Release Notes for Cisco Clean Access (NAC Appliance) Version 3.6(4)

Revised: April 16, 2008, OL-8543-01

Contents

These release notes provide late-breaking and release information for Cisco® Clean Access (NAC Appliance), release 3.6(x). This document describes new features, changes to existing features, limitations and restrictions ("caveats"), fixes, upgrade instructions, and related documentation. These release notes supplement the Cisco Clean Access documentation included with the distribution. Read these release notes carefully and refer to the upgrade instructions before installing this release.

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

Cisco Clean Access (NAC Appliance) Releases

Cisco Clean Access (NAC Appliance) Version	Availability
3.6.4.4 GD	April 1, 2008
3.6.4.3 GD	January 22, 2007
3.6.4.2 GD	September 18, 2006
3.6.4.1 GD	August 4, 2006
3.6(4) GD	August 2, 2006
3.6(3) GD	June 21, 2006
3.6.2.2 ED	March 29, 2006
3.6.2.1 ED	March 24, 2006
3.6(2) ED	March 20, 2006
3.6.1.1 ED	February 21, 2006
3.6(1) ED	February 15, 2006
3.6.0.1 ED	December 30, 2005
3.6(0) ED	December 9, 2005

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 *Cisco NAC Appliance Service Contract/Licensing Support*.

System and Hardware Requirements

This section describes the following:

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

Hardware Supported

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

- Supported server hardware configurations
- Pre-installation instructions for applicable server configurations
- System requirements for Clean Access Manager (CAM), Clean Access Server (CAS), Clean Access Agent (CAA)
- Troubleshooting information for network card driver support

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 Clean Access. Elements in the same row are compatible with each other.

Table 1 VPN and Wireless Components Supported By Cisco® Clean Access For SSO

Cisco Clean Access Version	VPN Concentrator/Wireless Controller	VPN Clients
3.6(x)	Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs)	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	

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

For further details, see the *Cisco Clean Access (NAC Appliance) Manager Installation and Administration Guide, Release 3.6* and the *Cisco Clean Access (NAC Appliance) Server Installation and Administration Guide, Release 3.6*.

Software Compatibility

This section describes software compatibility for releases of Cisco Clean Access:

- Software Compatibility Matrixes
- Determining the Software Version
- Web Browser Compatibility

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

- Clean Access Supported AV/AS Product List, page 43
- Clean Access Agent Version Summary, page 63

Software Compatibility Matrixes

This section describes the following:

- Release 3.6(x) Compatibility Matrix
- Release 3.6(x) CAM/CAS Upgrade Compatibility Matrix
- Release 3.6(x) Agent Upgrade Compatibility Matrix

Release 3.6(x) Compatibility Matrix

Table 3, "Release 3.6(x) Compatibility Matrix" shows Clean Access Manager and Clean Access Server compatibility and the Agent version bundled with each CCA 3.6(x) release (if applicable). CAM/CAS/Agent versions displayed in the same row are compatible with one another. Cisco recommends that you synchronize your software images to match those shown as compatible in the table.

Table 2 Release 3.6(x) Compatibility Matrix

Clean Access Manager	Clean Access Server	Clean Access Agent [1]
3.6.4.4 [2]	3.6.4.4 [2]	3.6.5.0
3.6.4.3 [3]	3.6.4.3 [3]	
3.6.4.2 [4]	3.6.4.1 [5]	3.6.4.0
3.6.4.1 [5]		
3.6(4)	3.6(4)	
3.6(3)	3.6(3)	3.6.3.1[6]
		3.6.3.0
3.6.2.2 [7]	3.6.2.1 [8]	3.6.2.0
3.6.2.1 [8]		
3.6(2)	3.6(2)	
3.6.1.1 [9]	3.6.1.1 [9]	3.6.1.0
3.6(1) [10]	3.6(1) [10]	
3.6.0.1 [11]	3.6.0.1 [11]	3.6.0.1 [11]
3.6(0)	3.6(0)	3.6.0.0

1. 3.6(x) Clean Access Agents have 4-digit versioning (last digit shows updates related to Supported AV/AS Product List). Prior versions of the 3.6.x.x. Clean Access Agent are compatible with the latest 3.6(x) CAM/CAS release, unless otherwise specified.
2. Patch release 3.6.4.4 is a general patch release for the CAM and CAS that addresses a Cisco PSIRT issue involving caveat CSCsj33976. See Resolved Caveats - Release 3.6.4.4, page 67 for more information. In-place upgrade is not supported.
3. Patch release 3.6.4.3 is an upgrade-only patch applied to the CAM and CAS. Your system must be running 3.6(x) to upgrade to 3.6.4.3; CD installation and in-place upgrade are not supported. See Enhancements for Release 3.6.4.3, page 10 and Resolved Caveats - Release 3.6.4.3, page 68 for details.
4. Patch release 3.6.4.2 is applied to the CAM only. For complete upgrade compatibility details and instructions, see Enhancements for Release 3.6.4.2, page 13. See also Resolved Caveats - Release 3.6.4.2, page 70 for details.
5. Release 3.6.4.1 must be applied only when **upgrading** 3.6(x) CAM/CAS systems, and resolves caveat CSCse97903, page 71. If upgrading a 3.6(x) system, you must upgrade to 3.6.4.1. If migrating from 3.5(x) or performing a **new** 3.6(x) installation, you can use the 3.6(4) ISO CD and there is no need to install the 3.6.4.1 patch. See Enhancements for Release 3.6.4.1, page 15.
6. Agent 3.6.3.1 resolves caveats CSCse72371, CSCse72384, CSCse72396. See Clean Access Agent Enhancements (3.6.3.1), page 19.
7. Release 3.6.2.2 is applied to 3.6.2.1 CAMs and resolves caveat CSCsd79205, page 73. See Enhancements for Release 3.6.2.2, page 20.
8. Release 3.6.2.1 is applied to 3.6(2) systems and resolves caveat CSCsd74376, page 74. See Enhancements for Release 3.6.2.1, page 22.
9. Release 3.6.1.1 is applied to 3.6.x-to-3.6.1 upgraded systems. You do not need to apply it to 3.5.9-to-3.6.1 migrated systems. See Enhancements for Release 3.6.1.1, page 28 for details.
10. Release 3.6(1) and above resolves caveat CSCsd08348, page 79.
11. Release 3.6.0.1 and above includes CCA Security Patch-CSCsc85405 and upgrade to CAM/CAS/Agent 3.6.0.1 or above is necessary to support Spybot AS products. CAM/CAS 3.6(0) supports Agent 3.6.0.1 minus Enhancements for Release 3.6.0.1, page 34.

Release 3.6(x) CAM/CAS Upgrade Compatibility Matrix

Table 3, "Release 3.6 CAM/CAS Upgrade Compatibility Matrix" shows 3.6 CAM/CAS upgrade compatibility. You can upgrade/migrate your CAM/CAS from the previous release(s) specified to the latest release shown in the same row.

Table 3 Release 3.6 CAM/CAS Upgrade Compatibility Matrix

Clean Access Manager		**Clean Access Server**	
Upgrade From:	**To:**	**Upgrade From:**	**To:**
3.6(x)	3.6.4.4 [1]	3.6(x)	3.6.4.4 [1]
3.6(x)	3.6.4.3 [2]	3.6(x)	3.6.4.3 [2]
3.6.4.1	3.6.4.2[3]	-	-
3.6(4) 3.6(3) 3.6(2) 3.6(1) 3.6(0)	3.6.4.1[4]	3.6(4) 3.6(3) 3.6(2) 3.6(1) 3.6(0)	3.6.4.1 [4]
3.6(1) 3.6(0) 3.5(11) [5] 3.5(10) 3.5(9) 3.5(8) 3.5(7)	3.6(4)	3.6(1) 3.6(0) 3.5(11) [5] 3.5(10) 3.5(9) 3.5(8) 3.5(7)	3.6(4)

Table 3 Release 3.6 CAM/CAS Upgrade Compatibility Matrix

Clean Access Manager		Clean Access Server	
Upgrade From:	**To:**	**Upgrade From:**	**To:**
3.6.2.2 3.6.2.1 3.6(2) 3.6(1) 3.6.0.1 3.6(0) 3.5(10) [5] 3.5(9) 3.5(8) 3.5(7)	3.6(3)	3.6.2.1 3.6(2) 3.6(1) 3.6.0.1 3.6(0) 3.5(10) [5] 3.5(9) 3.5(8) 3.5(7)	3.6(3)
3.6.2.1	3.6.2.2 [6]	3.6(2)	3.6.2.1 [7]
3.6(2)	3.6.2.1 [7]		
3.6(1) 3.6.0.1 3.6(0) 3.5(10) [5] 3.5(9) 3.5(8) 3.5(7)	3.6(2)	3.6(1) 3.6.01 3.6(0) 3.5(10)[5] 3.5(9) 3.5(8) 3.5(7)	3.6(2)
3.6(1)	3.6.1.1 [8]	3.6(1)	3.6.1.1 [8]
3.6.0.1 3.5(9) [5]	3.6(1) [9]	3.6.0.1 3.5(9) [5]	3.6(1) [9]
3.6(0)	3.6.0.1 [10]	3.6(0)	3.6.0.1 [10]
3.5(8) [5] 3.5(7)	3.6(0)	3.5(8) [5] 3.5(7)	3.6(0)

1. Patch release 3.6.4.4 is a general patch release for the CAM and CAS that addresses a Cisco PSIRT issue involving caveat CSCsj33976. See Resolved Caveats - Release 3.6.4.4, page 67 for more information. In-place upgrade is not supported.
2. Patch release 3.6.4.3 is an upgrade-only patch applied to the CAM and CAS. Your system must be running 3.6(x) to upgrade to 3.6.4.3; CD installation and in-place upgrade are not supported. See Enhancements for Release 3.6.4.3, page 10 and Resolved Caveats - Release 3.6.4.3, page 68 for details.
3. Patch release 3.6.4.2 is applied to the CAM only. For complete upgrade compatibility details and instructions, see Enhancements for Release 3.6.4.2, page 13. See also Resolved Caveats - Release 3.6.4.2, page 70 for details.
4. Release 3.6.4.1 must be applied only when **upgrading** 3.6(x) CAM/CAS systems, and resolves caveat CSCse97903, page 71. If upgrading a 3.6(x) system, you must upgrade to 3.6.4.1. If migrating from 3.5(x) or performing a **new** 3.6(x) installation, you can use the 3.6(4) ISO CD and there is no need to install the 3.6.4.1 patch. See Enhancements for Release 3.6.4.1, page 15.
5. To upgrade from a 3.5(x) release to a 3.6(x) release you must use the migration/upgrade procedure. See Migrating/Upgrading from 3.5(7)/3.5(8)/3.5(9)/3.5(10)/3.5(11) to 3.6(x), page 87 for details.
6. Release 3.6.2.2 is applied to 3.6.2.1 CAMs and resolves caveat CSCsd79205, page 73. See Enhancements for Release 3.6.2.2, page 20.
7. Release 3.6.2.1 is applied to 3.6(2) systems and resolves caveat CSCsd74376, page 74. See Enhancements for Release 3.6.2.1, page 22.
8. Release 3.6.1.1 is applied to 3.6.x-to-3.6.1 upgraded systems. You do not need to apply it to 3.5.9-to-3.6.1 migrated systems. See Enhancements for Release 3.6.1.1, page 28 for details.
9. Release 3.6(1) and above resolves caveat CSCsd08348, page 79.
10. Release 3.6.0.1 and above includes CCA Security Patch-CSCsc85405 and upgrade to CAM/CAS/Agent 3.6.0.1 or above is necessary to support Spybot AS products. CAM/CAS 3.6(0) supports Agent 3.6.0.1 minus Enhancements for Release 3.6.0.1, page 34.

Release 3.6(x) Agent Upgrade Compatibility Matrix

Table 4, "Release 3.6(x) Agent Upgrade Compatibility Matrix" shows Clean Access Agent upgrade compatibility.

Table 4 Release 3.6(x) Agent Upgrade Compatibility Matrix

Clean Access Manager	Clean Access Server	Clean Access Agent [1]	
		Upgrade From:	To Latest Version: [2]
3.6(x)	3.6(x)	3.6.x.x	3.6.5.0
		3.5.x [3,4]	

1. 3.6(x) Clean Access Agents have 4-digit versioning (last digit shows updates related to Supported AV/AS Product List). Prior versions of the 3.6.x.x. Clean Access Agent are compatible with the latest 3.6(x) CAM/CAS release, unless otherwise specified. See Clean Access Agent Version Summary, page 63 for additional details.
2. Agent 3.6.3.1 resolves caveats CSCse72371, CSCse72384, CSCse72396. See Clean Access Agent Enhancements (3.6.3.1), page 19.
3. Upgrade 3.5.12 Agent directly to 3.6.2.0+ Agent. You cannot upgrade 3.5.12 Agent to 3.6.0.0/3.6.0.1/3.6.1.0.
4. Upgrade 3.5.11 Agent directly to 3.6.1.0/3.6.2.0 Agent. You cannot upgrade 3.5.11 Agent to 3.6.0.0/3.6.0.1. See caveat CSCsd28300, page 80 for details.

Note

- Except for the Agent upgrade restrictions noted in Table 4, auto-upgrade is supported from any 3.5.1+ Agent directly to the latest 3.6.x.x Agent.
- Agents are not supported across major releases. Do not use 3.6.x.x Agents with 3.5(x) releases or vice versa. However, the upgrade of 3.5.x Agents to 3.6.x.x Agents is supported.

Web Browser Compatibility

- The 3.6(x) CAM/CAS web admin console supports the Internet Explorer 6.0 browser. The web admin console requires high encryption (64 or 128 bit) and does not accept 56-bit encryption.
- High encryption is also required for client browsers for web login and Clean Access Agent authentication.

Note Cisco NAC Appliance does not support beta versions of third-party software, except where specifically noted.

Determining the Software Version

Clean Access Manager

- From the web administration console, you can determine the version of the CAM from **Administration > CCA Manager > System Upgrade**. The software version and date are listed in the **Current Version** field.
- From an SSH connection to the machine, you can determine the version of code running on a Clean Access server image by entering: `cat /perfigo/build`

Clean Access Server

- From the CAM web administration console, you can determine the version of the CAS by going to **Device Management > CCA Server**, clicking the **Manage** icon for the Server in the **List of Servers**, then clicking the **Misc** tab, which displays the **Update** page by default. The software version and date are listed in the **Current Version** field.
- From an SSH connection to the machine, you can determine the version of code running on a Clean Access server image by entering: `cat /perfigo/build`
- From the CAS's direct access web console (**https://<CAS_eth0_IP>/admin**), you can determine the version of the CAS by going to **Administration > Software Update**. The software version and date are listed in the **Current Version** field.

