Administration > Software Update | Current Version** (CAS direct console is accessed via **https://<CAS_eth0_IP>/admin**)
- Or, SSH to the machine and type: `cat /perfigo/build`

Note If configuring High Availability CAM or CAS pairs, see also Access Web Consoles for High Availability, page 79 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 8)
- **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 21 and Cisco Pre-Configured Rules (“pr_”), page 20 for additional details.

New and Changed Information

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

- Enhancements in Release 4.1.0.2, page 9
- Enhancements in Release 4.1.0.1, page 10
- New Features and Enhancements in Release 4.1(0), page 11

For additional details, see also:

- Clean Access Supported AV/AS Product List, page 21
- Clean Access Agent Version Summary, page 39
- Caveats, page 40
- Known Issues for Cisco NAC Appliance, page 53

Enhancements in Release 4.1.0.2

Note Releases 4.1(0), 4.1.0.1, or 4.1.0.2 do not support Windows Vista. Only 4.0(x) releases starting from 4.0(4) and 4.0.x.x Agent versions starting from 4.0.4.0 support Windows Vista.

Release 4.1.0.2 is a general and important bug fix release for the Clean Access Manager (CAM) and Clean Access Server (CAS) that resolves the caveats described in Resolved Caveats - Release 4.1.0.2, page 47. No new features are added.

Note

- Release 4.1.0.2 is a mandatory CAM/CAS upgrade for 4.1(0) systems.
- Release 4.1.0.2 obsoletes release 4.1(0) and 4.1.0.1 and incorporates all 4.1(0) and 4.1.0.1 features.
- Release 4.1.0.2 can be applied to 3.5(x), 3.6(x), 4.0(x), and 4.1(0) systems.
- The 4.1.0.2 release includes an update to the Windows Agent (version 4.1.0.2). The Mac OS version of the Agent remains at 4.1.0.0. See Clean Access Agent Enhancements (4.1.0.2), page 10.

For additional details, see the following sections:

- Software Compatibility Matrixes, page 4
- Resolved Caveats - Release 4.1.0.2, page 47
- Upgrading to 4.1(0), page 58 (for upgrade instructions)

Enhancements

- Clean Access Agent Enhancements (4.1.0.2)
- Supported AV/AS Product List Enhancements (Version 50)

Clean Access Agent Enhancements (4.1.0.2)

Note Releases 4.1(0), 4.1.0.1, or 4.1.0.2 do not support Windows Vista. Only 4.0(x) releases starting from 4.0(4) and 4.0.x.x Agent versions starting from 4.0.4.0 support Windows Vista.

- Version 4.1.0.2 of the Agent resolves caveat CSCsg95811, page 47 (Symantec Corporate AntiVirus) and provides additional AVAS product support. See Supported AV/AS Product List Version Summary, page 36 for details.
- For CAM/CAS release 4.1.0.2, upgrade to 4.1.0.2 Agent only applies to Windows OS. The Mac OS version of the Agent remains at 4.1.0.0.

See also Clean Access Agent Version Summary, page 39.

Supported AV/AS Product List Enhancements (Version 50)

- See Clean Access Supported AV/AS Product List, page 21 for the latest AV/AS product charts.
- See Supported AV/AS Product List Version Summary, page 36 for details on each update to the list.

Enhancements in Release 4.1.0.1

Warning **Release 4.1.0.1 has been obsoleted. If your system is running 4.1.0.1, please upgrade to release 4.1.0.2. If your system is running 4.0(x), 3.6(x), or 3.5(x) and you wish to upgrade to release 4.1(0), please upgrade to release 4.1.0.2 directly.**

Release 4.1.0.1 is a general and important bug fix release and patch for the Clean Access Manager (CAM) only that resolves the caveats described in Resolved Caveats - Release 4.1.0.1, page 48. No new features are added.

Note

- The 4.1.0.1 release is a mandatory patch release that must be applied to applied to all 4.1(0) systems.
- The 4.1.0.1 patch is applied to the Clean Access Manager only.
- The 4.1.0.1 patch can only be applied to 4.1(0) systems. If running a previous CCA version, you must upgrade your system to 4.1(0) first (as described in Upgrading to 4.1(0), page 58) before applying this patch.

Note Additionally with patch release 4.1.01, the **Check** and **Success/Failure** search option is removed from the searchable Clean Access Agent Reports feature introduced in release 4.1(0) (for details, see Searchable Clean Access Agent Reports, page 16).
This affects the following page of the CAM web console: **Device Management > Clean Access > Clean Access Agent > Reports** (new **Check** and **Success/Failure** option is removed).

See the following sections:

- Upgrade Instructions for 4.1.0.1, page 11
- Resolved Caveats - Release 4.1.0.1, page 48

See also Software Compatibility Matrixes, page 4 for additional details.

Upgrade Instructions for 4.1.0.1

To upgrade your CAM to 4.1.0.1, perform the following steps.

Step 1 Download the **cam_upgrade-4.1.0.1.tar.gz** upgrade file to your local computer from the http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-4.1.0 folder.

Step 2 Apply the 4.1.0.1 patch to your 4.1(0) CAM using one of the following procedures. Carefully follow instructions to upgrade the CAM:

- Upgrade CAM from CAM Web Console, page 74, or
- Console/SSH Upgrade—Standalone Machines, page 75, or
- Upgrading from 3.6(x)/4.0(x)—HA Pairs, page 78 (for HA-CAMs only)

New Features and Enhancements in Release 4.1(0)

Warning **Release 4.1(0) has been obsoleted. If your system is running 4.1(0), please upgrade to release 4.1.0.2. If your system is running 4.0(x), 3.6(x), or 3.5(x) and you wish to upgrade to release 4.1(0), please upgrade to release 4.1.0.2 directly.**

Warning **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. You will be able to upgrade NAC 3300 Series appliances to upcoming release 4.1(1) (which includes Cavium SSL accelerator support). Refer to the *Release Notes for Cisco NAC Appliance (Cisco Clean Access) for Version 4.1(1)* for details.**

This section details the new features delivered with Cisco NAC Appliance release 4.1(0) for the Clean Access Manager and Clean Access Server, as well as enhancements from release 4.0(x).

New Features

- CAS Policy Fallback
- Clean Access Agent/ActiveX/Applet DHCP Release/Renew
- Support for GPO Update Trigger
- Online Update to Retrieve Switch OIDs
- Qualified Remediation Program Launch
- Clean Access Agent for Mac OS X Authentication
- Clean Access Agent Installation Options
- Clean Access Agent Language Template Support

- Clean Access Agent Silent Auditing
- Searchable Clean Access Agent Reports

Enhancements

- Certified Devices Timer Enhancements for Periodic Assessment
- DHCP Renewal Enhancements
- DHCP Subnet List Enhancements
- DHCP Global Option Enhancements
- IE 7.0 Support
- Clean Access Agent Enhancements (4.1.0.0)
- Port Profile Management for OOB Users
- Enhancements to Check Parameters
- Daylight Savings Time Support
- Supported AV/AS Product List Enhancements (Version 42)

Deprecated Features

- Deprecated IPsec/L2TP/PPTP/PPP Features
- Deprecated Roaming Features

CAS Policy Fallback

Release 4.1(0) provides CAS Fallback to allow administrators to configure the behavior of the Clean Access Server (CAS) when the Clean Access Manager (CAM) becomes unreachable to the CAS. For example, if a remote CAS attempts to reach the CAM, but the WAN link fails, the CAS Fallback feature can be used to specify the user access policy.

With release 4.1(0), the CAS checks the status of the CAM periodically, according to the Detect Interval specified. If the CAM is not reachable before the specified Detect Timeout, the CAS declares the CAM as dead, and sets the traffic policy of every user role to "Allow All, "Block All" or "Ignore" based on the Fallback Policy chosen. The CAS Fallback Policy can be configured as:

- Allow All — Allow all traffic for all users (authenticated and new)
- Block All — Block all traffic for all users (authenticated and new)
- Ignore (default) — Allow traffic only for authenticated users but block new users

This affects the following page of the CAM web console:

- **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Fallback**

Note The CAS fallback feature is for situations where communication between the CAS and CAM is lost. For protection against CAS failure itself in a Central Deployment, Cisco recommends using the CAS failover bundle.

Clean Access Agent/ActiveX/Applet DHCP Release/Renew

Release 4.1(0) provides complete support for L2/L3 OOB deployments in IP telephony environments. With release 4.1(0) and version 4.1.0.0 of Agent, port bouncing is no longer required to release or renew client DHCP addresses in an OOB deployment. For devices with the 4.1.0.0 Agent installed, the Agent will automatically trigger the device to perform DHCP release/renew. For Agent-less devices, the web login page will trigger the device to perform DHCP release/renew via ActiveX/Java Applet.

To enable this feature:

- Upgrade/install 4.1(0) on your CAM/CAS
- For devices with the Clean Access Agent already installed, the Agent version must be 4.1.0.0 or above, and no additional configuration required
- For Agent-less devices, the web login page must be configured to trigger the device DHCP release/renew via ActiveX/Java applet execution.
  - Go to **Administration > User Pages > Login Page > Add/ Edit | General**
  - Select a **Web Client (ActiveX/Applet)** option (ActiveX Only, Java Applet Only, ActiveX Preferred, Java Applet Preferred, ActiveX on IE, Java Applet on non-IE Browser)
  - Enable **Use web client to detect client MAC address and Operating System** (this allows the ActiveX control/Java applet to be launched from the user web login page)
  - Enable **Use web client to release and renew IP address when necessary (OOB)** (this allows the OOB client acquire new IP address after authentication without bouncing the switch port)
  - Optionally for Linux/MacOS clients, click **Install DHCP Refresh tool into Linux/MacOS system directory** (this facilitates DHCP release and renew for Linux/MacOS clients when the web client is used)
- In addition, the administrator may need to finetune the timers under **Switch Management > Profiles > SNMP Receiver > Advanced Settings**, such as the Port Bounce Interval delay between port-off and port-on, or any of the following new timer options:
  - **DHCP Release Delay**—Delay between user login and DHCP release
  - **VLAN Change Delay**—Delay between user login and VLAN Change
  - **DHCP Renew Delay**—Delay between DHCP release and DHCP renew

For Agent users, the Agent login success dialog displays “Refreshing IP address, please wait.” and “Refreshing IP address succeeded” messages after login credentials are entered.