Clean Access Agent

- From the web admin console, you can determine the version of the Clean Access Agent from either:
  - **Monitoring > Summary**, or
  - **Device Management > Clean Access > Clean Access Agent > Distribution**, or
  - **Device Management > Clean Access > Clean Access Agent > Updates**
- From the Clean Access Agent itself, you can determine the version of the client by right-clicking the Clean Access Agent icon from the task bar and choosing **About**.

Note Stating with Cisco Clean Access release 3.6(0) and above, the Clean Access Agent has four-digit versioning (e.g. 3.6.0.0).

New and Changed Information

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

For additional details, see also:

- Clean Access Supported AV/AS Product List, page 43
- Clean Access Agent Version Summary, page 63
- Caveats, page 64
- Known Issues for Cisco Clean Access, page 82

Enhancements for Release 3.6.4.4

Release 3.6.4.4 is a general patch release for the Clean Access Manager (CAM) and Clean Access Server (CAS) that addresses a Cisco PSIRT issue involving caveat CSCsj33976. See Resolved Caveats - Release 3.6.4.4, page 67 for more information. No new features are added.

Installation/Upgrade Information

- CD Installation Instructions for 3.6.4.4, page 9
- Important Information for 3.6.4.4 Upgrade, page 9
- Upgrade Instructions for 3.6.4.4, page 10

CD Installation Instructions for 3.6.4.4

To install release 3.6.4.4, from a CD-ROM, refer to the instructions in New Installation of Release 3.6(x), page 84.

Important Information for 3.6.4.4 Upgrade

Note

- Release 3.6.4.4 is applied to the Clean Access Manager and Clean Access Server(s) and is a mandatory upgrade for 3.6(x) systems.
- In-place upgrade is not supported.
- The 3.6.4.4 release incorporates all fixes in the 3.6.4.1, 3.6.4.2, 3.6.4.3, and Patch-CSCsg24153 patches. It is not necessary to apply these patches first before upgrading to 3.6.4.4, and you can upgrade directly from any 3.6(x) release.
- When upgrading from 3.6(x) to 3.6.4.4, you can perform **web console** upgrade of standalone 3.6(x) CAM/CAS machines if the following conditions are met:
  - 3.6(x) CAM machines have already been patched for caveat CSCsg24153, page 69.
  - 3.6(x) CAS machines have already been patched for caveat CSCsg24153, page 69 **and** the CAS web console password is NOT cisco123.
- For all other cases, you must use the Upgrading via Console/SSH, page 101 procedure to upgrade your 3.6(x) system to 3.6.4.4.
- If upgrading high-availability (failover) CAM/CAS pairs, use the instructions in Upgrading High Availability Pairs, page 103.

Upgrade Instructions for 3.6.4.4

To upgrade your 3.6(x) CAM and CAS to 3.6.4.4, perform the following steps.

Step 1 Download the **cca_upgrade_3.6.x-to-3.6.4.4.tar.gz** upgrade file to your local computer from the http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.6.4 folder.

Step 2 For standalone 3.6(x) systems, refer to Upgrade Instructions for 3.6(x) Minor Releases and Patches, page 95 to upgrade your 3.6(x) CAM/CAS to 3.6.4.4. If planning to perform web upgrade, refer to Important Information for 3.6.4.4 Upgrade, page 9 first. Otherwise, you can use the Upgrading via Console/SSH, page 101 procedure for all 3.6(x) systems.

Step 3 For HA (failover) 3.6(x) system refer to Upgrading High Availability Pairs, page 103 to upgrade your HA-CAM and HA-CAS pairs to 3.6.4.4.

Enhancements for Release 3.6.4.3

Release 3.6.4.3 is a general and important bug fix release and patch for the Clean Access Manager (CAM) and Clean Access Server (CAS) that resolves the caveats described in Resolved Caveats - Release 3.6.4.3, page 68 and adds the following enhancements.

Enhancements

- Broadcast ARP Server Management Option Removed, page 11
- Clean Access Agent (3.6.5.0), page 11
- Supported AV/AS Product List Enhancements (Version 48), page 11

For further details, see also:

- Resolved Caveats - Release 3.6.4.3, page 68

Upgrade Information

- Important Information for 3.6.4.3 Upgrade, page 10
- Upgrade Instructions for 3.6.4.3, page 11
- Software Compatibility Matrixes, page 4

Important Information for 3.6.4.3 Upgrade

Note

- Release 3.6.4.3 is applied to the Clean Access Manager and Clean Access Server(s) and is a mandatory upgrade for 3.6(x) systems.
- Release 3.6.4.3 is an upgrade-only patch. CD install and in-place upgrade are not supported.
- Your CAM/CAS must already be running 3.6(x) to upgrade to release 3.6.4.3. If running 3.5(x) or below, you must perform in-place upgrade to 3.6(4) before you can upgrade to 3.6.4.3.
- The 3.6.4.3 release incorporates all fixes in the 3.6.4.1, 3.6.4.2, and Patch-CSCsg24153 patches. It is not necessary to apply these patches first before upgrading to 3.6.4.3, and you can upgrade directly from any 3.6(x) release.

- When upgrading from 3.6(x) to 3.6.4.3, you can perform **web console** upgrade of standalone 3.6(x) CAM/CAS machines if the following conditions are met:
  - 3.6(x) CAM machines have already been patched for caveat CSCsg24153, page 69.
  - 3.6(x) CAS machines have already been patched for caveat CSCsg24153, page 69 **and** the CAS web console password is NOT cisco123.
- For all other cases, you must use the Upgrading via Console/SSH, page 101 procedure to upgrade your 3.6(x) system to 3.6.4.3.
- If upgrading high-availability (failover) CAM/CAS pairs, use the instructions in Upgrading High Availability Pairs, page 103.

Upgrade Instructions for 3.6.4.3

To upgrade your 3.6(x) CAM and CAS to 3.6.4.3, perform the following steps.

Step 1 Download the **cca_upgrade_3.6.x-to-3.6.4.3.tar.gz** upgrade file to your local computer from the http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.6.4 folder.

Step 2 For standalone 3.6(x) systems, refer to Upgrade Instructions for 3.6(x) Minor Releases and Patches, page 95 to upgrade your 3.6(x) CAM/CAS to 3.6.4.3. If planning to perform web upgrade, refer to Important Information for 3.6.4.3 Upgrade, page 10 first. Otherwise, you can use the Upgrading via Console/SSH, page 101 procedure for all 3.6(x) systems.

Step 3 For HA (failover) 3.6(x) system refer to Upgrading High Availability Pairs, page 103 to upgrade your HA-CAM and HA-CAS pairs to 3.6.4.3

Broadcast ARP Server Management Option Removed

The Clean Access Manager web console no longer offers the "Continuously broadcast gratuitous ARP with VLAN ID" Clean Access Server management option.

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

- **Device Management > CCA Servers > Manage [CAS_IP] > Advanced > ARP**.

Clean Access Agent (3.6.5.0)

Version 3.6.5.0 of the Clean Access Agent adds support for IE 7.0, and new AV/AS product support.

For further details, see Clean Access Agent Version Summary, page 63 and Supported AV/AS Product List Version Summary, page 59.

Note The 3.6.5.0 Agent does **not** support Microsoft Windows Vista operating system. If Vista OS is used, it will be detected as Win ALL.

Supported AV/AS Product List Enhancements (Version 48)

- See Supported AV/AS Product List Version Summary, page 59 for details on each update to the list.

- See Clean Access Supported AV/AS Product List, page 43 for the latest AV/AS product charts as of the latest release.

Enhancements for Release 3.6.4.2

Release 3.6.4.2 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 3.6.4.2, page 70. No new features are added.

Note

- The 3.6.4.2 patch is applied to the Clean Access Manager only.
- The 3.6.4.2 patch is a mandatory patch for the 3.6.4.1 and all prior 3.6(x) CAMs. To apply the patch:
  - If you are running 3.6.4.1, you can apply the 3.6.4.2 patch directly to your CAM.
  - If you are running 3.6(4) on a system that was upgraded to 3.6(4) from 3.5(x), 3.6(0) or 3.6(1) using a CD, you can apply the 3.6.4.2 patch directly to your CAM.
  - If you are running 3.6(4) on a system that was upgraded to 3.6(4) from 3.6(2) or 3.6(3), then you must first apply the 3.6.4.1 patch to your CAM prior to applying the 3.6.4.2 patch.
    NOTE: This is an important step that must be performed manually–the 3.6.4.2 patch does not apply any updates/fixes contained in the 3.6.4.1 patch.
  - If you are running 3.6(0) or 3.6(1) or 3.6(2) or 3.6(3), you must apply the 3.6.4.1 patch to your CAM prior to applying the 3.6.4.2 patch.
    NOTE: This is an important step that must be performed manually–the 3.6.4.2 patch does not apply any updates/fixes contained in the 3.6.4.1 patch.
  - If you are running 3.5(x) and want to upgrade to 3.6(x), you can upgrade to 3.6(4) using the upgrade procedure and the 3.6(4) CD, following which you can apply the 3.6.4.2 patch.
- The 3.6.4.2 patch includes a script to update all the existing ARP entries on your CAM to ensure that only the right ARP entries are present.

See the following sections:

- Upgrade Instructions for 3.6.4.2
- Resolved Caveats - Release 3.6.4.2

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

Upgrade Instructions for 3.6.4.2

To upgrade your CAM to 3.6.4.2, perform the following steps.

Step 1 Download the **cam_upgrade-3.6.4.2.tar.gz** upgrade file to your local computer from the http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.6.4 folder.

Step 2 If running either 3.6.4.1 or 3.6(4) on a system that was upgraded to 3.6(4) from 3.5(x), 3.6(0) or 3.6(1) using a CD, upgrade the CAM to the 3.6.4.2 patch using one of the following procedures. Carefully follow instructions to upgrade the CAM:

- Upgrade CAM from CAM Web Console, page 99, or
- Upgrading via Console/SSH, page 101, or
- Upgrading High Availability Pairs, page 103 (for HA-CAMs only)

Step 3 If running 3.6(4) on a system that was upgraded to 3.6(4) from 3.6(2) or 3.6(3), or running 3.6(0) or 3.6(1) or 3.6(2) or 3.6(3) on your system, you must first apply the 3.6.4.1 patch to your CAM prior to applying the 3.6.4.2 patch. Refer to the instructions in Enhancements for Release 3.6.4.1, page 15 to apply the 3.6.4.1 patch, then follow the instructions in Step 2 above to apply the 3.6.4.2 patch.

Step 4 After the CAM has been upgraded to 3.6.4.2, access the console for each attached Clean Access Server (CAS) and perform **`service perfigo restart`**. (Or you can perform **`service perfigo reboot`** if preferred.) For a CAS HA-pair, it is sufficient to perform **`service perfigo restart`** on the currently active CAS.

Enhancements for Release 3.6.4.1

Release 3.6.4.1 is a general and important bug fix release and patch for the Clean Access Manager and Clean Access Server that resolves caveat CSCse97903, page 71. No new features are added.

Note

- Release 3.6.4.1 must be applied only when upgrading 3.6(x) CAM/CAS systems. **If upgrading your 3.6(x) system, you must upgrade to 3.6.4.1**.
- If migrating from 3.5(x) or performing a new 3.6(x) installation, you can use the 3.6(4) ISO CD and there is no need to install the 3.6.4.1 patch.
- The patch must be applied to the CAS and CAM simultaneously during the same maintenance window.

Information for the 3.6.4.1 patch is in the following sections:

- Upgrade Instructions for 3.6.4.1
- Resolved Caveats - Release 3.6.4.1

Upgrade Instructions for 3.6.4.1

To upgrade your 3.6(x) system to the latest release, please execute the following update procedure steps on your CAM and CAS.

Step 1 Download the **cca_upgrade_3.6.x-to-3.6.4.1.tar.gz** upgrade file to your local computer from the http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.6.4 folder.

Step 2 If running 3.6(x), upgrade each CAS using one of the following procedures. Carefully follow instructions to upgrade each CAS:

- Upgrade CAS from CAS Management Pages, page 97, or
- Upgrade CAS from CAS Direct Access Web Console, page 98, or
- Upgrading via Console/SSH, page 101, or
- Upgrading High Availability Pairs, page 103 (for HA-CASes only)

Step 3 If running 3.6(x), upgrade the CAM using one of the following procedures. Carefully follow instructions to upgrade the CAM:

- Upgrade CAM from CAM Web Console, page 99, or
- Upgrading via Console/SSH, page 101, or
- Upgrading High Availability Pairs, page 103 (for HA-CAMs only)

Enhancements for Release 3.6(4)

This section details enhancements delivered with release 3.6(4) of the Clean Access Manager and Clean Access Server.

See also:

OOB Support for 3750 NME Modules for Cisco 2800/3800 ISRs

With release 3.6(4)+, Cisco NAC Appliance OOB adds support for the following Cisco 3750 EtherSwitch service module (NME) cards for Cisco 2800/3800 Series Integrated Services Routers:

- NME-16ES-1G
- NME-16ES-1G-P
- NME-X-23ES-1G
- NME-X-23ES-1G-P
- NME-XD-24ES-1S-P
- NME-XD-48ES-2S-P

These NMEs are essentially a Cisco Catalyst 3750 switch packaged as a blade for the 2800/3800 ISR router, and are supported on these ISRs only (e.g. 2600 is not supported).

Note Adding 3750 NME modules to the CAM for OOB switch management requires the same steps as if adding a 3750 switch. When configuring the switch profile for these NMEs, choose **Cisco Catalyst 3750 series** under **Switch Management > Profiles > Switch > New | Switch Model**.

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

Support for "Ignore" Global Device Filter for IP Phones in OOB Deployments

Release 3.6(4)+ provides a new "**ignore**" global device filter control which when set for the specified MAC address will ignore SNMP traps from managed switches in Out-of-Band deployments. This feature is intended to support OOB client machines connected to the network via IP phones.

Note After 3.6(4)+ upgrade, administrators should reconfigure any "allow" device filters specified for IP phones with previous CCA releases to the new "ignore" option.

Note The "**ignore**" option applies to OOB deployments and global device filters only. It does not apply to CAS-specific filters, and for IB deployments this option has no effect.

This new feature enhances the following web admin console page:

- **Device Management > Filters > New/Edit** (new "**ignore**" option)

Clean Access Agent (3.6.4.0)

Version 3.6.4.0 of the Clean Access Agent provides the following enhancements:

- Support for new TrendMicro, Sophos and Grisoft AV/AS products.
- Version 3.6.4.0 adds support for IE 7 Beta 3.

Note Support for any future IE 7 releases will only be added after testing and certification has been performed on those releases.

For further details, see Clean Access Agent Version Summary, page 63 and Supported AV/AS Product List Version Summary, page 59.

Supported AV/AS Product List Enhancements (Version 44)

- See Supported AV/AS Product List Version Summary, page 59 for details on each update to the list.
- See Clean Access Supported AV/AS Product List, page 43 for the latest AV/AS product charts as of the latest release.

Enhancements for Release 3.6(3)

This section details enhancements delivered with release 3.6(3) of the Cisco Clean Access Manager and Cisco Clean Access Server.

See also Resolved Caveats - Release 3.6(3), page 73

For upgrade instructions, see Upgrading to 3.6(x), page 85.

OOB Page Redirection Timers (SNMP Receiver Advanced Settings)

When configuring OOB for web login users, release 3.6(3) provides new "**Redirection Delay with/without Bouncing**" options for additional control of webpage redirection intervals (to allow time for port bouncing or to minimize redirection time if no port bouncing is required). This allows the port to be bounced after a configured interval, and the page to be redirected after another configured interval. The total of these configured intervals then becomes the redirection interval experienced by the user after login, by default 20 seconds when the port is bounced. The client will then be on the Access VLAN.

- When the port is not bounced, the total redirection interval that the user experiences is the value of the **Redirection Delay without Bouncing** field.

- When the port is bounced, the total redirection interval that the user experiences is the sum of 2 fields: **Redirection Delay with Bouncing** and **Port Bounce Interval**.

This enhancement modifies the following web admin console page:

- **Switch Management > Profiles > SNMP Receiver > Advanced Settings** (new **"**Redirection Delay without Bouncing" and "Redirection Delay with Bouncing" fields)

Authentication Cache Timeout

For performance reasons, the Clean Access Manager caches the authentication results from user authentication for 2 minutes by default. Release 3.6(3) provides a new "Authentication Cache Timeout" control on the Auth Server list page that allows administrators to configure the number of seconds the authentication result will be cached in the CAM. When a user account is removed from the authentication server (LDAP, RADIUS, etc), administrators can restrict the time window a user can login again into CCA by configuring the Authentication Cache Timeout.

This enhancement modifies the following web admin console page:

- **User Management > Auth Servers > Auth Servers > List** (new **"**Authentication Cache Timeout" field)

API Enhancements

The Clean Access API for your Clean Access Manager is accessed from a web browser as follows: **https://<cam-ip-or-name>/admin/cisco_api.jsp**. With release 3.6(3), the Cisco Clean Access API utility script, cisco_api.jsp, provides the following enhancements:

New APIs:

- **kickuserbymac** — Removes in-band logged in user(s) by MAC address. For multiple users, you can specify a comma-separated list of MAC addresses.
- **changeloggedinuserrole** - Change in-band user access permissions by modifying a user's logged in role to the specified role. For multiple users, you can specify a comma-separated list of IP addresses.

Enhanced APIs:

- **changeuserrole**— With 3.6.3+, change in-band user access permissions by removing the user from the Online Users list and adding the user's MAC address to the Device Filters with new specified role. (Note: For 3.6(2) and prior, this function only changes the logged in user's role.)
- **kickoobuser**—Removes logged-in out-of-band user(s). With 3.6(3)+ you can specify a comma-separated list of IP addresses to remove multiple users.
- **kickuser**— Removes logged-in in-band user(s). With 3.6(3)+ you can specify a comma-separated list of IP addresses to remove multiple users.
- **removemac**— Removes MAC address(es) from Device Filters list. With 3.6(3)+ specify a comma-separated list of MAC addresses to remove multiple addresses.

New "service perfigo maintenance" CLI Command for CAS

Release 3.6(3) provides a new **`service perfigo maintenance`** CLI command that can be issued on the CAS machine to maintain network connectivity when bringing the CAS into maintenance mode. In maintenance mode, only the basic CAS router runs and continues to handle VLAN-tagged packets. The new command allows communication through the management VLAN to the CAS, and is intended for

environments where the CAS is in trunk mode and the native VLAN is different than the management VLAN. This command provides a better alternative to the **service perfigo stop** command, which when issued and the management VLAN is set, causes the CAS to lose network connectivity.

Note `service perfigo maintenance` is available on the CAS CLI only (does not apply to CAM).

Clean Access Agent Enhancements (3.6.3.1)

Version 3.6.3.1 of the Clean Access Agent resolves the following AV/AS related caveats:CSCse72371, page 73, CSCse72384, page 73, CSCse72396, page 73.

For details, see Clean Access Agent Version Summary, page 63 and Resolved Caveats - Release 3.6(3), page 73.

Clean Access Agent Enhancements (3.6.3.0)

Version 3.6.3.0 of the Clean Access Agent resolves caveat CSCsd94974, page 73 and provides additional AV product support (Windows XP/2000). See Supported AV/AS Product List Version Summary, page 59 for details.

For additional details, see also Clean Access Agent Version Summary, page 63.

Supported AV/AS Product List Enhancements (Version 42)

- See Supported AV/AS Product List Version Summary, page 59 for details on each update to the list.
- See Clean Access Supported AV/AS Product List, page 43 for the latest AV/AS product charts as of the latest release.

Enhancements for Release 3.6.2.2

Patch release 3.6.2.2 is a general and important bug fix release and patch for high-availability (HA) Clean Access Manager (CAM) systems that resolves caveat CSCsd79205, page 73. No new features are added. See SSH Upgrade Instructions for 3.6.2.2 (HA-CAMs), page 20 for how to apply this patch.

Note

- The 3.6.2.2 patch is a required upgrade for all HA-CAM systems running 3.6.2.1 or 3.6(2). Customers currently running 3.6(2) on HA-CAMs must upgrade to 3.6.2.1 then 3.6.2.2 to apply this patch.
- The 3.6.2.2 patch is not required for customers running 3.6(2)/3.6.2.1 on standalone (non-HA) CAMs. However, it is recommended to apply the patch to keep your system current should you have a future need to configure your CAMs for HA.
- This patch is a CAM-only patch. The 3.6.2.2 patch can only be applied to CAM systems running 3.6.2.1. It cannot be applied to 3.6.2.1 CAS systems. After applying this patch the CAM version will be 3.6.2.2, and the CAS version remains 3.6.2.1.
- You must execute the procedure described in SSH Upgrade Instructions for 3.6.2.2 (HA-CAMs), page 20 to upgrade HA-CAM pairs. Do NOT perform 3.6.2.2 web upgrade on HA-CAMs.
- After applying the 3.6.2.2 patch, no reboot occurs nor is required.

SSH Upgrade Instructions for 3.6.2.2 (HA-CAMs)

The following instructions are required to upgrade your HA-CAM pairs from release 3.6.2.1 to 3.6.2.2. Please carefully review the procedure described below prior to upgrading your CAMs.

Caution Do NOT use web upgrade to perform 3.6.2.2 upgrade on HA-CAMs.

Step 1 Log into Cisco Secure Software and download the **cam-3.6.2.1-to-3.6.2.2-upgrade.tar.gz** patch file to your local computer from the 3.6.2 folder under:
http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.6.2

Step 2 Copy the **cam-3.6.2.1-to-3.6.2.2-upgrade.tar.gz** upgrade file to the /store directory of each CAM in the HA pair using WinSCP, SSH File Transfer or PSCP as described below.

If using WinSCP or SSH File Transfer:

a. Copy **cam-3.6.2.1-to-3.6.2.2-upgrade.tar.gz** to the /store directory of each CAM.

Or, if using PSCP:

a. Open a command prompt on your Windows computer.

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

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

```
> pscp cam-3.6.2.1-to-3.6.2.2-upgrade.tar.gz root@ipaddress_manager:/store
```

Step 3 Determine the “inactive” CAM of the HA-CAM pair, as follows:

a. Access the Primary CAM by opening the web console for the Primary’s IP address.

b. Access the Secondary CAM by opening the web console for the Secondary’s IP address.

The web console for the inactive CAM will only display the **CCA Manager** module menu. Future references in these instructions that specify “active” or “inactive” refer to the results of this test as performed at this time.

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

Step 4 On the inactive CAM, untar the upgrade file:

```
cd /store
tar xvzf cam-3.6.2.1-to-3.6.2.2-upgrade.tar.gz
```

Step 5 Cd to the untarred upgrade directory:

```
cd cam_upgrade_3.6.2.2/
```

Step 6 Run the upgrade:

```
./UPGRADE.sh
```

Step 7 Run the following command on the **inactive CAM** only:

```
service perfigo restart
```

Step 8 On the active CAM, untar the upgrade file:

```
cd /store
tar xvzf cam-3.6.2.1-to-3.6.2.2-upgrade.tar.gz
```

Step 9 Cd to the untarred upgrade directory:

```
cd cam_upgrade_3.6.2.2/
```

Step 10 Run the upgrade:

```
./UPGRADE.sh
```

Step 11 This completes the upgrade. No “service perfigo restart” is needed on the active CAM.

Upgrade Instructions for 3.6.2.2 (Standalone CAM Only)

The 3.6.2.2 patch is not required for customers running 3.6(2)/3.6.2.1 on standalone (non-HA) CAMs. However, it is recommended to apply the patch to keep your system current should you have a future need to configure your CAMs for HA. You may use either SSH or web upgrade procedures to apply the 3.6.2.2 patch to a standalone CAM system only. Carefully review the instructions described in Upgrade Instructions for 3.6(x) Minor Releases and Patches prior to upgrading your CAM.

Note After 3.6.2.2 patch upgrade, no automatic reboot occurs on the CAM and no reboot is required.

Step 1 Log into Cisco Secure Software and download the **cam-3.6.2.1-to-3.6.2.2-upgrade.tar.gz** patch file to your local computer from the 3.6.2 folder under:
http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.6.2

Step 2 Perform web upgrade on your standalone CAM as described in Upgrade CAM from CAM Web Console, page 99.

Step 3 Alternatively, if you prefer SSH patch upgrade on your standalone CAM:

- Review the instructions in Upgrading via Console/SSH, page 101
- Follow the CAM procedure in Download the Upgrade File and Copy to CAM/CAS, page 101.
- Follow the procedure to Perform SSH Upgrade on the CAM, page 102.

Enhancements for Release 3.6.2.1

Release 3.6.2.1 is a general and important bug fix release and patch for the Clean Access Manager and Clean Access Server that resolves caveat CSCsd74376, page 74. No new features are added. See Upgrade Instructions for 3.6.2.1 for how to apply this patch.

Note If you are using Broadcom 5702/5703/5704 NIC cards in your CAM/CAS servers, refer to the instructions described in Known Issues with Broadcom NIC 5702/5703/5704 Chipsets, page 82 prior to upgrading to release 3.6.2.1. Server models with Broadcom 5702/5703/5704 NIC cards may include: Dell PowerEdge 850, CCA-3140-H1, HP ProLiant DL140 G2/ DL360/DL380.

Note

- The 3.6.2.1 patch is a required patch for all 3.6(2) systems. All customers running 3.6(2) should apply this patch.
- The 3.6.2.1 patch can only be applied to 3.6(2) systems.
- Customers running 3.6.0 and 3.6.1 with Clean Access Servers affected by caveat CSCsd74376 must first upgrade to 3.6(2), then perform 3.6.2.1 patch upgrade.
- The patch must be applied to the CAS and CAM simultaneously during the same maintenance window.
- Web upgrade is recommended to upgrade from release 3.6(2) to 3.6.2.1.

Upgrade Instructions for 3.6.2.1

Web upgrade is recommended to upgrade from release 3.6(2) to 3.6.2.1. Prior to upgrading your CAS(es) and CAM, carefully review the instructions described in Upgrade Instructions for 3.6(x) Minor Releases and Patches.

Note For 3.6.2.1 patch upgrade via web console, the machine (CAS or CAM) automatically reboots after upgrade. The patch upgrade should complete in 2-5 minutes.

Step 1 Log into Cisco Secure Software and download the **cca-3.6.2-to-3.6.2.1-upgrade.tar.gz** patch file to your local computer from the 3.6.2 folder under:
http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.6.2

Step 2 Upgrade each CAS using one of the following procedures. Carefully follow instructions:

- Upgrade CAS from CAS Management Pages, or
- Upgrade CAS from CAS Direct Access Web Console

Step 3 Upgrade your CAM using the following procedure:

- Upgrade CAM from CAM Web Console, page 99

Step 4 Alternatively:

a. If upgrading CAS HA pairs, refer to Upgrading High Availability Pairs, page 103

b. If SSH upgrade on the CAS is preferred, refer to Upgrading via Console/SSH, page 101

Enhancements for Release 3.6(2)

This section details enhancements delivered with release 3.6(2) of the Cisco Clean Access Manager and Cisco Clean Access Server.

Note Please also refer to Known Issues with Broadcom NIC 5702/5703/5704 Chipsets, page 82.

CE500 Support Enhancement

When the Cisco Catalyst Express 500 Series (CE500) is added to the Clean Access Manager as a managed switch, it will use linkup/linkdown SNMP trap notification by default. With release 3.6(2) and above, the CE500 can be configured to use mac-notification traps using the Advanced configuration page for the switch (under **Switch Management > Devices > List > Config [Switch IP] > Config > Advanced**).

Note If running an IOS version lower than 12.2(25) SEG, the switch ports of the CE500 must be assigned to the OTHER role (not Desktop or IP phone) on the switch's Smartports configuration, otherwise, mac-notification will not be sent out. See also Supported Switches for Cisco NAC Appliance, page 3.

Heartbeat Timer Enhancements for L3 Deployments

With release 3.6(2) and above, the Heartbeat Timer behaves as inactivity/idle timer for L3 deployments in addition to L2 deployments. For L2 deployments, there is no change in Heartbeat Timer function.

For L3 deployments, the Heartbeat Timer now behaves as described in the following cases:

- **L3 deployments where routers do not perform proxy ARP:**

If the Clean Access Servers sees no packets from the user for the duration of time that the heartbeat timer is set to, then the user will be logged out. Even if the user's machine is connected to the network but does not send a single packet on the network that reaches the CAS, it will be logged out. Note that this is highly unlikely because modern systems send out many packets even when the user is not active (e.g. chat programs, Windows update, AV software, ads on web pages, etc.)