For web login users, “Renewing IP address...” and web redirect time interval messages will displays after user login credentials are entered in the login page. When successfully logged in, the redirect page appears.

Support for GPO Update Trigger

With release 4.1(0), administrators can configure the Clean Access Agent to retrigger Group Policy update after the user login is complete. In effect, the 4.1.0.0+ Agent will execute a “gpupdate” command to re-trigger the Group Policy update.

Note Since Microsoft Group Policies are only available since the advent of Active Directory (Windows 2000 and newer), the GPO trigger update feature is only available on Windows XP/2000 machines.

This affects the following CAM web console page:

- **Device Management > Clean Access > General Setup > Agent Login |** new checkbox for **"Refresh Windows domain group policy after login (for Windows)"**

Online Update to Retrieve Switch OIDs

To help simplify support for an OOB deployment, Release 4.1(0) allows administrators to update the object IDs (OIDs) of supported switches through the CAM. For example, if a new switch (such as C3750-XX-NEW) of a supported model (Catalyst 3750 series) is released, customers only need to update the switch OIDs online to obtain support, instead of performing an upgrade.

This feature affects the following CAM web console page:

- **Device Management > Clean Access > Updates > New Summary | Settings**

Note This feature applies only to existing models. If a new switch series is introduced, customers will still need to upgrade to ensure OOB support for the new switches.

Qualified Remediation Program Launch

Release 4.1(0) adds a new "Requirement Type" that allows administrators to launch a qualified remediation program from the Clean Access Agent. The administrator can create a check/rule condition; upon its failure, the administrator can configure to launch any remediation program to fix the machine. Multiple programs are permitted, and they are launched in the same sequence as specified by the administrator.

The Clean Access Agent launches the programs in two ways, depending on the user privileges of the device. If the user has admin rights on his or her machine, the program is launched directly. If the user does not have administrative rights, the Clean Access stub must be installed to launch the program. In this case, the Clean Access stub will verify that the program is signed by a trusted certificate authority before launching the program. This feature is applicable to Windows 2000 and Windows XP machines only. These options are configurable at:

- **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement**

Clean Access Agent for Mac OS X Authentication

Release 4.1(0) introduces a Clean Access Agent that performs authentication on Mac OS X machines. The Agent is in the form of a universal binary that supports Mac OS 10.2 to 10.4. The Mac OS X Clean Access Agent supports single-sign on with VPN deployments but does not support single-sign on with Active Directory. You can view the distribution options for the Mac OS X Clean Access Agent in the following page of the CAM web console:

- **Device Management > Clean Access > Clean Access Agent > Distribution**

Clean Access Agent Installation Options

Release 4.1(0) introduces Clean Access Agent installation options to allow the administrator control over the level of user interaction when the Agent is initially installed. The installation options apply to both direct installation of the Agent (where the user installs the Agent directly on the client machine), and stub installation (where the Agent installer is launched through the stub installer), and are as follows:

- **User Interface:**

  - **No UI** —Only the dialog for the extracting installer is shown.
  - **Reduced UI**— Most of the installation dialogs are shown, but users are not allowed to choose the target location.
  - **Full UI** (default)—All of the installation dialogs are shown, and users are allowed to choose target location. The user must click through the panes to complete the installation.
- **Run Agent After Installation**:
  - **Yes** (default)—The Agent Login screen pops up after the Agent is installed.
  - **No** —The Agent Login screen does not appear after Agent installation, and the user must double-click the desktop shortcut to start the Agent

Note 4.1(0) Installation options apply to Windows Agent installer only (not Mac OS).

This adds the following page to the CAM web console:

- **Device Management > Clean Access > Clean Access Agent > Installation**

See also Clean Access Agent Enhancements (4.1.0.0), page 18.

Clean Access Agent Language Template Support

With release 4.1(0), the Clean Access Agent supports multiple European languages using language templates. In addition to English, version 4.1.0.0 of the Clean Access Agent supports German, Italian, Finnish, Czech, Norwegian, Spanish, Danish, French, Russian, Swedish, Turkish, Serbian, and Catalan for text-based Agent user dialog displays.

In addition, Agent error messages warnings and Properties data are all based on the supported language templates.

The Agent picks the correct template based on the Locale settings of the local computer. To use the localized Agent, the user needs to change the Windows locale setting to the corresponding language under **Control Panel > Regional and Language Option**s. For example, to use the Agent in French, the user needs to set the Windows locale to French.

In addition, Agent error messages warnings and **Properties** data are all based on the supported language templates.

Cisco recommends using the localized Agent in a localized version of Windows, for example, Russian Agent in Russian Windows, as the English version of Windows may not be able to display all characters correctly.

For administrators, the name of requirements/ descriptions are as configured on the CAM. On the CAM, these can be configured using characters of the appropriate language.

Note While all text based messages will appear in the supported language, the names of the actual checks/rules will be as configured on the CAM.

Note Agent template support is **not** the same as support for different client OSes for the Agent Installer or for AV/AS products. The Agent language template only controls what the viewer sees after the Agent is installed.

Clean Access Agent Silent Auditing

Release 4.1(0) introduces silent auditing functionality for Clean Access Agent posture assessment. The silent **Audit** feature quietly executes the checks configured for the requirement in the background and submits the failed or passed status in the client report on the CAM. This allows administrators to review the user reports and determine the effectiveness of any new configured rule/check before making a requirement mandatory for user access. For example, if the administrator wants to block use of an instant messenger program on the network, the administrator can use silent audit first to determine how many users are on the program and how the network will be affected if a requirement is enforced. The Clean Access Agent does not present any dialogs to the user when the silent audit is performed in the background.

This affects the following pages of the CAM web console:

- **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement** (new **Enforce Type** [Mandatory | Optional | **Audit**] dropdown menu for all Requirement Types)

Searchable Clean Access Agent Reports

Clean Access Agent report logging and searching is enhanced in release 4.1(0) to facilitate information gathering for the administrator. The **Reports** page now provides an "**Advanced/Simple**" toggle option that expands the search criteria to include the following options:

- **AV/AS Software**:
  The AV/AS Software dropdown menu allows you to search/display client reports for the following cases:
  - AntiVirus Software Installed
  - AntiSpyware Software Installed
  - Unknown AV/AS Software Installed
- **Requirement** and **Success/Failure**:
  The **Requirement** dropdown lists all Clean Access Agent requirements configured in the system, and the **Success/Failure** dropdown option allows you to search/display success or failure client reports for the chosen requirement.
- The **Check** and **Success/Failure**:
  The **Check** dropdown lists all Clean Access Agent checks in the system (system "pc_" or "av_" checks, or administrator-created custom checks). The **Success/Failure** dropdown option allows you to search/display reports for success or failure of the check on client systems.

Note To optimize performance, the **Check** and **Success/Failure** option is removed starting from patch release 4.1.0.1.

Clicking the **Show** button after selecting any of the **Simple** or expanded **Advanced** search options will display a summary of all entries that match the criteria as well the detailed administrator report for each client. This affects the following page of the CAM web console:

- **Device Management > Clean Access > Clean Access Agent > Reports** (new **Advanced/Simple** toggle for search features)

Certified Devices Timer Enhancements for Periodic Assessment

Release 4.1(0) enhances Certified Devices Timer configuration to provide better periodic assessment capabilities. The Certified Devices List no longer needs to be cleared in its entirety each time the timer is applied. Administrators can now clear the Certified Devices List per Clean Access Server, per User Role, per Auth Provider, or a combination of all three.

The Timer page also provides the following new options:

- When **Keep Online Users** option is checked, user sessions are not immediately ended when clearing the list, but at user logout time (or at linkdown for OOB). Devices can re-enter the list after user authentication and device remediation.
- Certified Device List entries can now be cleared all at one time or in steps. You can clear devices according to how long they have been on the list and/or in fixed time interval batches. This facilitates CAM database management when clearing large numbers of devices.
- Administrators can create and save multiple instances of Certified Device Timers (similar to a Scheduled Job/Task). Each Timer is independent of the others and can be maintained separately. For example, if managing 6 CAS pairs, the administrator can create a different Timer for each CAS.

This affects the following page of the CAM web console:

- **Device Management > Clean Access > Certified Devices > Timer**

DHCP Renewal Enhancements

Release 4.1(0) offers two new DHCP enable/disable enhancements to ensure client IP addresses are renewed properly when the CAS is configured as the DHCP server for your network:

- **User Logout on DHCP Lease Expiration**—This enhancement is disabled by default. Clicking the **Enable** button causes the user to be logged out (either Agent logout or web logout) from the Cisco NAC Appliance when the client's DHCP lease expires.
- **DHCP FORCERENEW**—This enhancement is disabled by default. Clicking the **Enable** button instructs the DHCP server to execute a DHCP NAK command, which releases IP addresses assigned to a client by other DHCP servers. Following the NAK command, the DHCP client will be assigned a valid IP address as configured on the CAS.

This affects the following page of the CAM web console:

- **Device Management > CCA Servers > Manage [CAS_IP] > Network > DHCP > DHCP Status**

Note Prior to this admin console option, a manual `ipconfig / renew` could be performed on the client from a command line tool to achieve the same effect.

DHCP Subnet List Enhancements

With release 4.1(0), the warning messages for too many IPs/subnets are changed.

This affects the following page of the CAM web console:

- **Device Management > CCA Servers > Manage [CAS_IP] > Network > DHCP > Subnet List**

Note For release 4.1(0) and later, the CAS DHCP Server responds with a NAK to IP addresses not entered into the subnet list but originating from a known subnet.

DHCP Global Option Enhancements

Release 4.1(0) adds new server directives to the DHCP Global Options "option type" menu. These directives instruct the server to behave in new ways, respond to new protocols, or change data sent outside of the DHCP options list

When specifying DHCP Global Options, you may select a particular DHCP option by entering its number in the "Option #" input box. If the desired option number is not known, or if specifying a server directive which changes server behavior but has no corresponding DHCP option number then you can select the name of the option or directive from the dropdown menu next to the "set option type" button. Click the "set option type" button after the desired DHCP option type has been selected.

This affects the following pages of the CAM web console:

- **Device Management > CCA Servers > Manage [CAS_IP] > Network > DHCP > Global Options [New Root Global Option | New Scoped Global Option | New Class Option]**

Note DHCP option numbers are specified in RFC 2132

IE 7.0 Support

Release 4.1(0) and Clean Access Agent 4.1.0.0 support Internet Explorer 7.0 for the CAM web console, web login user page, Agent login/logout, Agent install/uninstall/upgrade, Agent requirements (e.g. Windows Update, Launch URL, File Download), and for L3 OOB (ActiveX, Applet, Agent).