- **L3 deployments where the router/VPN concentrator performs proxy ARP for IP addresses on the network:**

  In this scenario, if a device is connected to the network the router will perform proxy ARP for the device's IP address. Otherwise, if a device is not connected to the network, the router does not perform proxy ARP. Typically only VPN concentrators behave in this way. In this case, if the Clean Access Server sees no packets, the CAM/CAS attempts to perform ARP for the user. If the router responds to the CAS because of proxy ARP, the CAM/CAS will not logout the user. Otherwise, if the router does not respond to the CAS, because the device is no longer on the network, the CAM/CAS will log out the user.

- **L3 deployments where the router/VPN concentrator performs proxy ARP for the entire subnet:**

  In this scenario, the router/VPN concentrator performs proxy ARP irrespective of whether individual devices are connected. In this case, the Heartbeat Timer behavior is unchanged, and the CAM/CAS never log out the user.

CAM SSH Upgrade Enhancements

When upgrading the CAM from release 3.6(x) to release 3.6(2) and above, the SSH upgrade script provides an additional prompt to choose whether or not to upgrade the Clean Access Agent files inside the Clean Access Manager. Choosing **`Yes`** upgrades the Agent Setup Installation and Patch Installation files to the latest Agent version bundled with the release (for example, Agent 3.6.2.0 for release 3.6(2)). Choosing **`No`** leaves the original Agent Setup and Patch Installation files that were on your CAM prior to upgrade.

See Perform SSH Upgrade on the CAM, page 102 for details.

Note Once release 3.6(2) is installed on the CAM/CAS, an "Upgrade Agent" checkbox option will be displayed on the CAM web console when performing web upgrade to a future release.

Support Log and Log Level Enhancements

With release 3.6(2) and above, log level controls are added to the Support Logs pages of the CAM web console and CAS direct access web console to facilitate setting the level of various loggers on the CAM/CAS for troubleshooting purposes. This enhancement affects the following web console pages:

- **Administration > CCA Manager > Support Logs**
- **CAS direct access console: Monitoring > Support Logs**

Note To optimize CAS memory usage, the following page is removed:
Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Misc > Support Logs
With release 3.6(2) and above, CAS-specific support logs are obtained from the CAS direct console only.

For troubleshooting, see also Downloading CAM/CAS Support Logs, page 108.

SSL Certificate Enhancements

For release 3.6(2) and above, the "Delete Certificate Temporarily Created for Export" buttons are removed, and exported certificate filename extensions are changed as follows:

- CSR: *.pem
- private key: *.pem
- certificate: *.cer (was *.pem)
- root/intermediate CA: *.cer (was *.pem)

These enhancements affect the following web console pages:

- CAM web console: **Administration > CCA Manager > SSL Certificate | Export CSR/Private Key/Certificate**
- CAS management pages: **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs | Export CSR/Private Key/Certificate**
- CAS direct access web console: **https://<CAS_IP>/admin/Administration > SSL Certificate | Export CSR/Private Key/Certificate**

Auth Test UI Enhancements

The **Auth Test** page is improved in release 3.6(2)+ to display additional error messages to assist in debugging authentication sources, particularly LDAP/RADIUS servers.

This affects the following CAM web console page:

- **User Management > Auth Servers > Auth Test**

RADIUS "Malformed Packets" Option Enhancement

The RADIUS "malformed packets" option is improved to authenticate the user properly even if the RADIUS packet is malformed due to empty attributes only.

The name of the option is changed from "Allow Badly Formed RADIUS Packets" to "Accept RADIUS packets with empty attributes from some old RADIUS servers." This affects the following CAM web console pages:

- **User Management > Auth Servers > New Server |** Authentication Type: **Radius**
- **User Management > Auth Servers > Edit Server** (Radius)

VPN SSO Troubleshooting Enhancement

An additional "Active VPN Clients" page is added to the CAS management pages and CAS direct access console to list IP addresses known to the CAS through VPN Single Sign-On (SSO). This affects the following web console pages:

- CAM web console: **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Authentication > VPN Auth > Active Clients**
- CAS direct access console (https://<CAS_IP>/admin/): **Monitoring > Active VPN Clients**

Support for Solaris OS for Web Login Users

Support for the Solaris operating system is added to web console pages where OS is used as one of the selection attributes (e.g. web login, scan setup, general setup pages). This affects the following web console pages:

CAM web console:

- **Administration > User Pages > Login Page > Add/Edit | Operating System**
- **Device Management > Clean Access > General Setup | Operating System**
- **Device Management > Clean Access > Network Scanning** (OS dropdown menus for all subpages)

CAS web console:

- **Device Management > CCA Servers > Manage[CAS_IP] > Authentication > Login Page > Add / Edit | Operating System**

Unauthenticated Role Enhancement

The unauthenticated role is denoted as "Unauthenticated Role (not common)" in the User Role selection dropdown menus for network scanning-related pages of the Clean Access module. This enhancement is intended to remind administrators not to configure the unauthenticated role for these pages, unless there is a special need to assign a user to this role **after** authentication.

This enhancement affects the following web console pages:

- **Device Management > Clean Access > General Setup**
- **Device Management > Clean Access > Network Scanning > Scan Setup >** (all subpages: Plugins | Options | Vulnerabilities | User Agreement | Test)

CAM File Upload Enhancements

With release 3.6(2) and above, the location of files uploaded to the Clean Access Manager using **Administration > User Pages > File Upload** is changed from /perfigo/control/tomcat/normal-webapps/admin to /perfigo/control/tomcat/normal-webapps/**upload** in the CAM. This enhancement requires that new files uploaded to the CAM are specified using URL format https://<CAM_IP>/**upload**/file_name.htm when configuring user pages that reference these files.

Note

- Files uploaded to the CAM prior to 3.6(2)+ continue to be located under /perfigo/control/tomcat/normal-webapps/admin and are still referenced by https://<CAM_IP>/**admin**/file_name.htm.
- The location of files uploaded to the CAS is unchanged.

This enhancement affects the following web console pages:

- **Administration > User Pages > File Upload**
- **Administration > User Pages > Login Page (frame-based) > Add/Edit > Right Frame**
- **Device Management > Clean Access > Network Scanner > Scan Setup > User Agreement Page | Information Page Message (or URL)**
- **Device Management > Clean Access > General Setup | Show Network Policy to Clean Access Agent users [Network Policy Link:]**

Client Web Login Page Enhancement

With release 3.6(2)+, the client web login page sets the **Username** field as the initial insertion point, and accepts the **Enter** key when users submit login credentials. The user can immediately type their username and password then press the **Enter** key to get the login result. In prior releases, the user needed to move the pointer to the **Username** field, type credentials, then click the **Continue** button to submit credentials, and the Enter key was not accepted.

Clean Access Agent Enhancements (3.6.2.0)

Version 3.6.2.0 of the Clean Access Agent provides the following enhancements:

- Additional AV product support (Windows XP/2000). See Supported AV/AS Product List Version Summary, page 59 for details.

For additional details, see also Clean Access Agent Version Summary, page 63.

Supported AV/AS Product List Enhancements (Version 36)

- See Supported AV/AS Product List Version Summary, page 59 for details on each update to the list.
- See Clean Access Supported AV/AS Product List, page 43 for the latest AV/AS product charts as of the latest release.

Enhancements for Release 3.6.1.1

Release 3.6.1.1 is a general and important bug fix release and patch for the Clean Access Manager and Clean Access Server. No new features are added. See Resolved Caveats - Release 3.6.1.1, page 75 for details on this caveats resolved by this patch. See Upgrade Instructions for 3.6.1.1, page 28 for how to apply this patch.

Note

- The 3.6.1.1 patch is a recommended patch for all 3.6.x-to3.6.1 upgraded systems. All customers who have upgraded from 3.6.x to 3.6(1) should apply this patch. New 3.6(1) installations, and systems that have been migrated from 3.5(9) to 3.6(1) are not affected and do not need to upgrade to this patch release.
- This patch will run only on 3.6(1) systems.
- The patch must be applied to the CAS and CAM simultaneously during the same maintenance window. This is to ensure users cannot download the Clean Access Agent in the interim before it is properly synchronized between the CAM and the CAS.
- Web upgrade is recommended to upgrade from release 3.6(1) to 3.6.1.1.

Upgrade Instructions for 3.6.1.1

Web upgrade is recommended to upgrade from release 3.6(1) to 3.6.1.1. Carefully review and execute the instructions described in Upgrade Instructions for 3.6(x) Minor Releases and Patches to upgrade your CAS(es) and CAM.

Note For 3.6.1.1 patch upgrade via web console, the machine (CAS or CAM) will NOT automatically reboot. The patch upgrade should complete in 2-5 minutes.

Step 1 Log into Cisco Secure Software and download the **cca-3.6.1-to-3.6.1.1-upgrade.tar.gz** patch file to your local computer from the 3.6.1 folder under:
http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.6.1

Step 2 Upgrade each CAS using one of the following procedures. Carefully follow instructions:

- Upgrade CAS from CAS Management Pages, or
- Upgrade CAS from CAS Direct Access Web Console

Note You must upgrade your CAS and CAM machines during the same maintenance window.

Step 3 Upgrade your CAM using the following procedure:

- Upgrade CAM from CAM Web Console, page 99

Step 4 Alternatively:

a. If upgrading CAS HA pairs, refer to Upgrading High Availability Pairs, page 103

b. If SSH upgrade on the CAS is preferred, refer to Upgrading via Console/SSH, page 101

Important Notes for Release 3.6(1)

Note Patch release 3.6.1.1 supersedes the workaround described below. See Enhancements for Release 3.6.1.1, page 28 for details.

If web-based login connection issues are experienced after upgrading to release 3.6(1), there is a simple workaround to resolve the issue. Please perform the following steps:

1. SSH to the Clean Access Server and login as user **`root`**.
2. At the root prompt, type the following command:

   ```
   chmod 770 /perfigo/access/apache/logs/fastcgi
   ```

3. This completes the workaround. You do not need to reboot or restart the CAS.

New Features and Enhancements for Release 3.6(1)

This section details new features delivered with release 3.6(1) of the Cisco Clean Access Manager and Cisco Clean Access Server, as well as enhancements from release 3.6.0.1.

New Features:

- MAC Address Wildcard Support for Device Filters
- NAT Session Throttle

Enhancements:

- New Hardware Driver Support (tg3)
- Supported Server Configurations Added
- CAS HA (Failover) UI Enhancements
- CAS IP Page UI Enhancement
- OOB Switch Support Added for Cisco Catalyst Express 500
- OOB Handling of Trunk Native VLAN
- Separation of In-Band VLAN and OOB VLAN in User Role
- OOB Port Profile Page Enhancement
- Traffic Policy Port Range Enhancements
- Auth Server and CAS Status Page Modifications
- SSL Page Enhancements
- Clean Access Agent New Requirement Page Enhancement
- Clean Access Agent Enhancements (3.6.1.0)
- Supported AV/AS Product List Enhancements (Version 28)

MAC Address Wildcard Support for Device Filters

Release 3.6(1) provides the ability to specify wildcards and ranges in device filter entries to allow administrators to specify a single entry for a whole range of devices, for example: "`00:01:4A:* Sony-Playstations`". This new feature affects the following web console pages:

- **Device Management > Filters > Devices > New / Edit / List**
- **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Filter > Devices**

NAT Session Throttle

Release 3.6(1) provides the ability to set up throttles/threshold on a per-host basis when the CAS is running as a NAT Gateway. This allows the CAS to restrict the total number of connections per host, thereby eliminating the chance of one host consuming all the connections. This affects the following web console page:

- **Device Management > CCA Servers > Manage[CAS_IP] > Advanced > NAT** (new page)

New Hardware Driver Support (tg3)

Release 3.6(1) provides a new tg3 driver that resolves the release 3.6(0) Broadcom NIC workaround (IPMI feature had to be disabled) specified in caveat CSCsd08348, page 79. With this new driver, VLAN tags are retained and the need to disable the IPMI feature using the Broadcom utility is eliminated.

Note If upgrading to release 3.6(1), you do NOT need to use the Broadcom utility, but performance will not be affected if IPMI settings have already been changed.

Supported Server Configurations Added

The *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)* is updated for release 3.6(1) with support added for:

- Dell PowerEdge 850
- PowerEdge 1850
- IBM eServer xSeries 336

See Hardware Supported, page 3 for details.

CAS HA (Failover) UI Enhancements

For an HA-Primary Mode or HA-Standby Mode Clean Access Server, the Disable Serial Login feature is now presented as a checkbox option to display the current status of serial login on the CAS direct access console. This affects the following page:

- CAS direct access console: **Administration > Network Settings > Failover**

CAS IP Page UI Enhancement

The L3 support checkbox is changed from "Enable L3 support for Clean Access Agent" to "Enable L3 support" on the CAS IP page to more accurately reflect the setting. For multi-hop L3 in-band deployments, this setting enables/disables L3 discovery of the CAS for both web login users and Clean Access Agent users at the CAS level. This affects the following web console page:

- **Device Management > CCA Servers > List of Servers > Manage [CAS_IP] > Network > IP**

OOB Switch Support Added for Cisco Catalyst Express 500

Release 3.6(1) adds out-of-band switch management support for the Cisco Catalyst Express 500 Series switch (CE500)

Note Cisco Catalyst Express 500 supports link-up/link-down SNMP traps only.

See also Supported Switches for Cisco NAC Appliance, page 3.

OOB Handling of Trunk Native VLAN

Release 3.6(1), when deployed for Out-of-Band provides support for Cisco IP Phone deployments where the port is a trunk port and the native VLAN is the data VLAN.

Note Because Cisco Clean Access can control switch trunk ports for OOB in release 3.6(1), please ensure the uplink ports for controlled switches are configured as "uncontrolled" ports after upgrade. This can be done in one of two ways:

- Before upgrading, change the **Default Port Profile** for the entire switch to "uncontrolled" under **Switch Management > Devices > Switches > List > Config[Switch_IP] > Default Port Profile | uncontrolled**, or
- After upgrading, change the **Profile** to "uncontrolled" for the applicable uplink ports of the switch under **Switch Management > Devices > Switches > List > Ports [Switch_IP] | Profile**

This will prevent unnecessary issues when the Default Port Profile for the switch has been configured as a managed/controlled port profile.

This affects the following web console page:

- **Switch Management > Devices > Switches > List > Ports [Switch IP]**

Separation of In-Band VLAN and OOB VLAN in User Role

Release 3.6(1) provides the ability to separate in-band and out-of-band VLANs when specifying VLAN assignment via the user role. This allows administrators to use the same system user role in cases where different Clean Access Servers – one inband and the other OOB – are being used and different VLANs need to be applied for in-band versus out-of-band users in the role. This affects the following web console pages:

- **User Management > User Roles > New Role**
- **User Management > User Roles > List of Roles | Edit Role**

OOB Port Profile Page Enhancement

The **Port Profile** page layout is enhanced to be more user-friendly and now includes the ability to switch a machine to either a User Role-based VLAN or Initial Port VLAN if the device is certified and not on the Out-of-Band Online User List. This affects the following web console pages:

- **Switch Management > Profiles > Port > New**
- **Switch Management > Profiles > Port > List | Edit Profile**

Traffic Policy Port Range Enhancements

Release 3.6(1) provides the ability to specify individual ports, a port range, a combination of ports and port ranges, or wildcards when configuring IP-based traffic policies. For example, the interface now allows specifying port values such as: "*" or "21, 1024-1100" to cover multiple ports in one policy. Previously, one port needed to be specified per policy. This reduces the number of policies that need to be configured to achieve the same effect. This enhancement affects the following web console pages:

- **User Management > User Roles > Traffic Control > IP > Add Policy**
- **User Management > User Roles > Traffic Control > IP > Edit Policy**

Auth Server and CAS Status Page Modifications

The "802.1x Filter" entry is removed from the **Status** tab of the CAS management pages and "Transparent 802.1x" is removed from the **Authentication Type** dropdown menu of the New Auth Server configuration page. This affects the following web console pages:

- **Device Management > CCA Servers > Manage [CAS_IP] > Status**
- **User Management > Auth Servers > New Server | Authentication Type**

SSL Page Enhancements

Release 3.6(1) provides additional page layout enhancements to the SSL management forms for the CAM and CAS.

- The order for the "**Choose an action**" dropdown is now:
  - Generate Certificate
  - Export CSR/Private Key/Certificate
  - Import Certificate
- Under **Import Certificate**, the **File Type** dropdown changes from "CA-signed Certificate" to "CA-signed PEM-encoded X.509 Cert" to help users request the proper certificate type from their CA provider.
- Under **Export CSR/Private Key/Certificate**, exported file extensions are changed from "xxx.csr" to "xxx.pem".

These enhancements affect the following web console pages:

- CAM web console: **Administration > CCA Manager > SSL Certificate**
- CAS management pages: **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs**
- CAS direct access web console: **https://<CAS_IP>/admin/Administration > SSL Certificate**

Clean Access Agent New Requirement Page Enhancement

Notes for AV and AS vendors are moved up to the **Vendor Name** dropdown menu, and the table title is changed from "Products" to "Product versions supported for Update via Clean Access Agent" for the New Requirements page. This affects the following web console page:

- **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement** (for **AV Definition Update** or **A S Definition Update** Requirement Types)
- **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement List | Edit** (for **AV Definition Update** or **A S Definition Update** Requirement Types)

Clean Access Agent Enhancements (3.6.1.0)

Version 3.6.1.0 of the Clean Access Agent provides the following enhancements:

- Additional AV product support (Windows XP/2000). See Supported AV/AS Product List Version Summary, page 59 for details.
- The Clean Access Agent can now be run by a restricted user on the local machine (user is not an administrator or power user). Administrator privileges are still necessary to perform the initial Agent installation.
- The event.log file used for Agent debug logging is now stored in the user's home directory (e.g. C:\Documents and Settings\<username>\Application Data\CiscoCAA\event.log) instead of the Agent installation directory, and the path of the registry key changes to HKEY_CURRENT_USER. See Enable Debug Logging on the Clean Access Agent, page 110 for details.

Note It is not recommended to upgrade the Agent from version 3.5.11 to 3.6.0.0 or 3.6.0.1. There may be issues with the uninstall/install procedure with selective files not being upgraded correctly or subsequent uninstalls failing. If you are using 3.5.11, it is recommended that you upgrade directly to the 3.6.1.0 Agent (bundled with Cisco Clean Access release 3.6(1)). For details, see caveat CSCsd28300, page 80

For additional details, see also:

- Clean Access Agent Version Summary, page 63
- Resolved Caveats - Release 3.6(1), page 76.

Supported AV/AS Product List Enhancements (Version 28)

- See Supported AV/AS Product List Version Summary, page 59 for details on each update to the list.
- See Clean Access Supported AV/AS Product List, page 43 for the latest AV/AS product charts as of the latest release.

Enhancements for Release 3.6.0.1

Release 3.6.0.1 is a general and important bug fix release and patch for the Clean Access Manager and Clean Access Server. No new features are added.

Note

- The 3.6.0.1 patch is a recommended patch for all 3.6(0) systems. All customers on 3.6(0) should apply this patch.
- This patch will run only on 3.6(0) systems.
- The patch must be applied to both the CAS and the CAM.
- Web upgrade is recommended to upgrade from release 3.6(0) to 3.6.0.1.

Information for the 3.6.0.1 patch is in the following sections:

- Upgrade Instructions for 3.6.0.1, page 34
- Resolved Caveats - Release 3.6.0.1, page 80

Upgrade Instructions for 3.6.0.1

Web upgrade is recommended to upgrade from release 3.6(0) to 3.6.0.1. Carefully review and execute the instructions described in Upgrade Instructions for 3.6(x) Minor Releases and Patches to upgrade your CAS(es) and CAM.

Note For 3.6.0.1 patch upgrade via web console, the machine (CAS or CAM) will NOT automatically reboot. The patch upgrade should complete in 2-5 minutes.

Step 1 Log into Cisco Secure Software and download the **cca-3.6.0-to-3.6.0.1-upgrade.tar.gz** patch file to your local computer from the 3.6.0 folder under http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.6.0

Step 2 Upgrade each CAS using one of the following procedures. Carefully follow instructions:

- Upgrade CAS from CAS Management Pages, or
- Upgrade CAS from CAS Direct Access Web Console

Step 3 Upgrade your CAM using the following procedure:

- Upgrade CAM from CAM Web Console, page 99

Step 4 Alternatively:

a. If upgrading HA pairs, refer to Upgrading High Availability Pairs, page 103

b. If SSH upgrade is preferred, refer to Upgrading via Console/SSH, page 101

Important Notes for Release 3.6(0)

Important Notes for 3.6(0)/3.6.0.1 Clean Access Server Machines with Broadcom NIC Controllers

Servers with Broadcom NIC controllers, upon installing/upgrading to 3.6.0/3.6.0.1, may demonstrate issues with networks where VLAN tags are of importance. Cisco has made instructions available to modify a setting on Broadcom controllers to address the issue. See CSCsd08348, page 79 for complete details.

Note This issue is resolved with release 3.6(1) and above. See Resolved Caveats - Release 3.6(1), page 76.

Important Notes for 3.6(0) Installation

Cisco Clean Access recommends performing the 3.6(0) new installation if you have an immediate need for a new installation or new deployment of Cisco Clean Access NAC Appliance.

If no immediate features are needed, Cisco recommends waiting for subsequent minor releases of 3.6(x) (for example, 3.6(1) or 3.6(2)) before performing upgrade to the 3.6(x) platform.

If immediate features and upgrade are required, Cisco Clean Access provides a 3.6(0) upgrade procedure. In this case, before upgrading to 3.6(0) ED, please ensure you understand the following:

- Cisco Clean Access release 3.6(0) ED is a major software release with Early Deployment status.
- You can only upgrade to 3.6(0) from release 3.5(7) or 3.5(8).
- Read and review the installation or upgrade process completely before starting.
- The 3.6(0) migration differs from minor release upgrades and requires physical CD installation, in addition to an upgrade file.
- 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 box before upgrading your production Clean Access environment, you will need to get a trial license for your test servers. For details, see “How to Obtain Evaluation Licenses” in *Cisco NAC Appliance Service Contract/Licensing Support*.

- Do not upgrade to release 3.6(0) if you are currently using **Monitoring > SNMP** traps from the Clean Access Manager.
- If you need further assistance, contact TAC, as described in Obtaining Documentation and Submitting a Service Request, page 115.

Important Notes for Nessus Plugins with 3.6(0) Upgrade

When upgrading to 3.6(0), and using network scanning (Nessus) plugins for any specified client OS, be sure to enable the same plugins in the "ALL" OS category (and deselect "Enable scanning with selected plugins" for the "ALL" OS category, if applicable). This will prevent users from being quarantined with no way to remediate or be removed. This issue is resolved in release 3.6.0.1 of Cisco Clean Access. See caveat CSCsc82522, page 80 for details.

New Features and Enhancements in Release 3.6(0)

This section details the new features delivered with release 3.6(0) of the Cisco Clean Access Manager and Cisco Clean Access Server, as well as enhancements from release 3.5(8).

Note Refer to General Preparation for Upgrade, page 85 for information on migration/upgrade.

Support for CCA-3140-H1

The CCA-3140-H1 is an affordable 1U, 1 Xeon 2.8GHz CPU Intel processor server equipped with features that provide customers with a platform for Cisco Clean Access Manager or Server deployment.

Expanded Support for RAID/SATA Hardware

Release 3.6(0) of Cisco Clean Access (NAC Appliance) provides support for the following:

- RAID controller support
- SATA servers
- SCSI controller support

Preconfigured Checks for Anti-Spyware Software

With release 3.6, Cisco Clean Access expands and adds new Clean Access Agent-based support for the detection of Anti-Spyware (AS) software and subsequent checking of AS application status. As with Antivirus product support, this is achieved through communicating with the installed Anti-Spyware software (if there is any installed AS software) through an API on the client device.

Administrators will be able to test for the existence of anti-spyware or spyware blocker software on clients, as well as if those products are up-to-date. Cisco Clean Access Agent Updates will incorporate the latest revisions of AS product support into the newly-combined **Supported AV/AS Product List**, providing support for 17 new AS vendors, in addition to support for 21 AV product vendors. See Expanded AV/AS Product List (Version 22), page 37 for details.

Table 5 summarizes changes related to the Antispyware integration for release 3.6(0).

Table 5 Summary of Web Console Page Enhancements for AS Integration

Changes to Web Console Pages Under Device Management > Clean Access > Clean Access Agent:	New Feature
Rules > New AS Rule	New AS Rule page added
Rules > AV/AS Support Info	AS information added to AV/AS Support Info page (Category: **Anti-Spyware** added to form, and page name changed from "Agent-AV Support Info")
Requirements > New Requirement	New **AS Definition Update** requirement type added to New Requirement page and to Clean Access Agent
Requirements > Requirement-Rules	AV/AS definition files allowed to be X days older than current system date or latest file date. See Support for AV/AS Definition Files to be Older than Current System Date, page 38
Reports > Report List | View report	Client AV/AS information and Agent version added to Agent report if AV/AS check fails
Updates | "Current Version of Supported AV/AS Product List" (was: "Current Version of Supported AV Product List")	AS chart integrated into Supported AV/AS Product List

For additional details, see the "Clean Access Agent" chapter of the *Cisco Clean Access (NAC Appliance) Manager Installation and Administration Guide, Release 3.6*.

Expanded AV/AS Product List (Version 22)

Cisco Clean Access release 3.6(0) integrates Antispyware product support in the newly-combined **Supported AV/AS Product List**, adding the following 17 AS vendors for Windows XP/2000:

- AhnLab, Inc.
- America Online, Inc
- Bullet Proof Soft
- Computer Associates International, Inc

- EarthLink, Inc.
- Javacool Software LLC
- Lavasoft, Inc.
- McAfee, Inc.
- MicroSmarts LLC
- Microsoft Corp.
- PC Tools Software
- Prevx Ltd.
- Safer Networking Ltd.
- Sunbelt Software
- Trend Micro Inc.
- Webroot Software, Inc.
- Yahoo!, Inc.

Note Cisco Clean Access currently provides Antispyware product support for Windows XP/2000 only.

In addition, Cisco Clean Access extends AV product support to 21 vendors with the addition of the following AV products for Windows XP/2000:

- AhnLab Security Pack, 2.x
- V3Pro 2004, 6.x
- avast! Antivirus, 4.x
- EarthLink Protection Control Center AntiVirus, 1.x
- Panda Titanium 2006 Antivirus + Antispyware, 5.x
- Norton Internet Security, 9.x
- SBC Yahoo! Anti-Virus, 7.x

See Clean Access Supported AV/AS Product List, page 43 for the latest AV/AS product charts as of the latest release.

See Supported AV/AS Product List Version Summary, page 59 for details on what has changed for each version of the list.

Support for AV/AS Definition Files to be Older than Current System Date

Release 3.6(0) introduces the ability to configure AV Virus Definition rules and AS Spyware Definition rules to allow definition files to be any number of days older than the latest file date or current system date.

Note For AS Spyware Definition rules, the system will enforce this feature (allowing the definition files to be X days older then the current system date) until Cisco Update service is available to regularly update the date/version for Spyware definition files.

This feature affects the following web console pages:

- New checkbox options for AV and AS rules are added under **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement-Rules**
- Notes are also added under:
  - **Device Management > Clean Access > Clean Access Agent > Rules > New AS Rule**
  - **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info | Category: Anti-Spyware**
  - **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement | Requirement Type: AS Definition Update**

Enhanced OS Fingerprinting

By default, the system uses the User-Agent string from the HTTP header to determine the client OS. Release 3.6.0 provides additional detection options to include using the platform information from JavaScript, or OS fingerprinting from the TCP/IP handshake to determine the client OS. This feature is intended to prevent users from changing identification of their client operating systems through manipulating HTTP information. Note that this is a "passive" detection technique (accomplished without Nessus) that only inspects the TCP handshake and is not impacted by the presence of a personal firewall.

This new feature affects the following web console pages:

- There is a new update entry for "**Current Version of OS Detection Fingerprint**" under **Device Management > Clean Access > Clean Access Agent > Updates**.
- There is a new **OS Detection** link and page under **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > OS Detection**.

Enhanced L2 Strict Mode User Support (Agent Only)

With release 3.6(0) CAM/CAS and 3.6.0.0 Agent, administrators can restrict Clean Access Agent clients to be connected to the Clean Access Server directly as their only gateway using the "Enable L2 strict mode for Clean Access Agent."