Clean Access Agent Enhancements (4.1.0.0)

Version 4.1.0.0 adds the following enhancements to the Clean Access Agent:

- **Installer Configuration Options**— The Agent install for Windows machines includes two configurable options, which apply whether the Agent install is invoked directly or through the Agent stub installer. The first option sets the level of user interface visible during the installation process: choices are Full, Reduced, and None. The second option configures whether to launch the Agent after installation. See also Clean Access Agent Installation Options, page 14.
- **Login/logout Screen Auto-close**— This enhancement allows administrators to eliminate the display of the Clean Access Agent Login Success and/or Logout screens, or set a time after which either dialog will close. Prior to this feature, users had to click the **OK** button in either screen to close the dialog. Setting the time to zero seconds prevents display of the login or logout success dialog, or administrators can choose a value from 0 to 300 seconds after which to automatically close the user dialog. Configure the following CAM web console page to enable this feature:
  - **Device Management > Clean Access > General Setup > Agent Login** — New checkboxes for:
    Automatically close login success screen after [] secs (for Windows)
    Automatically close logout success screen after [] secs (for Windows)

See also Clean Access Agent Version Summary, page 39.

Port Profile Management for OOB Users

Release 4.1(0) includes a new option for managing port profiles in out-of-band deployments. The enhancement enables administrators to remove other online out-of-band users on the switch port when a new user is detected on the same port. It also allows for the modification of the port profile if an existing user is seen on a different switchport.

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

- **Switch Management > Profiles > Port**

Enhancements to Check Parameters

For three types of checks, Release 4.1(0) allows users to specify “older than” or “newer than” by more than or fewer than x days to the current date. The check types include registry value, file date, and Windows update.

Daylight Savings Time Support

Release 4.1(0) and above support the Daylight Savings Time (DST) change to March (second Sunday) and November (first Sunday) starting in 2007. Prior to 2007, DST started in April (first Sunday) and ended in October (last Sunday). See also CSCsg44268, page 52 for details.

Note For more information, see *U.S. Daylight Saving Time (DST) Changes for 2007* and *CSCsg44268 Bug Details*.

Supported AV/AS Product List Enhancements (Version 42)

- See Clean Access Supported AV/AS Product List, page 21 for the latest AV/AS product charts.
- See Supported AV/AS Product List Version Summary, page 36 for details on each update to the list.

Deprecated IPsec/L2TP/PPTP/PPP Features

The IPsec/L2TP/PPTP/PPP features (for encrypted connection between the CAS and end users) have been deprecated and will be removed in upcoming releases.

This affects the following pages of the CAM web console:

- **Device Management > CCA Servers > Manage [CAS_IP] > Network > IPsec/L2TP/PPTP/PPP**

Deprecated Roaming Features

The Roaming feature (for roaming between Clean Access Servers) has been deprecated and will be removed in upcoming releases.

This affects the following pages of the CAM web console:

- **Device Management > Roaming**

Cisco Pre-Configured Rules ("pr_")

Cisco NAC Appliance provides a set of pre-configured rules and checks that are downloaded to the CAM via the **Updates** page on the CAM web console (under **Device Management > Clean Access > Clean Access Agent > Updates**).

Pre-configured rules have a prefix of "pr" in their names (e.g. "pr_XP_Hotfixes"), and can be copied (for use as a template), but cannot be edited or removed. You can click the **Edit** button for any "pr_" rule to view the rule expression that defines it. The rule expression for a pre-configured rule will be composed of pre-configured checks (e.g. "pc_Hotfix835732") and boolean operators. The rule expression for pre-configured rules is updated via Cisco Updates. For example, when new Critical Windows OS hotfixes are released for Windows XP, the pr_XP_Hotfixes rule will be updated with the corresponding hotfix checks.

Pre-configured rules are listed under **Device Management > Clean Access > Clean Access Agent > Rules > Rule List**. Pre-configured checks have a prefix of "pc" in their names and in turn are listed under **Device Management > Clean Access > Clean Access Agent > Rules > Check List**

Note Cisco pre-configured rules provide support for Critical Windows OS hotfixes.

Note For complete details on configuring Clean Access Agent requirements, rules, and checks see the *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide*.

Using Cisco Rules to Check for CSA

You can use Cisco rules to create a Clean Access Agent requirement that checks if the Cisco Security Agent (CSA) is already installed and/or running on a client (from version 14663 and above of the Cisco Updates ruleset). To do this:

1. Create a new Link Distribution or File Distribution requirement (for Windows XP/2000).
2. Associate the requirement to one or both of the following rules (for Windows XP/2000):
   - pr_CSA_Agent_Version_5_0
   - pr_CSA_Agent_Service_Running
3. Associate the requirement to the user role(s) for which it will apply.

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 XP / 2000), page 22
- Clean Access AV Support Chart (Windows ME / 98), page 30
- Clean Access AS Support Chart (Windows XP / 2000), page 32

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 36
- Clean Access Agent Version Summary, page 39

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 Administration Guide* 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 XP / 2000)

Table 5 lists Windows 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 XP/2K) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (Sheet 1 of 8)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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
V3Pro 2004	6.x	yes (3.5.10.1)	yes (3.5.12)	yes
ALWIL Software				
avast! Antivirus	4.x	yes (3.5.10.1)	yes (3.5.10.1)	yes
avast! Antivirus (managed)	4.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
avast! Antivirus Professional	4.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
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
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
ClamWin				
ClamWin Antivirus	0.x	yes (3.5.2)	yes (3.5.2)	yes

Table 5 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (Sheet 2 of 8)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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
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)	-
Eset Software				
NOD32 antivirus system	2.x	yes (3.5.5)	yes (3.5.5)	yes
Frisk Software International				
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

Table 5 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (Sheet 3 of 8)

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

Table 5 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (Sheet 4 of 8)

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

Table 5 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (Sheet 5 of 8)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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 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)	-
SalD Ltd.				
Dr.Web	4.32.x	yes (3.5.0)	yes (3.5.0)	yes
Dr.Web	4.33.x	yes (3.5.11.1)	yes (3.5.11.1)	yes
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)	-
BitDefender 9 Standard	9.x	yes (3.5.8)	yes (3.5.8)	-
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.				

Table 5 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (Sheet 6 of 8)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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 version 3.80	3.8	yes (3.5.0)	yes (3.5.0)	-
Symantec Corp.				
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 2002	8.00.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2002	8.x	yes (3.5.1)	yes (3.5.1)	yes
Norton AntiVirus 2002 Professional	8.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2002 Professional Edition	8.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2003	9.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2003 Professional	9.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2003 Professional Edition	9.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2004	10.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2004 Professional	10.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2004 Professional Edition	10.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2004 (Symantec Corporation)	10.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2005	11.0.x	yes (3.5.0)	yes (3.5.0)	yes
Norton AntiVirus 2006	12.0.x	yes (3.5.5)	yes (3.5.5)	yes
Norton AntiVirus 2006	12.x	yes (3.5.5)	yes (3.5.5)	yes
Norton AntiVirus Corporate Edition	7.x	yes (3.5.1)	yes (3.5.1)	yes
Norton Internet Security	7.x	yes (3.5.0)	yes (3.5.0)	yes
Norton Internet Security	8.0.x	yes (3.5.0)	yes (3.5.0)	yes
Norton Internet Security	8.2.x	yes (3.5.1)	yes (3.5.1)	yes
Norton Internet Security	8.x	yes (3.5.1)	yes (3.5.1)	yes
Norton Internet Security	9.x	yes (3.5.10.1)	yes (3.5.10.1)	yes
Norton Internet Security (Symantec Corporation)	10.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Norton 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

Table 5 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (Sheet 7 of 8)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2, 3]
		Installation	Virus Definition	
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 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
Trend Micro, Inc.				
PC-cillin 2002	9.x	yes (3.5.1)	yes (3.5.1)	-
PC-cillin 2003	10.x	yes (3.5.0)	yes (3.5.0)	-
ServerProtect	5.x	yes (4.1.0.0)	yes (3.6.5.0)	-
Trend Micro Antivirus	11.x	yes (3.5.0)	yes (3.5.0)	yes
Trend Micro AntiVirus	15.x	yes (3.6.5.0)	yes (3.6.5.0)	-
Trend Micro 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 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)	-
Trend Micro PC-cillin Internet Security 2005	12.x	yes (3.5.3)	yes (3.5.3)	-
Trend Micro PC-cillin Internet Security 2006	14.x	yes (3.5.8)	yes (3.5.8)	-
Trend Micro PC-cillin Internet Security 2007	15.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Yahoo!, Inc.				
SBC Yahoo! Anti-Virus	7.x	yes (3.5.10.1)	yes (3.5.10.1)	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 XP/2K) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (Sheet 8 of 8)

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 XP/2000.)