When this feature is enabled, the Clean Access Agent will send the MAC addresses for all interfaces on the client machine with the login request to the CAS. The CAS then checks this information to ensure no NAT exists between the CAS and the client. The CAS verifies and compares MAC addresses to ensure that the MAC address seen by the CAS is the MAC address of the Agent client machine only. If user home-based wireless routers or NAT devices are detected between the client device and the CAS, the user is not allowed to log in. With release 3.6(0), administrators have the following options:

- Enable L3 support for Clean Access Agent —The CAS allows all users from any hops away.
- Enable L2 strict mode for Clean Access Agent — The CAS does not allow users who are more than one hop away from the CAS. The user will be forced to remove any router between the CAS and the user's client machine to gain access to the network.
- Both options left unchecked (Default setting)— The CAS performs in L2 mode and expects that all clients are one hop away. The CAS will not be able to distinguish if a router is between the CAS and the client and will allow the MAC address of router as the machine of the first user who logs in and any subsequent users. Checks will not be performed on the actual client machines passing through the router as a result, as their MAC addresses will not be seen.

Note

- Enabling or disabling L3 or L2 strict mode ALWAYS requires an **Update** and **Reboot** of the CAS to take effect. **Update** causes the web console to retain the changed setting until the next reboot. **Reboot** causes the process to start in the CAS.
- L3 and L2 strict options are mutually exclusive. Enabling one option will disable the other option.

This affects the following web console pages:

- There is a new "**Enable L2 strict mode for Clean Access Agent**" option under **Device Management > CCA Servers > Manage [CAS_IP] > Network > IP**.

Agent Patch File Upload

Release 3.6(0) now supports uploading of the Agent Patch Upgrade file (upgrade.tar.gz) in addition to the Agent Setup Installation File (setup.tar.gz) through the same **Distribution** page interface control. This feature allows administrators to revert to a previous patch upgrade file for distribution. Previously, only setup installation files for new installations of the Clean Access Agent could be reverted to prior versions.

This feature is only available for release 3.6(0) and above and Clean Access Agent version 3.6.0.0 or above.

Caution Because the CAM differentiates the Agent setup and upgrade file types by filename, it is mandatory for users to retain the same names used for the files on Cisco Secure Downloads, for example, CCAAgent**Setup**-3_6_0_0.tar.gz or CCAAgent**Upgrade**-3_6_0_0.tar.gz.

This enhancement affect the following web console page:

- The functioning and name of the "**Clean Access Agent Setup to Upload**" field is changed to "**Clean Access Agent Setup/Patch to Upload**" under **Device Management > Clean Access > Clean Access Agent > Distribution**.

Clean Access Agent (3.6.0.0)

- Version 3.6.0.0 and above of the Clean Access Agent supports the new Anti-Spyware (AS) integration provided with release 3.6(0).
- The 3.6.0.0 Agent adds a new dialog screen to show all of the AV and AS products installed on the client machine. Right-clicking the Agent icon in the system tray (taskbar menu) and selecting **Properties** will display the installed AV/AS product details for the client machine.
- Cisco Clean Access Release 3.6(0) introduces new 4-digit versioning of the Clean Access Agent to differentiate feature upgrades from periodic updates for AV/AS product support:
  - The first 2 digits reflect the Cisco Clean Access version with which it is bundled (e.g. 3.6.x.x for release 3.6(0))
  - The 3rd digit reflects non-AV/AS changes to Agent functionality (e.g. 3.6.1.x)
  - The 4th digit indicates upgrades related to Supported AV/AS Product list updates (e.g. 3.6.0.1)

For additional details, see also:

- Agent Patch File Upload, page 40

- Clean Access Agent Version Summary, page 63

SSL Certificate Chain is Verified Before Installation

Release 3.6(0) now verifies the SSL certificate chain before installing certificates on the CAM and CAS. Cisco Clean Access will not allow installation of an unverifiable certificate chain, and only restarts CAM/CAS web service after the entire certificate chain is verified and installed. This enhancement removes the need to import certificates in a certain sequence (as was necessary for prior releases), as certificates are imported to a temporary store first before being verified and installed. This feature is also intended to support administrators using intermediate signing authorities, in cases where several intermediate certificates may need to be imported. When importing any of the following:

- Private key from backup
- CA-signed certificate
- Intermediate root certificates

The CAM/CAS will place these into a temporary store, verify the certificate chain, install the uploaded certificates, and only restart CAM and CAS web service if the verification and installation of uploaded certificates is successful.

Page layouts have been enhanced for certificate forms, and Private Key and Installed Certificate Details can now be viewed from individual popups on the Import Certificate and Export Certificate forms, respectively.

These enhancements affects CAM web console, CAS management pages and CAS direct access web console pages as follows:

CAM web console:

- **Administration > CCA Manager > SSL Certificate | Import Certificate**
- **Administration > CCA Manager > SSL Certificate | Export Current Certificate**

CAS management pages:

- **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs | Import Certificate**
- **Device Management > CCA Servers > Manage [CAS_IP] > Network > Certs | Export Certificate Request**

CAS direct access web console:

- **https://<CAS_IP>/admin/Administration > SSL Certificate | Import Certificate**
- **https://<CAS_IP>/admin/Administration > SSL Certificate | Export Current Certificate**

In addition, the following notes are added to the Import Certificate form on the CAS management pages and CAS direct access web console:

> (* “Trust Non-Standard CA” is for communication between the Clean Access Manager and Clean Access Server. If the Clean Access Manager cert is signed by a CA that is not well known, import the CA cert here to have it accepted. Clean Access Server must be rebooted to take effect.)

The following note is added to the Import Certificate form on the CAM SSL Certificate tab:

> (* Non-Standard CA is for SSL communication between the Clean Access Manager and some authentication servers, e.g. LDAP Server.)

Ports Changed for CAM/CAS Connectivity Across Firewall

The Clean Access Manager uses RMI for parts of its communication with the Clean Access Server, which means it uses dynamically allocated ports for this purpose. For customer deployments that have firewalls between the CAS and the CAM, Cisco recommends setting up rules in the firewall that allow communication between the CAS and CAM machines, that is, a rule that allows traffic originating from the CAM destined to the CAS (and vice versa).

In release 3.6, the port range is changed to TCP 8995~8996.

For release 3.6, TCP ports 80, 443, 1099, and 8995~8996 are required.

Maximum Simultaneous Connections Supported in NAT Gateway Mode

In release 3.6, ports 20000-65535 are used for NAT Gateway mode, supporting a maximum of 45,536 simultaneous connections.

Nessus 2.2 Plugin Support

With release 3.6(0) and above, you can use Nessus 2.2 plugins to perform network scanning in Cisco Clean Access. The filename of the uploaded Nessus plugin archive must be **plugins.tar.gz**.

Note that most Nessus 2.2 plugins are backwards compatible with Nessus 2.0. Plugins not compatible with Nessus 2.2 can be updated by uploading a new plugins.tar.gz archive.

Note Prior releases 3.5(8) and below support Nessus 2.0 plugins only.

Note Due to a licensing requirement by Tenable, Cisco does not bundle pre-tested Nessus plugins or automated plugin updates to Cisco Clean Access, effective as of Release 3.3.6/3.4.1. Customers can still download Nessus plugins selectively and manually through the Nessus site. For details on available plugins, see http://www.nessus.org/plugins/index.php?view=all.
For details on Nessus plugin feeds, see http://www.nessus.org/plugins/index.php?view=feed.

Network Scanner (Nessus) Page Enhancements

Enhancements to the **Plugins** page layout greatly improve GUI response time when selecting Nessus plugins and move the "Show [Selected] Plugins" dropdown to the bottom of the page. The Nessus plugin **Options** page layout is also enhanced to differentiate Category from Preference Name dropdown menus, and Enable checkbox, if applicable.

These enhancements affect the following pages of the CAM web console, respectively:

- **Device Management > Clean Access > Network Scanner > Scan Setup > Plugins**
- **Device Management > Clean Access > Network Scanner > Scan Setup > Options**

General Setup Page Enhancements

The **Device Management > Clean Access > General Setup** page layout is improved to differentiate **Clean Access Agent** controls from **Web Login** user controls.

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** for AS and AV integration support in release 3.6(x). 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 and CAM/CAS 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 that you keep 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 that you keep 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 Cisco Clean Access release:

- Clean Access AV Support Chart (Windows XP/2000), page 44
- Clean Access AV Support Chart (Windows ME / 98), page 52
- Clean Access AS Support Chart (Windows XP/2000), page 55

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 what has changed from version to version of the Supported AV/AS Product List or Clean Access Agent, see also:

- Supported AV/AS Product List Version Summary, page 59
- Clean Access Agent Version Summary, page 63

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, it is recommended to use AV/AS Rules mapped to AV/AS Definition Update Requirements when checking for antivirus/antispyware software on clients. In the case of a non-supported AV/AS product, or if an AV/AS product/version is not available through AV/AS Rules, administrators always have the option of using Cisco provided pc_ checks and pr_rules for the AV or AS vendor or of creating their own custom checks, rules, and requirements through **Device Management > Clean Access > Clean Access Agent** (use New Check, New Rule, and New File/Link/Local Check Requirement). See the *Cisco Clean Access (NAC Appliance) Manager Installation and Administration Guide, Release 3.6* for configuration details.

Note that Cisco 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 products by AV/AS vendors, the Cisco Clean Access team will upgrade 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 6 lists Windows XP/2000 Supported Antivirus Products as of the latest release of the Cisco NAC Appliance software. (See Table 7 for Windows ME/98).

Table 6 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 49, Release 3.6.4.4 / 3.6.5.0 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				

Table 6 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 49, Release 3.6.4.4 / 3.6.5.0 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 Antivirus	0.x	yes (3.5.2)	yes (3.5.2)	yes
ClamWin Free Antivirus	0.x	yes (3.5.4)	yes (3.5.4)	yes
Computer Associates International, Inc.				
CA Anti-Virus	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
CA eTrust Antivirus	7.x	yes (3.5.0)	yes (3.5.0)	yes
CA eTrust Internet Security Suite AntiVirus	7.x	yes (3.5.11)	yes (3.5.11)	yes
CA eTrustITM Agent	8.x	yes (3.5.12)	yes (3.5.12)	yes
eTrust EZ Antivirus	6.1.x	yes (3.5.3)	yes (3.5.8)	yes
eTrust EZ Antivirus	6.2.x	yes (3.5.0)	yes (3.5.0)	yes
eTrust EZ Antivirus	6.4.x	yes (3.5.0)	yes (3.5.0)	yes
eTrust EZ Antivirus	7.x	yes (3.5.0)	yes (3.5.0)	yes
eTrust EZ Armor	6.1.x	yes (3.5.0)	yes (3.5.8)	yes
eTrust EZ Armor	6.2.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
eTrust EZ Armor	7.x	yes (3.5.0)	yes (3.5.0)	yes
Defender Pro LLC				
Defender Pro Anti-Virus	5.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
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

Table 6 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 49, Release 3.6.4.4 / 3.6.5.0 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	6.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
F-Secure Internet Security	7.x	yes (4.0.4.0)	yes (4.0.4.0)	-
F-Secure Internet Security 2006 Beta	6.x	yes (3.5.8)	yes (3.5.8)	yes
GData Software AG				
AntiVirusKit 2006	2006.x	yes (4.1.0.0)	yes (4.1.0.0)	-
Grisoft, Inc.				
Antivirussystem AVG 6.0	6.x	yes (3.5.0)	yes (3.5.0)	-
AVG 6.0 Anti-Virus - FREE Edition	6.x	yes (3.5.0)	yes (3.5.0)	-
AVG 6.0 Anti-Virus System	6.x	yes (3.5.0)	yes (3.5.0)	-
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

Table 6 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 49, Release 3.6.4.4 / 3.6.5.0 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	3.x	yes (3.5.8)	yes (3.5.8)	yes
McAfee Managed VirusScan	4.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
McAfee VirusScan	10.x	yes (3.5.4)	yes (3.5.4)	yes
McAfee VirusScan	11.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
McAfee VirusScan	4.5.x	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan	8.x	yes (3.5.1)	yes (3.5.1)	yes
McAfee VirusScan	8xxx	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan	9.x	yes (3.5.1)	yes (3.5.1)	yes
McAfee VirusScan	9xxx	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan Enterprise	7.0.x	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan Enterprise	7.1.x	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan Enterprise	7.5.x	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan Enterprise	8.0.x	yes (3.5.0)	yes (3.5.0)	yes
McAfee VirusScan Enterprise	8.x	yes (3.6.5.0)	yes (3.6.5.0)	yes
McAfee VirusScan 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)	-

Table 6 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 49, Release 3.6.4.4 / 3.6.5.0 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 Lite	3.x	yes (3.5.9)	yes (3.5.9)	-
Panda Antivirus Platinum	7.04.x	yes (3.5.0)	yes (3.5.0)	yes
Panda Antivirus Platinum	7.05.x	yes (3.5.0)	yes (3.5.0)	yes
Panda Antivirus Platinum	7.06.x	yes (3.5.0)	yes (3.5.0)	yes
Panda Client Shield	4.x	yes (4.0.4.0)	yes (4.0.4.0)	-
Panda Internet Security 2007	11.x	yes (4.0.4.0)	yes (4.0.4.0)	yes
Panda 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)	-
SaID Ltd.				
Dr.Web	4.32.x	yes (3.5.0)	yes (3.5.0)	yes
Dr.Web	4.33.x	yes (3.5.11.1)	yes (3.5.11.1)	yes
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)	-

Table 6 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 49, Release 3.6.4.4 / 3.6.5.0 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 Plc.				
Sophos Anti-Virus	3.x	yes (3.5.3)	yes (3.5.3)	-
Sophos Anti-Virus	4.x	yes (3.6.3.0)	yes (3.6.3.0)	-
Sophos Anti-Virus	5.x	yes (3.5.3)	yes (3.5.3)	yes
Sophos Anti-Virus	6.x	yes (4.0.1.0)	yes (4.0.1.0)	yes
Sophos Anti-Virus 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

Table 6 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 49, Release 3.6.4.4 / 3.6.5.0 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	8.x	yes (3.5.3)	yes (3.5.3)	yes
Norton SystemWorks 2005 Premier	8.x	yes (3.5.3)	yes (3.5.3)	yes
Norton SystemWorks 2006 Premier	12.0.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Symantec AntiVirus	10.x	yes (3.5.3)	yes (3.5.3)	yes
Symantec AntiVirus	9.x	yes (3.5.0)	yes (3.5.0)	yes
Symantec AntiVirus Client	8.x	yes (3.5.0)	yes (3.5.0)	yes
Symantec AntiVirus Server	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
Symantec 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 6 Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 49, Release 3.6.4.4 / 3.6.5.0 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 7 lists Windows ME/98 Supported AV Products as of the latest release of the Cisco NAC Appliance software. (See Table 6 for Windows XP/2000.)