Table 6 Clean Access Antivirus Product Support Chart (Windows ME/98) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (Sheet 1 of 2)

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

Table 6 Clean Access Antivirus Product Support Chart (Windows ME/98) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (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 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	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 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 XP / 2000)

Table 7 lists Windows 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 XP/2000) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (Sheet 1 of 4)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
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
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
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
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	9.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
CA eTrust PestPatrol	5.x	yes (3.6.1.0)	-	yes
CA eTrust PestPatrol Anti-Spyware	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes

Table 7 Clean Access Antispyware Product Support Chart (Windows XP/2000) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (Sheet 2 of 4)

		AS Checks Supported (Minimum Agent Version Needed)[1]		
Product Name	**Product Version**	**Installation**	**Spyware Definition**	**Live Update[2]**
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)	-
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
Javacool Software LLC				
SpywareBlaster v3.1	3.1.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
SpywareBlaster v3.2	3.2.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
SpywareBlaster v3.3	3.3.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
SpywareBlaster v3.4	3.4.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
SpywareBlaster v3.5.1	3.5.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Lavasoft, Inc.				
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
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)	-	-

Table 7 Clean Access Antispyware Product Support Chart (Windows XP/2000) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (Sheet 3 of 4)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
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.				
Windows Defender	1.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
PC Tools Software				
Spyware Doctor	4.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Spyware Doctor 3.0	3.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
Spyware Doctor 3.1	3.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
Spyware Doctor 3.2	3.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
Spyware Doctor 3.5	3.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Spyware Doctor 3.8	3.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
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)	-
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
SOFTWIN				
BitDefender 9 Antispyware	9.x	yes (4.1.0.0)	yes (4.1.0.0)	-
Sunbelt Software				
Sunbelt CounterSpy	1.x	yes (3.6.0.0)	-	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.x	yes (3.6.0.0)	-	-
Trend Micro PC-cillin Internet Security 2007 AntiSpyware	15.x	yes (4.1.0.0)	-	yes
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)	-	-

Table 7 Clean Access Antispyware Product Support Chart (Windows XP/2000) Version 50, Release 4.1.0.2 / 4.1.0.2 Agent (Sheet 4 of 4)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
Yahoo!, Inc.				
SBC Yahoo! Applications	2005.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
Yahoo! Anti-Spy	1.x	yes (3.6.0.0)	yes (3.6.0.0)	-

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

[2] The Live Update column indicates whether the Agent supports live update for the product via the 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 21 for the latest Supported AV list as of the latest release. See New and Changed Information, page 9 for the release feature list

Table 8 Supported AV /AS Product List Versions

Version	Enhancements
Release 4.1.0.2 —4.1.0.2 Agent	
Version 50	**Added AV Products:** • AhnLab V3 Internet Security 2007 Platinum, 7.x • Kingsoft Internet Security, 7.x • McAfee VirusScan Enterprise, 8.x • Trend Micro AntiVirus, 15.x • ServerProtect, 5.x **Added AS Products:** • AhnLab SpyZero 2007, 3.x • Primary Response SafeConnect, 2.x
Version 49 and 48	Minor internally used data change.
Release 4.1(0) —4.1.0.0 Agent	
Version 47	Minor internally used data change.
Version 46	McAfee VirusScan 10.x—changed def date/version checks from normal to special update.
Version 45	**Added AV products:** • avast! Antivirus (managed), 4.x • avast! Antivirus Professional, 4.x • Active Virus Shield, 6.x • AOL Safety and Security Center Virus Protection, 2.x • CA Anti-Virus, 8.x • eTrust EZ Armor, 6.2.x • Aluria Security Center AntiVirus, 1.x • F-Secure Anti-Virus 2005, 5.x • F-Secure Anti-Virus Client Security, 6.x • F-Secure Internet Security, 6.x • F-Secure Anti-Virus, 6.x • AntiVirusKit 2006, 2006.x • AntiVir PersonalEdition Classic Windows, 7.x • Avira AntiVir PersonalEdition Premium, 7.x

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

Version	Enhancements
	• Kaspersky Anti-Virus 6.0, 6.x • Kaspersky Anti-Virus 6.0 Beta, 6.x • Kaspersky Internet Security, 6.x • Kingsoft AntiVirus 2004, 2004.x • Kingsoft Internet Security 2006 +, 2006.x • McAfee VirusScan, 11.x • Windows Live OneCare, 1.x • eScan Anti-Virus (AV) for Windows, 8.x • eScan Corporate for Windows, 8.x • eScan Internet Security for Windows, 8.x • eScan Professional for Windows, 8.x • eScan Virus Control (VC) for Windows, 8.x • Norman Virus Control, 5.x
	• Panda Titanium Antivirus 2004, 3.02.x • Panda TruPrevent Personal 2006, 3.x • Norton AntiVirus, 14.x • Norton Internet Security (Symantec Corporation), 10.x • Norton SystemWorks 2006 Premier, 12.0.x • Symantec AntiVirus Server, 8.x • ServerProtect, 5.x • Trend Micro Client/Server Security, 6.x • Trend Micro PC-cillin Internet Security 2007, 15.x
	Added AS products: • AOL Safety and Security Center Spyware Protection, 2.0.x • AOL Safety and Security Center Spyware Protection, 2.1.x • AOL Safety and Security Center Spyware Protection, 2.2.x • AOL Safety and Security Center Spyware Protection, 2.3.x • Anonymizer Anti-Spyware, 1.x • Anonymizer Anti-Spyware, 3.x • BPS Spyware &amp; Adware Remover, 9.x • BPS Spyware Remover, 9.x • CA eTrust Internet Security Suite AntiSpyware, 9.x • CA eTrust PestPatrol Anti-Spyware, 8.x • Aluria Security Center AntiSpyware, 1.x • X-Cleaner Deluxe, 4.x

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

Version	Enhancements
	• SpywareBlaster v3.5.1, 3.5.x • McAfee AntiSpyware, 1.5.x • McAfee AntiSpyware, 2.x • McAfee AntiSpyware Enterprise, 8.x • Spyware Begone, 6.x • Spyware Begone, 8.x • Spyware Begone V7.95, 7.95.x • Spyware Begone V8.20, 8.20.x • Spyware Begone V8.25, 8.25.x • Windows Defender, 1.x • Spyware Doctor, 4.x • Spyware Doctor 3.5, 3.x • Spyware Doctor 3.8, 3.x
	• Prevx1, 1.x • Prevx1, 2.x • BitDefender 9 Antispyware, 9.x • Norton Spyware Scan, 2.x • Trend Micro PC-cillin Internet Security 2007 AntiSpyware, 15.x • Spy Sweeper, 5.x
	Removed AS products: • Microsoft AntiSpyware, 1.x

Clean Access Agent Version Summary

Note Releases 4.1(0), 4.1.0.1, or 4.1.0.2 do not support Windows Vista. Only 4.0(x) releases starting from 4.0(4) and 4.0.x.x Agent versions starting from 4.0.4.0 support Windows Vista.

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 21 for details on related AV/AS support.

Table 9 Clean Access Agent Versions

Agent Version [1]	Feature / Enhancement
4.1.0.2	• Version 4.1.0.2 of the Agent resolves caveat CSCsg95811, page 47 (Symantec Corporate AntiVirus) and provides additional AVAS product support. See Supported AV/AS Product List Version Summary, page 36 for details. • Upgrade to 4.1.0.2 Agent only applies for Windows OS. The Mac OS version of the Agent remains at 4.1.0.0. See also Clean Access Agent Enhancements (4.1.0.2), page 10.
4.1.0.0	Release 4.1.(0) with 4.1.0.0 Agent provides: • Clean Access Agent/ActiveX/Applet DHCP Release/Renew, page 13 • Support for GPO Update Trigger, page 13 • Qualified Remediation Program Launch, page 14 • Clean Access Agent for Mac OS X Authentication, page 14 • Clean Access Agent Installation Options, page 14 • Clean Access Agent Language Template Support, page 15 • Clean Access Agent Silent Auditing, page 16 • Searchable Clean Access Agent Reports, page 16 • IE 7.0 Support, page 18 • Enhancements to Check Parameters, page 19 See also Clean Access Agent Enhancements (4.1.0.0), page 18.

[1] See Release 4.1(0) Agent Upgrade Compatibility Matrix, page 6 for upgrade compatibility details.

Caveats

This section describes the following caveats:

- Open Caveats - Release 4.1.0.2, page 40
- Resolved Caveats - Release 4.1.0.2, page 47
- Resolved Caveats - Release 4.1.0.1, page 48
- Resolved Caveats - Release 4.1(0), page 49

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 4.1.0.2

Table 10 List of Open Caveats

	Software Release 4.1.0.2	
DDTS Number	**Corrected**	**Caveat**
CSCeh96620	No	Agent Installer Does Not Have Signature When the user downloads the 3.5.1 or above Clean Access Agent, most security alert O/S software will indicate that the installer doesn't have a known publisher and a valid digital signature.
CSCsd90433	No	Apache does not start on HA-Standby CAM after heartbeat link is restored.
CSCse37028	No	Cannot create DHCP Reserved IP address with Relay-IP restriction
CSCse45941	No	Hitting “Cancel” during the package selection will make install continue

Table 10 List of Open Caveats (continued)

DDTS Number	Software Release 4.1.0.2	
	Corrected	**Caveat**
CSCse86581	No	Agent does not correctly recognize def versions on the following Trend AV products: • PC-cillin Internet Security 2005 • PC-cillin Internet Security 2006 • OfficeScan Client Tested Clients: • PC-cillin Internet Security 2006 (English) on US-English Windows 2000 SP4 • OfficeScan Client (English) on US-English Windows 2000 SP4 • VirusBaster 2006 Internet Security (Japanese) on Japanese Windows XP SP2 • VirusBaster Corporate Edition (Japanese) on Japanese Windows XP SP2
CSCsg07369	No	Incorrect “IP lease total” displayed on editing manually created subnets Steps to reproduce: 1. Add a Managed Subnet having at least 2500+ IP addresses for 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” 2. Create a DHCP subnet with 2500+ hosts using CAM web page “Device Management > Clean Access Servers > Manage [IP Address] > Network > DHCP > Subnet List > New” 3. Edit the newly created subnet using CAM web page “Device Management > Clean Access Servers > Manage [IP Address] > Network > DHCP > Subnet List > Edit” 4. Click “Update”. The CAM 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. The issue does not affect DHCP functionality and is strictly known to be a cosmetic issue

Table 10 List of Open Caveats (continued)

	Software Release 4.1.0.2	
DDTS Number	**Corrected**	**Caveat**
CSCsg31307	No	IP refresh should be supported on Windows clients with restricted user privileges and Agent stub Steps to reproduce: 1. Setup OOB environment with Active Directory (AD) Single Sign-On (SSO) 2. Login on AD from Windows client machine using restricted user 3. IP refresh fails on Windows client machine Without this enhancement the administrator will be required to bounce the port after VLAN is changed
CSCsg38702	No	Agent cannot recognize Japanese Trend AV installation. Agent properties shows "Product Name" garbled. Client OS affected: • Japanese Windows XP Professional SP2 • Japanese Windows 2000 Professional SP4 AV product affected: • Japanese VirusBaster Corporate Edition 7.3 (US Product Name: Trend Micro OfficeScan Client) Steps to reproduce: Make a new AV rule: - Type: Installation - OS: Windows XP/2K - 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 Steps to reproduce: 1. Include the client's subnet or IP address in subnet based filter list using CAM web page "Device Management > Filters > Subnets" 2. Launch CCA Agent on the client machine (can be Windows or Mac OS

Table 10 List of Open Caveats (continued)

DDTS Number	Software Release 4.1.0.2	
	Corrected	**Caveat**
CSCsg66470	No	Changing hostname on both failover setting & system breaks HA-failover configuration. Steps to reproduce: 1. Configure HA-failover on both Clean Access Servers - CAS1 and CAS2 2. On CAS1, change peer hostname to “CAS2NEW” on HA-failover using CAS web page “Administration > Network Settings > Failover > General” 3. On CAS2, change peer hostname to “CAS1NEW” on HA-failover using CAS web page “Administration > Network Settings > Failover > General” 4. On CAS1, change the system hostname to “CAS1NEW” using CAS web page “Administration > Network Settings > DNS” 5. On CAS2, change the system hostname to “CAS2NEW” using CAS web page “Administration > Network Settings > DNS” 6. On CAS1, verify the HA-failover web page “Administration > Network Settings > Failover > General” displays correct hostname for local & peer machine 7. On CAS2, verify the HA-failover web page “Administration > Network Settings > Failover > General” displays correct hostname for local & peer machine 8. On both CASs, file /etc/ha.d/ha.cf lists one of the node names incorrectly, which breaks HA-failover configuration **Workaround** Click **Update** on HA-failover web page **Administration > Network Settings > Failover > General**. Alternatively, first change the hostname on the system and then on the HA-failover setting web page

Table 10 List of Open Caveats (continued)

DDTS Number	Software Release 4.1.0.2	
	Corrected	**Caveat**
CSCsg66511	No	Configuring HA-failover synchronization settings on 1st CAS takes an extremely long time The web page for HA-failover synchronization settings should not take so long upon configuring on the first CAS Steps to reproduce: 1. Configure HA-Failover on both CAS, except failover synchronization settings 2. Go to HA-Secondary CAS web page "Administration > Network Settings > Failover > Synchronization" 3. Enter peer SSH Client & SSH Server key 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

CSCsg98960	No	4.1(1) Installer does not recognize certain SCSI drives
		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:
		"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"
		Upgrades to 4.1(1) from previous versions are not affected by this bug.
		Workaround
		At the boot prompt that appears during installation, enter "DL140" and then <Enter>.
		`Cisco Clean Access Installer (C) 2006 Cisco Systems, Inc.`
		`Welcome to the Cisco Clean Access Installer!`
		`- To install a Cisco Clean Access device, press the <ENTER> key.`
		`- To install a Cisco Clean Access device over a serial console, enter serial at the boot prompt and press the <ENTER> key.`
		`boot:` **`DL140`**

Table 10 List of Open Caveats (continued)

DDTS Number	Software Release 4.1.0.2	
	Corrected	Caveat
CSCsi07595	No	DST fix will not take effect if generic MST, EST, HST, etc. options are specified Due to a Java runtime implementation, the DST 2007 fix does not take effect for Cisco NAC Appliances that are using generic time zone options such as "EST," "HST," or "MST" on the CAM/CAS UI time settings. **Workaround** If your CAM/CAS machine time zone setting is currently specified via the UI using a generic option such as "EST," "HST," or "MST." change this to a location/city combination, such as "America/Denver." **Note** CAM/CAS machines using time zone settings specified by the "service perfigo config" script or specified as location/city combinations in the UI, such as "America/Denver" are not affected by this issue.

Table 10 List of Open Caveats (continued)

DDTS Number	Software Release 4.1.0.2	
	Corrected	**Caveat**

CSCsi23228	No	CAM database performance degraded over time
		Clean Access Manager performance degrades over time, users may experience slowness during login process and CAM web administration interfaces. The slowness may start to exhibit itself after an extensive number of database delete/insert/modify operations.
		There are three workarounds for this issue which can be applied under different conditions.
		Workaround 1: This can be applied during maintenance window when CAM is not in service. Note that this may take up several minutes, please do not interrupt the process.
		1. `service perfigo stop`
		2. `su -l postgres`
		3. `vacuumdb -h 127.0.0.1 -a -f`
		4. `exit`
		5. `service postgresql restart`
		6. `service perfigo start`
		Workaround 2: This can be applied when system is in service with light load. Note that this may take up several minutes, please do not interrupt the process.
		1. `su -l postgres`
		2. `vacuumdb -h 127.0.0.1 -a -f`
		3. `exit`
		Workaround 3: This can be added as system daily cron job to prevent the potential slowness.
		1. Create a file named “db_vacuum.sh” under “/etc/cron.daily” with the following content:
		`#!/bin/sh`
		`su - postgres -c "vacuumdb -h 127.0.0.1 -a -f"`
		2. `cd /etc/cron.daily`
		3. `chmod +x db_vacuum.sh`

CSCsi86205	No	A kernel error results when a user manages a CAS with the “ifconfig eth1 down” command The *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide, Release 4.1(0)* 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. **Note** Future releases of the Cisco Clean Access system software will address the “ifconfig eth1 down” command issue.

Table 10 List of Open Caveats (continued)

DDTS Number	Software Release 4.1.0.2	
	Corrected	**Caveat**
CSCsi97216	No	CAM does not change port to Authentication VLAN when Certified Devices List is cleared using a port bounce When the CDL is cleared, the CAM does one of the following, depending on the **Remove out-of-band online user without bouncing the port** profile setting: • If the port setting is enabled (checked), the CAM changes the port to Authentication VLAN, but does not bounce the port. • If the above setting is disabled (unchecked), the CAM bounces the port, but does not change it to Authentication VLAN. The CAM must change the port to the Authentication VLAN every time the CDL is cleared (i.e., when user is removed from the Online Users list) regardless of whether the port is bounced or not. **Note** This issue is resolved in release 4.1(3).

Resolved Caveats - Release 4.1.0.2

Table 11 List of Closed Caveats

DDTS Number	Software Release 4.1.0.2	
	Corrected	**Caveat**
CSCsg95811	Yes	Symantec Corporate AntiVirus not recognized by Cisco Clean Access system after upgrade Symantec Corporate AntiVirus may not be recognized by Cisco Clean Access system after upgrade to 4.1(0). The Cisco Clean Access reports "Symantec unknown product" and users are assigned a temporary role even though their AntiVirus definitions are up-to-date. **Workaround** As a temporary workaround, you can configure custom rules instead of using the pre-configured/automated rules.
CSCsh15238	Yes	Memory Leak in RADIUS Authentication/Accounting Module If you are using a RADIUS server to perform authentication/accounting functions in your network (set up in either **User Management > Auth Server > Auth Server** or **User Management > Auth Server > Accounting**), a slow memory leak exists that can eventually cause the server to run out of memory.

Table 11 List of Closed Caveats (continued)

DDTS Number	Software Release 4.1.0.2	
	Corrected	**Caveat**
CSCsh22411	Yes	Allow Restricted Access option displays "Invalid Session" error When the CAM is configured to allow users temporary restricted access during web login instead of downloading the Agent, the "Invalid Session" error message appears after the user clicks **Allow Restricted Access**. **Workaround** Download the Cisco Clean Access Agent or configure a customized role for the users who can't use the Cisco Clean Access Agent. Alternatively, you can configure a filter for the remote client's MAC address.
CSCsh39119	Yes	Editing auto-generated DHCP subnet removes ARP entries from Clean Access Server (CAS), except for the very first auto-generated subnet. **Workaround** Disable the first DHCP auto-generated subnet. If there is any concern about the state of the ARP table, run arpregen.pl.

Resolved Caveats - Release 4.1.0.1

Table 12 List of Closed Caveats

DDTS Number	Software Release 4.1.0.1	
	Corrected	**Caveat**
CSCsg89516	Yes	4.1 fails user authentication if requirements are checked. High CAM CPU After upgrading to or installing 4.1(0), the CAM runs out of tomcat threads if requirements consisting of a large number of checks and rules are used.

Resolved Caveats - Release 4.1(0)

Table 13 List of Closed Caveats

	Software Release 4.1(0)	
DDTS Number	Corrected	Caveat
CSCse46141	Yes	SSO fail in case Clean Access Server [CAS] cannot reach Active Directory [AD] server during startup Steps to reproduce: 1. Shutdown CAS 2. Shutdown Active Directory Server 3. Start CAS and make sure it completely comes up 4. Start Active Directory Server 5. CAS cannot login onto AD and SSO fails Workaround: CAS requires manual login onto AD in case CAS cannot reach AD at startup time. This can be done by clicking “Update” on web page “Device Management > Clean Access Servers > IP Address > Authentication > Windows Auth”
CSCse68178	Yes	ActiveX control version checking fix IE may request installation of ocget.dll. While using activeX for L3 OOB, in some Windows machines, the IE browser pops up a request to install ocget.dll. This does not occur during initial web login when the ActiveX control is not yet installed on the machine. It occurs in subsequent web logins after the Active X control has already been installed. This is a Microsoft bug that makes an unnecessary POST request to ocget.dll.
CSCse69355	Yes	DHCP renew fails using new Relay IP feature but release/renew works This problem is seen when using the new CCA 4.0 feature where DHCP scopes can be defined on the CAS such that IP addresses are allocated based on the Relay IP address (say IP helper). In this scenario, we can see that when the DHCP client performs a ipconfig/renew, then the CAS sends a NAK. However, when the same client performs an ipconfig/release followed by ipconfig/renew, then the CAS is seen to be sending a ACK.