Table 7 Clean Access Antivirus Product Support Chart (Windows ME/98) Version 49, Release 3.6.4.4 / 3.6.5.0 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 7 Clean Access Antivirus Product Support Chart (Windows ME/98) Version 49, Release 3.6.4.4 / 3.6.5.0 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 8 lists Windows XP/2000 Supported Antispyware Products as of the latest release of the Cisco Clean Access software.

Table 8 Clean Access Antispyware Product Support Chart (Windows XP/2000) Version 49, Release 3.6.4.4 / 3.6.5.0 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

Table 8 Clean Access Antispyware Product Support Chart (Windows XP/2000) Version 49, Release 3.6.4.4 / 3.6.5.0 Agent (Sheet 2 of 4)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
CA eTrust PestPatrol Anti-Spyware	8.x	yes (4.1.0.0)	yes (4.1.0.0)	yes
CA eTrust PestPatrol Anti-Spyware Corporate Edition	5.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
PestPatrol Corporate Edition	4.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
PestPatrol Standard Edition (Evaluation)	4.x	yes (3.6.0.0)	yes (3.6.0.0)	yes
EarthLink, Inc.				
Aluria Security Center AntiSpyware	1.x	yes (4.1.0.0)	yes (4.1.0.0)	-
EarthLink Protection Control Center AntiSpyware	1.x	yes (3.6.0.0)	yes (3.6.0.0)	-
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)	-	-

Table 8 Clean Access Antispyware Product Support Chart (Windows XP/2000) Version 49, Release 3.6.4.4 / 3.6.5.0 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 V7.95	7.95.x	yes (4.1.0.0)	-	-
Spyware Begone V8.20	8.20.x	yes (4.1.0.0)	-	-
Spyware Begone V8.25	8.25.x	yes (4.1.0.0)	-	-
Microsoft Corp.				
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)	-	-

Table 8 Clean Access Antispyware Product Support Chart (Windows XP/2000) Version 49, Release 3.6.4.4 / 3.6.5.0 Agent (Sheet 4 of 4)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
Webroot Spy Sweeper Enterprise Client	2.x	yes (3.6.1.0)	-	-
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 9 details enhancements made per version of the Supported Antivirus/Antispyware Product List. See Clean Access Supported AV/AS Product List, page 43 for the latest Supported AV list as of the latest release. See New and Changed Information, page 8 for the release feature list.

Table 9 Supported AV /AS Product List Versions

Version	Enhancements
Release 3.6.4.4 —3.6.5.0 Agent	
Release 3.6.4.3 —3.6.5.0 Agent	
Version 49	**AV Chart (Windows XP/2000):** support added for the following new 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 • AhnLab SpyZero 2007, 3.x • Primary Response SafeConnect, 2.x
Version 48	Minor internally used data change
Version 47	**AV Chart (Windows XP/2000):** support added for the following new products: • AOL Safety and Security Center Virus Protection, 102.x • AOL Safety and Security Center Virus Protection, 210.x • Cox High Speed Internet Security Suite, 3.x • F-Secure Anti-Virus, 7.x • F-Secure Internet Security, 7.x • AVG 7.5, 7.x • McAfee Managed VirusScan, 4.x • Panda Antivirus 2007, 2.x • Panda Antivirus + Firewall 2007, 6.x • Panda ClientShield, 4.x • Panda Internet Security 2007, 11.x • Panda Platinum 2006 Internet Security, 10.x • BitDefender Antivirus Plus v10, 10.x • BitDefender Antivirus v10, 10.x • BitDefender Internet Security v10, 10.x **AS Chart (Windows XP/2000):** support added for the following new product: • Cox High Speed Internet Security Suite, 3.x
Release 3.6(4) —3.6.4.0 Agent	

Table 9 Supported AV /AS Product List Versions (continued)

Version	Enhancements
Version 46, 45	Minor internally used data change
Version 44	**AV Chart (Windows XP/2000):** support added for the following new products: • Sophos Anti-Virus, 6.x • Trend Micro HouseCall, 1.x • Trend Micro PC-cillin Internet Security 12, 12.x • Trend Micro PC-cillin Internet Security 14, 14.x
Version 43	Minor internally used data change
Release 3.6(3) —3.6.3.1/3.6.3.0 Agent	
Version 42	Minor internally used data change
Version 41	Added virus definition version check support for AVG Anti-Virus 7.1, 7.1.x
Version 40	Added support for the following two products: • AVG Anti-Virus 7.1, 7.1.x • Sophos Anti-Virus, 4.x
Release 3.6(2) —3.6.2.0 Agent	
Version 39, 38	Minor internally used data changes
Version 37	**AV Chart (Windows XP/2000):** Live Update support added for TrendMicro OfficeScan Client 5.x, 6.x and 7.x.
Version 36, 35, 34	Minor internally used data changes.
Version 33	**AV Chart (Windows XP/2000):** Live update support removed for Trend Micro OfficeScan Client 5.x and 6.x
Version 32	Minor internally used data change.
Version 31	**AV Chart (Windows XP/2000):** support added for the following new products: • Ahnlab V3Pro 2004, 6.x (def date support) • CA eTrustITM Agent, 8.x • F-Secure Anti-Virus 5.44 • Trend Micro Client/Server Security Agent, 7.x **AS Chart (Windows XP/2000**)—No changes **AV Chart (Windows ME/98) —** No changes
Version 30	**AV Chart (Windows XP/2000):** support added for Norton AntiVirus 2006, 12.x
Version 29	Minor internally used data change.
Release 3.6(1) —3.6.1.0 Agent	

Table 9 Supported AV /AS Product List Versions (continued)

Version	Enhancements
Version 28	**AV Chart (Windows XP/2000):** support added for the following new products: • AOL Safety and Security Center Virus Protection, 1.x • Microsoft Windows OneCare Live, 0.8.x • Rising Antivirus Software AV, 17.x • Rising Antivirus Software AV, 18.x • F-Prot for Windows, 3.16x • Dr.Web, 4.33.x • BitDefender 9 Internet Security AntiVirus, 9.x
	AS Chart (Windows XP/2000)—support added for the following new products: • Microsoft AntiSpyware, 1.X • AOL Safety and Security Center Spyware Protection, 2.x • CA eTrust Internet Security Suite AntiSpyware, 5.x • CA eTrust PestPatrol, 5.x • Ad-Aware SE Professional, 1.x • Ad-Aware SE Professional, 1.x • Spyware Begone V7.30, 7.30.x • Spyware Begone V7.40, 7.40.x • Webroot Spy Sweeper Enterprise Client, 2.x **Note** If planning to support Microsoft AntiSpyware 1.X, use the 3.6.1.0+ Agent. Microsoft AntiSpyware 1.X support is removed for 3.6.0.0/3.6.0.1 Agents. **AV Chart (Windows ME/98) —** No changes
Release 3.6.0.1 —3.6.0.1 Agent	
Version 27	No changes to support charts for 3.6.x.x Agents.
Version 26	**AV Chart (Windows XP/2000):** support added for the following new products: • F-Prot for Windows, 3.16c • F-Prot for Windows, 3.16d • Kaspersky Anti-Virus Personal Pro, 5.0.x • Microsoft Windows OneCare Live, 0.8.x • WebAdmin Client Antivirus, 3.x
Version 25	**AS Chart (Windows XP/2000**)—Removed support of the virus def date check for AVG Free Edition 7.x
Version 24	Minor internally used data change.
Version 23	**AS Chart (Windows XP/2000**) —Removed live update support for Spyware Doctor 3.2, 3.x
Release 3.6(0) —3.6.0.0 Agent	
Version 22	Removed entry for CA eTrust PestPatrol, 5.x

Table 9 Supported AV /AS Product List Versions (continued)

Version	Enhancements
Version 21	**AS Chart (Windows XP/2000**)—New anti-spyware product support for 17 AS vendors **AV Chart (Windows XP/2000) —**Adds support for the following new products: • AhnLab Security Pack, 2.x • V3Pro 2004, 6.x • avast! Antivirus, 4.x • EarthLink Protection Control Center AntiVirus, 1.x • Panda Titanium 2006 Antivirus + Antispyware, 5.x • Norton Internet Security, 9.x • SBC Yahoo! Anti-Virus, 7.x **AV Chart (Windows ME/98) —** No changes

Clean Access Agent Version Summary

This section consolidates information for the Clean Access Agent client software. Table 10 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 versions.

See Clean Access Supported AV/AS Product List, page 43 for details on related AV/AS support.

Table 10 Clean Access Agent Versions

Agent Version [1]	Feature / Enhancement
3.6.5.0	• Support for new AOL, F-Secure, AVG, McAfee, Panda, BitDefender, Cox AV/AS products. • Version 3.6.5.0 adds support for IE 7.0 See also Clean Access Agent (3.6.5.0), page 11 and Supported AV/AS Product List Version Summary, page 59.
3.6.4.0	• Support for new TrendMicro, Sophos and Grisoft AV/AS products. • Version 3.6.4.0 adds support for IE 7 Beta 3. See also Clean Access Agent (3.6.4.0), page 17 and Supported AV/AS Product List Version Summary, page 59
3.6.3.1	• Resolves caveat CSCse72371, page 73, CSCse72384, page 73, CSCse72396, page 73, See also Clean Access Agent Enhancements (3.6.3.1), page 19.
3.6.3.0	• Enhancements for AV/AS Rule (XP/2000) support • Resolves caveat CSCsd94974, page 73 See also Clean Access Agent Enhancements (3.6.3.0), page 19.
3.6.2.0	• Enhancements for AV/AS Rule (XP/2000) support See also Clean Access Agent Enhancements (3.6.2.0), page 27.
3.6.1.0	• Enhancements for AV Rule (XP/2000) support • Can be run by restricted user (non-administrator or power-user). • Event.log is now stored in user's home directory instead of installation directory. See Enable Debug Logging on the Clean Access Agent, page 110. See also Clean Access Agent Enhancements (3.6.1.0), page 33, Resolved Caveats - Release 3.6.1.1, page 75, and Resolved Caveats - Release 3.6(1), page 76.

Table 10 Clean Access Agent Versions

Agent Version [1]	Feature / Enhancement
3.6.0.1	• Resolves Caveat CSCsc89288, page 81. See also Enhancements for Release 3.6.0.1, page 34. **Note** Do not upgrade Agent from 3.5.11 (released 30-JAN-2006) to 3.6.0.0 or 3.6.0.1 (released December 2005). See caveat CSCsd28300, page 80.
3.6.0.0	• New 4-digit versioning; last digit indicates update for AV/AS support (e.g. 3.6.0.1) • New dialog shows all AV/AS products installed on the client machine. Right-click systray Agent icon > **Properties** to display installed AV/AS details. • Supports Enhanced L2 Strict Mode User Support (Agent Only), page 39 with 3.6(0) or above CAM/CAS. • Release 3.6(0) allows manual update of the Agent Upgrade file in addition to the Agent Setup file. See Agent Patch File Upload, page 40. See also Clean Access Agent (3.6.0.0), page 40. **Note** Do not upgrade Agent from 3.5.11 (released 30-JAN-2006) to 3.6.0.0 or 3.6.0.1 (released December 2005). See caveat CSCsd28300, page 80.

1. See Release 3.6(x) Agent Upgrade Compatibility Matrix, page 7 for upgrade compatibility details.

Caveats

This section describes the following caveats:

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

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

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

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

Open Caveats - Release 3.6.4.4

Table 11 List of Open Caveats

	Software Release 3.6.4.4	
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.
CSCsc40917	No	When performing 3.6.0 installation, the installer may crash if the “Back” button is chosen from the Package Group Selection screen.
CSCsc75542	No	During CD install, both CAS & CAM packages can be selected from Package Group Selection When installing CCA from the CD, both the packages “CCA Manager” & “CCA Server” can be selected from the “Package Group Selection” for installation. On clicking “OK”, the installation continues. Workaround: User is responsible for installing **only one** package on one machine. The user must not to select either both packages or no packages.
CSCsd90433	No	Apache does not start on HA-Standby CAM after heartbeat link is restored

Table 11 List of Open Caveats (continued)

	Software Release 3.6.4.4	
DDTS Number	**Corrected**	**Caveat**
CSCse60519	No	Cron job to sync system time not created or updated on HA-Inactive CAM The file /etc/cron.daily/sync-time gets created or updated on modifying the time servers for CAM. This cron file does not get created on high availability HA-Inactive CAM, thereby depriving the inactive system to sync the system time from the time servers on a regular basis. Steps to reproduce: 1. Setup CAM in HA-failover mode 2. Go to web page: Administration > Clean Access Manager > System 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 CAM 5. Check the HA-Inactive CAM 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 CAM should reflect the changes upon modification of time server settings on HA-Active CAM Workaround: After modifying the time servers setting on HA-Active CAM, do a failover by shutting down the active CAM; This will make the inactive CAM take over the Service IP address; Modify the time server settings; and start the other CAM.
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 11 List of Open Caveats (continued)

	Software Release 3.6.4.4	
DDTS Number	**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.

Resolved Caveats - Release 3.6.4.4

Table 12 List of Closed Caveats

	Software Release 3.6.4.4	
DDTS Number	**Corrected**	**Caveat**
CSCsj33976	Yes	CAM displays shared secret of CCA setup when adding CAS to CAM A vulnerability exists in the Cisco Network Admission Control (NAC) Appliance that can allow an attacker to obtain the shared secret that is used between the Cisco Clean Access Server (CAS) and the Cisco Clean Access Manager (CAM). Cisco has released free software updates that address this vulnerability. This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20080416-nac.shtml **Note** There is no workaround for this issue.