Table 13 List of Closed Caveats (continued)

DDTS Number	Software Release 4.1(0)	
	Corrected	Caveat
CSCse84000	Yes	Cron job to sync system time not created or updated on HA-Inactive CAS The file /etc/cron.daily/sync-time gets created or updated on modifying the time servers for CAS. This cron file does not get created on high availability HA-Inactive CAS, thereby depriving the inactive system to sync the system time from the time servers on a regular basis Steps to reproduce: 1. Setup CAS in HA-failover mode 2. Go to web page: Device Management > Clean Access Servers > IP Address > Misc > Time 3. Change the time servers to “clock.cisco.com” 4. Verify the changes have been reflected in cron job /etc/cron.daily/sync-time on active CAS 5. Check the HA-Inactive CAS for the cron file /etc/cron.daily/sync-time. The file may either not be present or have old time server settings Expected Results: The cron job file to sync the system time on HA-Inactive CAS should reflect the changes upon modification of time server settings on HA-Active CAS using either CAM or HA-Active CAS GUI Workaround: Modify the time servers on HA-Inactive CAS using GUI.
CSCsf01786	Yes	/etc/grub.conf should be a symbolic link to /boot/grub/grub.conf In 3.6.0~3.6.3 and 4.0.0, grub.conf is not changed correctly when ttyS0 is used as the heartbeat link. Some cutomers manually edited /etc/grub.conf manually as a workaround, and some of them break the symbolic link by mistake.The upgrade script should make sure /etc/grub.conf is a symbolic link to /boot/grub/grub.conf
CSCsf17230	Yes	Link creation from normal-webapps to webapps affects flexlm in HA The link from admin-webapps & normal-webapps to webapps upon switching from standby to primary is not being created before the licenses are copied from the database.
CSCsg00598	Yes	Private key needs to be imported back when importing signed certificate from CA When importing signed certificate from the CA, an error appears, stating “The Uploaded CA-Signed Certificate doesn't match the Uploaded Private Key.” Workaround: Import the Private Key that backed up when the CSR was imported

Table 13 List of Closed Caveats (continued)

DDTS Number	Software Release 4.1(0)	
	Corrected	**Caveat**
CSCsg11143	Yes	Unless CAS is rebooted, validation_table is not republished If Active CAS (CAS1) loses connectivity (not rebooted) with the CAM, CAS 2 then becomes active CAS. If user has not enabled heartbeat timer and fails to back to CAS1, the intern_validation_table on CAS1 is not republished from the CAM's database. Instead, it keeps adding to the older entries Workaround: Enabling heartbeat timer will make sure unused entries are deleted over a period of time.
CSCsg14148	Yes	Swap space is not loaded properly when using CCISS driver When the CCISS driver is being used, for e.g with Smartarray6i RAID controllers, the installer does not seem to load the swap space information correctly. Executing a free on the boxes shows no swap space. TOP reveals 0K of SWAP.Also, in some cases, the /etc/fstab file shows a jumbled set of characters for the swap space location
CSCsg23778	Yes	SNMP daemon hangs after executing “snmpwalk” from a remote host Steps to reproduce: 1. Enable SNMP on CAM using web page “Monitoring > SNMP” 2. Verify SNMP daemon running on CAM by executing “snmpwalk -Os -c public -v 2c <CAM_IP_Address> system”. The command will NOT timeout & returns output. 3. Execute “snmpwalk -Os -c public -v 2c <CAM_IP_Address> enterprises.16344”. Command returns partial response; timeouts and then reports no response. 4. Execute “snmpwalk -Os -c public -v 2c <CAM_IP_Address> system”. Command returns no response and timeout. The SNMP daemon hogs 100% CPU on CAM and needs to be restarted
CSCsg24153	Yes	“service perfigo config” does not update shared secret in /root/.secret When changing the shared secret in the CAS and CAM using ‘service perfigo config’, the shared secret between the CAM and CAS is not updated. The existing pre-shared key will remain in use. **Note** This caveat and workaround apply only to releases 4.0.0 to 4.0.3.2 and 3.6.0 to 3.6.4.2. **Note** Apply this workaround first before performing a web upgrade from 4.0(x)/3.6(x) to 4.1(0). **Workaround**: If the customer needs to change the shared secret between the CAM and CAS, then apply patch-CSCsg24153.tar.gz from http://www.cisco.com/cgi-bin/tablebuild.pl/cca-patches.

Table 13 List of Closed Caveats (continued)

DDTS Number	Software Release 4.1(0)	
	Corrected	Caveat
CSCsg41272	Yes	DHCP server re-assigns abandoned leases When the CAS is in Real-IP gateway mode and acting as the DHCP server for untrusted client, it will continue to try to hand out an address that someone has statically set on the network even though the DHCP Client sends a decline for the address. Workaround: Two workarounds are available: 1) Set ping-check to "true" on the DHCP server. This can slow down the connection process in large deployments; 2) Find the static addresses and force the users to use DHCP.
CSCsg41565	Yes	When authenticating w/cookie, cisco_api.jsp not allowed to post to API When using a cookie to authenticate to cisco_api.jsp, authentication fails. In one of the CCA releases, an additional means of security was added when using a cookie or session to see if POST to the API should be permitted or denied. cisco_api.jsp was accidentally left off this list.
CSCsg44268	Yes	Need to accommodate for new daylight saving time regime from 2007.
CSCsg44387	Yes	NAT gateway mode warning inconsistent with CCA documentation When trying to add a NAT Gateway CAS to the CAM, the warning presented, "NAT Gateway is only recommended for demo/testing purposes. For production deployments, Virtual or Real-IP Gateway is recommended", differs from documentation for the CAM, which states that NAT gateway is neither recommended nor supported for production environments. Warning rephrased to match CAM documentation.

Known Issues for Cisco NAC Appliance

This section describes known issues when integrating Cisco NAC Appliance with the following third-party elements:

- Known Issue with NAT/PAT Devices and L3 Deployments
- 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 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 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.

If you have DHCP issues with Airespace controllers after installing/upgrading to release 4.0(2) or above, the following will need to be done to restore DHCP functionality:

Step 1 Enable DHCP options on the CAS:

a. Go to **Device Management > CCA Servers > Manage [CAS_IP] > Network > DHCP > Global Options**

b. Click the **Enable** button (User-Specified DHCP Options).

Step 2 Create a new custom Global DHCP option with option number “54” and option type “IP-Address”:

a. Click the **New Option** link for the Root Global Option List.

b. Type **54** in the **ID** field.

c. Select **IP-Address** from the **Type** dropdown menu.

d. Click the **Create Custom Option** button.

Step 3 Set the value of this option to the CAS eth1 IP address (or eth1 Service IP if CAS is in HA mode):

a. Type the CAS eth1 IP address in the text field.

b. Click **Update**.

Step 4 This should restore DHCP capability with Airespace controllers.

Note For further details on configuring DHCP options, see the *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide*.

Known Issues with Broadcom NIC 5702/5703/5704 Chipsets

Customers running Cisco NAC Appliance release 4.0(x) 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. You will see messages such as the following in /var/log/messages:

```
Mar 21 11:43:02 cas2b kernel: NETDEV WATCHDOG: eth1: transmit timed out Mar 21 11:43:02
cas2b kernel: tg3: eth1: transmit timed out, resetting Mar 21 11:43:02 cas2b kernel: tg3:
tg3_stop_block timed out, ofs=1400 enable_bit=2
Mar 21 11:43:02 cas2b kernel: tg3: tg3_stop_block timed out, ofs=c00 enable_bit=2
Mar 21 11:43:02 cas2b kernel: tg3: eth1: Link is down.
Mar 21 11:43:05 cas2b kernel: tg3: eth1: Link is up at 1000 Mbps, full duplex.
Mar 21 11:43:05 cas2b kernel: tg3: eth1: Flow control is off for TX and off for RX.
```

The fundamental cause of this problem is a firmware bug in the Broadcom chipsets used in HP servers. Version 4.0(x) of the CCA software is impacted by this bug.

Solution

1. Verify the type of NIC controller being used on your CAM/CAS servers by looking at the output of the **`lspci -v`** command.
2. If your machine has the 5702/5703/5704 Broadcom chipset, you must apply the firmware upgrade from HP available at: http://h18023.www1.hp.com/support/files/networking/us/download/24056.html

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

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 above. 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(0)

Note Release 4.1.0.2 obsoletes and replaces releases 4.1.0.1 and 4.1(0).

Warning **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. You will be able to upgrade NAC 3300 Series appliances to upcoming release 4.1(1) (which includes Cavium SSL accelerator support). Refer to the *Release Notes for Cisco NAC Appliance (Cisco Clean Access) for Version 4.1(1)* for details.**

If you purchased and/or are performing a new 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(0), page 58.

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 60.
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 on each Clean Access Server and Clean Access Manager, as follows:
   a. Insert the product CD in the CD-ROM drive for each target installation machine, and follow the auto-run procedures.
   b. Or, login to Cisco Secure Software and download the latest 4.1.0.ISO 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. Follow the instructions in the auto-run installer.
4. After software installation, access the Clean Access Manager web admin console by opening a web browser and typing the IP address of the CAM as the URL. The Clean Access Manager License Form will appear the first time you do this to prompt you to install your FlexLM license files.
5. Install a valid FlexLM license file for the Clean Access Manager (either evaluation, starter kit, or individual license). You should have already acquired license files as described in Cisco NAC Appliance Service Contract/Licensing Support, page 2.
6. At the admin login prompt, login with the default user name and password **`admin/cisco123`** or with the web console username and password you configured when you installed the Clean Access Manager.
7. In the web console, navigate to **Administration > CCA Manager > Licensing** if you need to install any additional FlexLM license files for your Clean Access Servers.
8. For detailed software installation steps and further steps for adding the Clean Access Server(s) to the Clean Access Manager and performing basic configuration, refer to the following guides, available from: http://www.cisco.com/en/US/products/ps6128/products_user_guide_list.html:
   - *Cisco NAC Appliance - Clean Access Manager Installation and Administration Guide, Release 4.1*
   - *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide, Release 4.1*

Note Clean Access Manager 4.1.0.2 is bundled with Clean Access Agent 4.1.0.2.

Upgrading to 4.1(0)

This section provides instructions for how to upgrade your existing Cisco Clean Access system to release 4.1(0).

Refer to the following general information prior to upgrade:

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

If you need to perform a fresh installation of the software, refer instead to New Installation of Release 4.1(0), page 56.

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(0). 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(0) Upgrade

Note Release 4.1.0.2 obsoletes and replaces releases 4.1.0.1 and 4.1(0). If your system is running 4.0(x), 3.6(x) or 3.5(x), and you wish to upgrade to release 4.1(0), upgrade to release 4.1.0.2 directly.

Note Releases 4.1(0), 4.1.0.1, or 4.1.0.2 do not support Windows Vista. Only 4.0(x) releases starting from 4.0(4) and 4.0.x.x Agent versions starting from 4.0.4.0 support Windows Vista.

Warning **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. You will be able to upgrade NAC 3300 Series appliances to upcoming release 4.1(1) (which includes Cavium SSL accelerator support). Refer to the *Release Notes for Cisco NAC Appliance (Cisco Clean Access) for Version 4.1(1)* for details.**

If planning to upgrade to Cisco NAC Appliance (Cisco Clean Access) 4.1(0) ED, note the following:

- Cisco NAC Appliance (Cisco Clean Access) release 4.1(0) ED is a major software release with Early Deployment status.
- Cisco recommends using the console/SSH upgrade procedure to upgrade from release 3.6(x) or 4.0(x) to release 4.1(0). See Console/SSH Upgrade—Standalone Machines, page 75.

Note When upgrading from 3.6(x)/4.0(x) to the latest 4.1(0) release, you can only perform web console upgrade on **standalone** non-HA CAM machines if they have been patched for caveat CSCsg24153, page 51. Standalone CAS machines will still need to be upgraded from 3.6(x)/4.0(x) to the latest 4.1(0) release using the console/SSH upgrade procedure.

If the system has not already been patched, upgrade both your machines via console/SSH. For details on Patch-CSCsg24153, refer to the README-CSCsg24153 file under http://www.cisco.com/cgi-bin/tablebuild.pl/cca-patches.

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 80.**

- You can upgrade from release 3.5(x) to 4.1.0.2 using 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(0)—Standalone Machines, page 61. For HA systems, refer to In-Place Upgrade from 3.5(7)+ to 4.1(0)—HA-Pairs, page 64
- **Read and review the installation or upgrade instructions completely before starting. The 3.5(x)+ to 4.1(0) 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 running either 4.0(x) or 3.6(x) or upgrading from 3.5(x), you will need to perform a firmware upgrade from HP. See Known Issues with Broadcom NIC 5702/5703/5704 Chipsets, page 54 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, 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 3.5/3.6 to 4.1, 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.
- If you need further assistance, contact TAC as described in Obtaining Documentation, Obtaining Support, and Security Guidelines, page 92.

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 software and some running 4.0 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. 4.1.0 to 4.1.0.2), 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 the 3.5(x)+ to 4.1(0) in-place upgrade procedure, 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 re-establishes connectivity with the Clean Access Manager.

- **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. Make sure to download the snapshots to your desktop/laptop for safekeeping. 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 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 also Create CAM DB Backup Snapshot, page 71.

Warning **You cannot restore a 4.0 or earlier database to a 4.1 Clean Access Manager.**

- **Software Downgrade**

  Once you have upgraded your software to 4.1, 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.

- **Passwords**

  For upgrade via console/SSH, you will need your CAM and CAS **`root`** user password (default 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(0)—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(0) 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(0)—HA-Pairs, page 64.

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

- Upgrading to 4.1(0), page 58
- Settings That May Change With Upgrade, page 59
- General Preparation for Upgrade, page 60

In-Place Upgrade Summary

The Cisco Clean Access 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.

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(0) installation CD shipped with your deployment of Cisco NAC Appliance, continue to Mount the CD-ROM and Run the Upgrade File, page 62.

Step 2 If the 4.1(0) 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 Clean Access Software. On the Cisco Secure Software page for Cisco Clean Access, click the link for the appropriate 4.1(0) release. Download the following file to a local computer (replace the **.x** and **.y** in the filename with the appropriate version, for example, `cca-4.1_0_2-K9.iso`):

cca-4.1_x_y-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(0) 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 release 4.1(0).

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 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(0) 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.

Step 10 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 11 At the following prompt, type **y** to continue with the upgrade:

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

Step 12 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 13 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 Installer (C) 2006 Cisco Systems, Inc.
                Welcome to the Cisco Clean Access Installer!

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

Step 14 The 4.1(0) 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 15 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 16 After pressing Enter on the previous step, the machine will reboot, then reboot again, then come up normally.

Complete the In-Place Upgrade

Step 17 The 4.1(0) upgrade is successfully installed when the installation CD is ejected from the machine and the login prompt appears:

```
<ccahostname> login:
```

Step 18 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 19 This completes the 4.1(0) upgrade procedure. Repeat the procedure for each machine to be upgraded to 4.1(0).

Note After performing 3.5(x)-to-4.1(0) migration, the very first time you log into the 4.1(0) 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(0)—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(0) release.

If you have standalone CAM/CAS servers, refer instead to In-Place Upgrade from 3.5(7)+ to 4.1(0)—Standalone Machines, page 61.

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

- Upgrading to 4.1(0), page 58
- Settings That May Change With Upgrade, page 59
- General Preparation for Upgrade, page 60
- Upgrading from 3.6(x)/4.0(x)—HA Pairs, page 78 (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(0) product CD. If not, follow the steps to Create the Installation CD, page 62.

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.**

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(0) 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.

Step 10 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 11 At the following prompt, type **y** to continue with the upgrade:

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

Step 12 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 13 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 Installer (C) 2006 Cisco Systems, Inc.
                Welcome to the Cisco Clean Access Installer!
```

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

Step 14 The 4.1(0) 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 15 If a warning displays because NIC cards have been re-ordered, follow the instructions for Swap Ethernet Cables (if Necessary), page 63.

Note For CAM upgrade, the 4.1.0.2 upgrade script automatically upgrades the Clean Access Agent files inside the CAM to version 4.1.0.2.

Step 16 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 17 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 18 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 19 Wait until the active box is done shutting down:

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

Step 20 Boot up the standby box by powering up the box.

Step 21 **Insert the 4.1(0) installation CD into the CD-ROM drive of the standby machine to be upgraded.**

Step 22 Mount the CD-ROM on the standby machine (use the command: `mount /dev/cdrom /<mountpoint directory>`), for example:

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

Step 23 Change to the mountpoint directory:

```
cd /mnt
```

Step 24 Run the upgrade file:

```
./upgrade.sh
```

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

Step 25 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 4.0 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 26 At the following prompt, type **`y`** to continue with the upgrade:

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

Step 27 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 28 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 Installer (C) 2006 Cisco Systems, Inc.
                Welcome to the Cisco Clean Access Installer!

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

Step 29 The 4.1(0) 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 30 If a warning displays because NIC cards have been re-ordered, follow the instructions for Swap Ethernet Cables (if Necessary), page 63.

Note For CAM upgrade, the 4.1.0.2 upgrade script automatically upgrades the Clean Access Agent files inside the CAM to version 4.1.0.2.

Step 31 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 32 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 33 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 34 Power up the active box. Wait until it is running normally and connection to the web console is possible

Step 35 Power up the standby box.

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

Step 36 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(0) migration, the very first time you log into the 4.1(0) 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)—Standalone Machines

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

- Web Console Upgrade—Standalone Machines, page 72
- Console/SSH Upgrade—Standalone Machines, page 75

Note

- If upgrading high-availability (HA) pairs of CAM or CAS servers running 3.6(x)/4.0(x), refer instead to Upgrading from 3.6(x)/4.0(x)—HA Pairs, page 78.
- If upgrading your system from release 3.5(x), refer instead to In-Place Upgrade from 3.5(7)+ to 4.1(0)—Standalone Machines, page 61.

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

- Upgrading to 4.1(0), page 58
- Settings That May Change With Upgrade, page 59
- General Preparation for Upgrade, page 60

Summary of Steps for 3.6/4.0 Upgrade

The sequence of steps for standalone 3.6(x)/4.0(x) system upgrade is as follows:

1. Create CAM DB Backup Snapshot, page 71
2. Download the Upgrade File, page 71
3. Web Console Upgrade—Standalone Machines or
   Console/SSH Upgrade—Standalone Machines, page 75

Create CAM DB Backup Snapshot

Perform a full backup of your CAM database by creating a backup snapshot both before and after the upgrade. Make sure to download the snapshots to your desktop/laptop for safekeeping. 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 3.6 database.

Warning **Back up your database BEFORE you upgrade.**

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. 02_09_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, which is added to the snapshot list at the bottom of the page. Note that the software version is automatically recorded in the **Version** field and also appended to the name of the downloadable file for convenience (e.g. 02_09_07-14-58_snapshot_**VER_4.1.0.1.**gz).

Note The file still physically resides on the CAM machine, and can remain there for archiving purposes. However, to back up a configuration for use in case of system failure, the snapshot should be downloaded to another computer.

Step 4 To download the snapshot to another computer, click 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), 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) 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. Upgrade files use the following format (for patch upgrades, replace the .x and .y in the file name with the minor release version numbers to which you are upgrading, for example, `cca_upgrade-4.1.0.2.tar.gz`):

- **cca_upgrade-4.1.0.y.tar.gz** (CAM/CAS release upgrade file)
- **cam-upgrade-4.1.0.y.tar.gz** (CAM-only patch upgrade file)
- **cas-upgrade-4.1.0.y.tar.gz** (CAS-only patch upgrade file)

Step 3 Download the file to the local computer from which you are accessing the CAM web console.

Web Console Upgrade—Standalone Machines

Note Cisco recommends using console/SSH to upgrade your machines from 3.6(x)/4.0(x) to 4.1(0). See Console/SSH Upgrade—Standalone Machines, page 75.

When upgrading from 3.6(x)/4.0(x) to the latest 4.1(0) release, you can only perform web console upgrade on **standalone** non-HA CAM machines if they have been patched for caveat CSCsg24153, page 51. Standalone CAS machines will still need to be upgraded from 3.6(x)/4.0(x) to the latest 4.1(0) release using the console/SSH upgrade procedure.

If the system has not already been patched, upgrade both your machines via console/SSH. For details on Patch-CSCsg24153, refer to the README-CSCsg24153 file under http://www.cisco.com/cgi-bin/tablebuild.pl/cca-patches.

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 80.**

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_address] > Misc** (CAS management pages)
  - Or: **https://<CAS_eth0_IP>/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) or above must be installed and running on your CAM/CAS(es) before you can upgrade to release 4.1(0) via web console.
- If upgrading failover pairs, refer to Upgrading from 3.6(x)/4.0(x)—HA Pairs, page 78.
- Alternatively, you can always upgrade using the instructions in Console/SSH Upgrade—Standalone Machines, page 75.

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) or above to release 4.1(0) using web upgrade via the CAS management pages as described below or, if preferred, using the instructions for Upgrade CAS from CAS Direct Access Web Console, page 74.

Step 1 Create CAM DB Backup Snapshot, page 71.

Step 2 Download the Upgrade File, page 71.

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 file you just downloaded from Cisco Downloads (e.g., **cca_upgrade-4.1.0.y.tar.gz**).

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 7)

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

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

Upgrade CAS from CAS Direct Access Web Console

You can upgrade the CAS from the CAS direct access web console using the following instructions. To upgrade the CASes from the CAM web console, see Upgrade CAS from CAS Management Pages, page 73.

Step 1 Create CAM DB Backup Snapshot, page 71.

Step 2 Download the Upgrade File, page 71.

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>/admin** (for example, `https://172.16.1.2/admin`)

a. Accept the temporary certificate and log in as user `admin` (default password is `cisco123`).

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

Step 5 Click **Browse** to locate the upgrade file you just downloaded from Cisco Downloads (e.g., `cca_upgrade-4.1.0.y.tar.gz`).

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 7)

Step 10 Repeat steps 3 to 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 80.**

Step 1 Create CAM DB Backup Snapshot, page 71.

Step 2 Download the Upgrade File, page 71.

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 file you just downloaded from Cisco Downloads (e.g., `cca_upgrade-4.1.0.y.tar.gz`).

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 see the new version, “Cisco Clean Access Manager Version 4.1.0,” at the top of the web console. (See also Determining the Software Version, page 7.)

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) or 4.0(x) to the latest 4.1(0) 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), refer instead to Upgrading from 3.6(x)/4.0(x)—HA Pairs, page 78.
- If upgrading your system from 3.5(x), refer instead to In-Place Upgrade from 3.5(7)+ to 4.1(0)—Standalone Machines, page 61.

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 file, **cca_upgrade-4.1.0.y.tar.gz**, 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 above.

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) to 4.1 console/SSH upgrade instructions:

- Upgrading to 4.1(0), page 58
- Settings That May Change With Upgrade, page 59
- General Preparation for Upgrade, page 60

Summary of Steps for Console/SSH Upgrade from 3.6(x)/4.0(x)

Steps are as follows:

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

Download the Upgrade File and Copy to CAM/CAS

Step 1 Create CAM DB Backup Snapshot, page 71.

Step 2 Download the Upgrade File, page 71.

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 (for patch upgrades, replace the .x and .y in the file name with the minor release version numbers to which you are upgrading)

If using WinSCP or SSH File Transfer (replace .x with upgrade version number):

a. Copy **cca_upgrade-4.1.0.y.tar.gz** to the /store directory on the Clean Access Manager.

b. Copy **cca_upgrade-4.1.0.y.tar.gz** to the /store directory on **each** Clean Access Server.

If using PSCP (replace .x with upgrade version number):

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 (replace .x with upgrade version number) to the CAM:

```
pscp cca_upgrade-4.1.0.y.tar.gz root@ipaddress_manager:/store
```

d. Enter the following command to copy the file (replace .x with upgrade version number) to the CAS (copy to each CAS):

```
pscp cca_upgrade-4.1.0.y.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 the `root` user with root **password** (default password is `cisco123`)

c. Change directory to /store:

```
cd /store
```

d. Uncompress the downloaded file (replace .x with upgrade version number):

```
tar xzvf cca_upgrade-4.1.0.y.tar.gz
```

4. Execute the upgrade process (replace .x with upgrade version number):

```
cd cca_upgrade-4.1.0.y
./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 table entry in Resolved Caveats - Release 4.1(0), page 49.

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

Note For CAM upgrade, the 4.1.0.2 upgrade script automatically upgrades the Clean Access Agent files inside the CAM to version 4.1.0.2.

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` with root password (default password is `cisco123`)/

c. Change directory to /store:

```
cd /store
```

d. Uncompress the downloaded file (replace .x with upgrade version number):

```
tar xzvf cca_upgrade-4.1.0.y.tar.gz
```

5. Execute the upgrade process (replace .x with upgrade version number):

```
cd cca_upgrade-4.1.0.y
```

```
./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 table entry in Resolved Caveats - Release 4.1(0), page 49.

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)—HA Pairs

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

If you have standalone CAM/CAS servers, refer instead to Upgrading from 3.6(x)/4.0(x)—Standalone Machines, page 70.

Note Your system must be on 3.6(x)/4.0(x) 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(0)—HA-Pairs, page 64.

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.**

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 80.**

Note Review the following before proceeding with the 3.6(x)/4.0(x) to 4.1 HA upgrade instructions:

- Upgrading to 4.1(0), page 58
- Settings That May Change With Upgrade, page 59

- General Preparation for Upgrade, page 60

Steps for HA 3.6/4.0 Upgrade

The steps to upgrade HA 3.6(x)/4.0(x) 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>/admin**. For example, `https://172.16.1.2/admin`
- For the Secondary CAS, type: **https://<secondary_CAS_eth0_IP>/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.**

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 76 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 (replace the .x in the file name with the upgrade version number):

```
tar xzvf cca_upgrade-4.1.0.y.tar.gz
```

b. CD into the created “cca_upgrade-4.1.0.y directory” 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 79, 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-4.1.0.y" directory on the active box.

```
cd cca_upgrade-4.1.0
```

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-4.1.0.y"), 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 table entry in Resolved Caveats - Release 4.1(0), page 49.

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 4.1.0.2 upgrade script automatically upgrades the Clean Access Agent files inside the CAM to version 4.1.0.2.

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-4.1.0.y
```

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 4.1.0/4.0.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 71 for details.

Creating CAM/CAS Support Logs

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

- CAM web console: **Administration > CCA Manager > Support Logs**
- CAS direct access console (https://<CAS_eth0_IP>/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_address] > 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 4.1.0/4.0.x/3.6.x)

Use the following procedure to recover the root password for a 4.1.0/4.0.x/3.6.x 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. The time set on the CAM and the CAS must be 5 minutes apart or less:
(under **Administration > CCA Manager > System Time**, and
Device Management > CCA Servers > Manage [CAS_IP] > Misc > Time

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 IE 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 8)
- 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 7).
2. Version of client OS (e.g. Windows XP SP2)
3. Version of Cisco Updates ruleset (see Cisco Clean Access Updates Versioning, page 8(
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 86.
9. If necessary, provide CAM support logs as described in Creating CAM/CAS Support Logs, page 83.

Enable Debug Logging on the Clean Access Agent

For version 4.1.0.0+ 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 OSes, 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 below, 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 below, 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 below, the Agent installation directory is C:\Program Files\Cisco\Clean Access\.

Generate Mac OS Agent Debug Log

For Mac OS Agents (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 Clean Access (NAC Appliance) Version 4.1.0.x

Date	Description
1/30/08	Applied new template and updated trademark information
1/11/08	Added caveat CSCsi97216 to Open Caveats - Release 4.1.0.2, page 40
9/11/07	Added Known Issue with NAT/PAT Devices and L3 Deployments, page 53.
5/21/07	Removed Caveat CSCsg02412 (Unreproducible)
5/11/07	Add Caveat CSCsi86205 to Open Caveats - Release 4.1.0.2, page 40
4/26/07	Add Caveat CSCsg98960 to Open Caveats - Release 4.1.0.2, page 40
4/24/07	• Add Caveat CSCsi23228 to Open Caveats - Release 4.1.0.2, page 40 • Modified instances of “4.1(x)” and “4.1.x” to specify “4.1(0)” and “4.1.0” (for these release notes) • Reduced boilerplate to point to Obtaining Documentation, Obtaining Support, and Security Guidelines, page 92.
3/19/07	Moved Caveat CSCsi07595 to Open Caveats - Release 4.1.0.2, page 40.
3/9/07	Added Caveat CSCsi07595 to address the DST 2007 fix.
2/9/07	Updates for release 4.1.0.2 • Updated Software Compatibility Matrixes, page 4 • Added Enhancements in Release 4.1.0.2, page 9 • Updated Clean Access Supported AV/AS Product List, page 21 for version 50 • Updated Clean Access Agent Version Summary, page 39 for Agent release 4.1.0.2 • Added Open Caveats - Release 4.1.0.2, page 40 • Added Resolved Caveats - Release 4.1.0.2, page 47 • Updated Upgrading to 4.1(0), page 58
1/18/07	Added Symantec Enterprise products AntiVirus update footnote to Clean Access AV Support Chart (Windows XP / 2000), page 22.
1/11/07	Added caveat CSCsh39119 to Open Caveats - Release 4.1.0.2, page 40.

Table 14 Updates to Release Notes for Cisco Clean Access (NAC Appliance) Version 4.1.0.x

Date	Description
1/5/07	Various updates/corrections: • Updated CAM Lite, Standard, Super, page 7 section • Updated Release 4.1(0) CAM/CAS Upgrade Compatibility Matrix, page 6 and propagated NAC-3300 upgrade restriction note throughout. • Added note to Enhancements in Release 4.1.0.1, page 10 and Searchable Clean Access Agent Reports, page 16. • Added Clean Access Agent Installation Options, page 14 description • Added note to DHCP Subnet List Enhancements, page 17 • Updated Supported AV/AS Product List Version Summary, page 36. • Moved CSCsf17230, page 50 to Resolved Caveats - Release 4.1.0.1. Removed caveats CSCsf16537 and CSCsg01408 from Open Caveats - Release 4.1.0.2, page 40. • Various updates to Upgrading to 4.1(0), page 58 • Updated In-Place Upgrade from 3.5(7)+ to 4.1(0)—HA-Pairs, page 64, and Determine Active and Standby Machines, page 65. • Added Agent Error: “Network Error SSL Certificate Rev Failed 12057”, page 85 to Troubleshooting section • Updated Enable Debug Logging on the Clean Access Agent, page 86 for Mac OS. • Updated Related Documentation, page 90 • Updated template/boilerplate. • Corrected broken URL links; various other corrections throughout
12/4/06	Updates for patch release 4.1.0.1 • Updated Software Compatibility Matrixes, page 4 • Added Enhancements in Release 4.1.0.1, page 10 • Updated Clean Access Supported AV/AS Product List, page 21 for version 46 • Added Resolved Caveats - Release 4.1.0.1, page 48 • Added CSCsg44268 to Resolved Caveats - Release 4.1(0), page 49 Also: • Updated System Requirements, page 2 section • Reorganized subsections under Upgrading to 4.1(0), page 58. • Updated boilerplate info (“Obtaining Documentation” etc.) Removed sections: • “Current Supported Components Required for Super CAM” • “CCA Admin Console System Requirements” • Troubleshooting: “Clean Access Agent 4.0.1.0 and IE 7.0 Beta” and “Recovering Root Password for CAM/CAS (Release 3.5.x or Below)”
11/14/06	Release 4.1(0)

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 Administration Guide, Release 4.1(0)*
- *Cisco NAC Appliance - Clean Access Server Installation and Administration Guide, Release 4.1(0)*
- *What's New in Cisco NAC Appliance 4.1(0)*
- *Release Notes for Cisco NAC Appliance (Cisco Clean Access) Version 4.1(0)*
- *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, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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.

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.