Resolved Caveats - Release 3.6.4.3

Table 13 List of Closed Caveats

	Software Release 3.6.4.3	
DDTS Number	**Corrected**	**Caveat**
CSCsd52349	Yes	After viewing details on a user the agent report goes back to first page When viewing the Cisco Clean Access Agent report, if the Administrator clicks on a specific user ID to view details, the report refreshes back to the first/welcome page.
CSCse60046	Yes	Database connection failed entry visible in CAS log files Expected Results: Under the current architecture, CAS should never try to make a direct connection to the PostgreSQL database
CSCsf01786	Yes	/etc/grub.conf needs to be a symbolic link 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 customers 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
CSCsf03465	Yes	Certificate import does not delete old .tomcat.csr file When a private key/certificate combination is imported into either the CAM or the CAS, the existing .tomcat.csr file should be deleted. Otherwise, when the CSR is exported, it will be an incorrect CSR. As a precaution, it is better to always generate a new CSR based on the current key and cert.
CSCsf18821	Yes	Heartbeat Denial-of-Service (DOS) vulnerability Linux-HA heartbeat version older than 1.2.5 and 2.0.7 are subject to remote DOS attack. http://www.securityfocus.com/bid/19516/info
CSCsf98683	Yes	CAM does not send Class attribute in RADIUS accounting When you configure CAM to account user login events to a Radius server and use the Class attribute to account for a particular data, Class attribute is not sent in Radius Accounting packet.
CSCsg00598	Yes	Importing CA signed Cert required re-import of private key When you upload a CA Signed Certificate to the CAM, you are also required to import the associated private key.
CSCsg11143	Yes	validation_table only published on CAS reboot In an HA configuration, if the active Clean Access Server (CAS1) loses connectivity with the Clean Access Manager, but does not reboot, CAS2 then becomes active server. If you then fail back to CAS1, CAS1 does not republish the `intern_validation_table` from the CAM's database. Instead, CAM1 repeatedly adds older entries to the validation table.

Table 13 List of Closed Caveats (continued)

DDTS Number	Software Release 3.6.4.3 Corrected	Caveat
CSCsg24153	Yes	Shared secret not updated on service perfigo config "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. When updating the pre-shared key using 'service perfigo config' on the CLI, the script edits /root/.secret but the hash stays the same even after restarting. The shared secret is generated but is always the same constant string. **Workaround** If the customer needs to change the shared secret between the CAM and CAS, then follow the instructions in the README-CSCsg24153 file and apply patch-CSCsg24153.tar.gz from http://www.cisco.com/cgi-bin/tablebuild.pl/cca-patches.
CSCsg41272	Yes	DHCP server re-assigns abandoned leases The DHCP server can repeatedly assign an IP address that another user on the network has statically assigned to a machine. The DHCP server should abandon that IP after clients repeatedly decline it. There are two known workarounds for this bug, one is to enable the option "ping-check" and set it to "true" or "on". This will slow DHCP lease assignment and should not be used in large deployments. This workaround will not work if the user who assigned the static IP address is using a firewall. The other is to identify the network users who are statically assigning IP addresses in the DHCP range and make them stop.
CSCsg44268	Yes	Need to accommodate for new daylight savings time regime from 2007 DST is changing to March (second sunday) and November (first sunday) starting from 2007 instead of April and October.
CSCsg71490	Yes	The CAS web admin password code should be stored as a hashed value
CSCsg73620	Yes	Empty shared secret should not be allowed Empty shared secret should not be allowed by ssconf ("service perfigo config" on CAS), smconf ("service perfigo config" on CAM) or hashpatch.sh file. Allowing an empty shared secret leaves Clean Access Server (CAS) / Clean Access Manager (CAM) vulnerable
CSCsg92130	Yes	Windows Vista should not be recognized by Agent as Windows NT in 3.5.x and 3.6.x Although we don't support Vista in 3.5 and 3.6 branch, Vista machines should be recognized as Windows_ALL instead of Windows_NT when users log in

Table 13 List of Closed Caveats (continued)

	Software Release 3.6.4.3	
DDTS Number	**Corrected**	**Caveat**
CSCsh15238	Yes	Memory leak in RADIUS Authentication/Accounting module If Radius is configured as the authentication/accounting server in [User Management > Auth Server > Auth Server] or [User Management > Auth Server > Accounting], there is a slow memory leak and the system will run out of memory eventually.

Resolved Caveats - Release 3.6.4.2

Table 14 List of Closed Caveats

	Software Release 3.6.4.2	
DDTS Number	**Corrected**	**Caveat**
CSCsg02604	Yes	Default gateway ARP Entries for some DHCP scopes unexpectedly flushing out of the CAS ARP table.
CSCsg04433	Yes	Changes in Disabled / Enabled subnets list gets committed despite errors When editing an auto-generated subnet in the subnet list tab on CAM GUI "Device Management > Manage [IP_Address] > Network > DHCP > Subnet List > Edit", any changes made to the Disabled / Enabled subnets list are committed and saved even if the update failed due to an error or warning in other input provided. To reproduce the issue, add IP range that exceeds the recommended DHCP IP lease limit of 5000 and edit auto-generated subnet on CAM GUI "Device Management > Manage [IP_Address] > Network > DHCP > Subnet List > Edit". Alternatively, incorrect input such as incorrect VLAN ID can be provided instead of having DHCP IP lease limit of 5000. Expected Results: Either none or all the changes should be committed. The warning message must include that the requested changes are not being saved and clicking "Update" button again will save those changes in case of exceeding the recommended DHCP IP lease limit.

Resolved Caveats - Release 3.6.4.1

Table 15 List of Closed Caveats

	Software Release 3.6.4.1	
DDTS Number	**Corrected**	**Caveat**
CSCse97903	Yes	tg3 RPM must be unconditionally installed after upgrade of kernel RPM When upgrading from 3.6(x) versions containing latest tg3 rpm package tg3-2.6.11-2, the tg3 driver gets overwritten by the kernel rpm. Since tg3 rpm gets updated conditionally, the tg3 driver does not get updated post kernel rpm update in those versions. Expected Results: tg3 RPM must be unconditionally installed after upgrade of kernel RPM, which will install proper tg3 driver

Resolved Caveats - Release 3.6(4)

Table 16 List of Closed Caveats

	Software Release 3.6(4)	
DDTS Number	**Corrected**	**Caveat**
CSCse74152	Yes	Serial Login disabling does not work Serial Login capability did not work as intended in any 3.6 or 4.0 branch builds. On the Clean Access Server, the “Disable Serial Login” checkbox could be enabled or disabled, and the state of the Serial Login for that server would not change. On the Clean Access Manager, the instructions described a procedure that, if followed, would not alter the state of the Serial Login for that manager.
CSCse81871	Yes	Perfigo script is not copied to /etc/init.d/perfigo in upgrade script Perfigo script is modified to fix bug CSCse53459, however, this script is not copied (or linked) to /etc/init.d/perfigo
CSCse89648	Yes	Upgrade re-enables serial login 3.5.11, all 3.6 branch and all 4.0 branch upgrades enable serial login, even if it was previously disabled via the HA UI. Workaround: After upgrading to one of the affected versions, go in via the UI and disable serial login again. **Note** This issue affects 3.5(11), 3.6(3), 4.0(1)

Table 16 List of Closed Caveats (continued)

	Software Release 3.6(4)	
DDTS Number	**Corrected**	**Caveat**
CSCse90117	Yes	Macintosh breaks network connectivity if CAS configured w/ VLAN mapping On L2 Inband CAS with VLAN mapping configured, if a Macintosh is introduced on the untrusted network and if the Macintosh is sending out DHCP requests, it breaks packet forwarding on the CAS for all users in the VLAN. Symptoms include devices on the untrusted VLAN not being able to reach any device on the trusted network. Users will not be able to get an IP address. **Note** This issue affects 3.6.3 and 4.0.1 only.
CSCse91178	Yes	Old chain certificate not deleted when temporary certificate regenerated The old chain certificate (.chain.crt) is not deleted when a new temporary certificated is generated. Steps to reproduce: 1) Import a certificate 2) Import a root/intermediate root cert 3) Restart perfigo service 4) Generate a new temporary certificate You will get SSL handshake errors. The old .chain.crt is still present. It will need to be deleted before SSL handshake can successfully occur. **Note** This issue affects 3.6(3) 4.0(0)
CSCse91268	Yes	Post-3.5 to 3.6/4.0 upgrade NIC switch, HA issue with SSKEY When NICs are switched as a result of upgrading a 3.5 system to 3.6/4.0, the HA JSPs have an issue with the SSKEY. When CAM connects to the newly upgraded CASs, it detects that CAS SSKEY has changed and resets it to the old one. However, the CAS HA pages detect that the SSKEY is not what it should be and then changes it back.
CSCse96696	Yes	Changes in Time zone setting should be preserved across CAS / CAM reboot Steps to reproduce: 1. Configure CAM & CAS using GUI 2. Go to CAM web page “Device Management > Clean Access Servers > IP Address > Misc > Time” to modify CAS time zone. [Or “Administration > Clean Access Manager > System Time” to modify CAM time zone] 3. Change time zone from the drop down menu 4. Click “Update Time Zone” 5. Reboot the CAS [or CAM] 6. Check the time zone on CAS [or CAM]. The time zone will be reset Expected Results: Changes in time zone setting should be preserved across CAS / CAM reboot

Resolved Caveats - Release 3.6(3)

Table 17 List of Closed Caveats

	Software Release 3.6(3)	
DDTS Number	**Corrected**	**Caveat**
CSCsc75335	Yes	SNMP traps for CCA error conditions not sent properly
CSCsd73487	Yes	Upgrade script fails to enable DHCP failover after migration from 3.5.x
CSCsd84038	Yes	CCA in-band virtual-access does not forward traffic between Access VLANS
CSCsd94974	Yes	CCA Agent after reboot falsely indicates client logged in as previous temp role.
CSCse38790	Yes	OS Detection Fingerprint updates not replicated to HA-Standby CAM
CSCse56062	Yes	OOB online users are not deleted when timer removes certified devices
CSCse72371	Yes	CCA Agent could not recognize McAfee Enterprise + Anti-Spyware Module 8.0.0
CSCse72384	Yes	With 3.6.3.0 Agent, the Update button could not launch McAfee update
CSCse72396	Yes	CCA Agent could not recognize CA eTrust Antivirus 7.1

Resolved Caveats - Release 3.6.2.2

Table 18 List of Closed Caveats

	Software Release 3.6.2.2	
DDTS Number	**Corrected**	**Caveat**
CSCsd79205	Yes	DB Sync in HA CAMs can be broken by restarting standby In a CAM Failover configuration, if the standby (inactive) CAM is restarted (service perfigo restart), then the DB synchronization is broken from that point on. This is because pg_sync_peer fails and the DB connections to the remote peer fail. Errors can be found in /tmp/pg_sync_log. See Enhancements for Release 3.6.2.2, page 20 for details.

Resolved Caveats - Release 3.6.2.1

Table 19 List of Closed Caveats

	Software Release 3.6.2.1	
DDTS Number	**Corrected**	**Caveat**

CSCsd74376	Yes	CCA 3.6.x Reset Issues with HP servers with Broadcom NICs
		
		In the past, CSCsd08348 has covered issues with Broadcom NICs, namely the BCM5702/BCM5703/BCM5704 which could be resolved by a firmware update from HP. Currently, we're seeing newer revisions of the Broadcom NIC which are not patched by this firmware update, including the BCM5721. NICs are currently resetting and not coming back up which leads to users being unable to SSH/ping/manage the CCA servers. This can be confirmed by checking /var/log/messages for output similar to that which is shown below:
		
		`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.`
		
		Solution:
		1. Customers can verify which type of NIC controller is being used on their CAM/CAS servers by looking at the output of the **`lspci -v`** command.
		2. Customers with machines that have the 5702/5703/5704 Broadcom chipsets need to perform two steps:
		a. Apply the firmware upgrade from HP: http://h18023.www1.hp.com/support/files/networking/us/download/24056.html
		b. Apply the CCA 3.6.2.1 patch as described in Enhancements for Release 3.6.2.1, page 22.
		3. Customers with machines that have other 57xx Broadcom chipsets need to perform only one step:
		a. Apply the CCA 3.6.2.1 patch as described in Enhancements for Release 3.6.2.1, page 22.
		
		See also Known Issues with Broadcom NIC 5702/5703/5704 Chipsets, page 82 for additional information.

Resolved Caveats - Release 3.6(2)

Table 20 List of Closed Caveats

	Software Release 3.6(2)	
DDTS Number	**Corrected**	**Caveat**
CSCsd43158	Yes	Nessus scanning is not working on trunk - 802.1q VLAN packets
CSCsd47291	Yes	Issues removing entries in Filters >Subnets In 3.6.1 and 3.6.0, removing the entry removes it from the CAM DB and UI but does not remove it from the CAS filters and you will see an error in /var/log/messages or on the console. That error message should disappear and the filter should no longer be applied after it has been removed.
CSCsd48226	Yes	Kernel Panic errors seen when using Enhanced OS Fingerprinting
CSCsd53056	Yes	Failed login attempts should be logged in CAM event log with the remote IP address, username and time of login attempt. The failed login event log entry would be quite similar to that of a failed login attempt [from untrusted side] on the CAS.
CSCsd65839	Yes	Upgrade script fails to transfer the snapshot to non-CCA machine from CAS
CSCsd70048	Yes	Edit Filter Subnets for CCA Server does not work

Resolved Caveats - Release 3.6.1.1

Table 21 List of Closed Caveats

	Software Release 3.6.1.1	
DDTS Number	**Corrected**	**Caveat**
CSCsd41503	Yes	3.6.x-to-3.6.1 upgrade breaks browser-based login Upgrade from 3.6.x to 3.6.1 can disable web-login (browser-based login). This happens to be due to tightened permissions on one of the apache directories with 3.6.1
CSCsd42874	Yes	Upgrading to 3.6.1 from 3.6.0 does not upgrade the CCA agent properly With 3.6.1 upgrade from 3.6.0, the CCA agent does not get upgraded properly. The previous agent may remain in the database while the database values change to the upgraded ones.

Resolved Caveats - Release 3.6(1)

Table 22 List of Closed Caveats

	Software Release 3.6(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsc64719	Yes	CA AV configured to use a local http server, Agent cause CA to check FTP The customer has the CA AV configured to only check a local HTTP server. When the agent attempts to update, the agent is causing the CA software to check a FTP server on the Internet instead of the customer custom configure local http server. Symptom: CA Antivirus fails to update from locally configured http server. When the CCA Agent is starting the update connection. Conditions: CA Antivirus is configured to download its update from a local http server instead of the FTP server on the Internet. CCA agent detects that the AV software isn't up to date. User select for the CCA agent to update the AV client. Workaround: Use default setting for the CA AV or manually start the update from CA AV.
CSCsc72195	Yes	DHCP options cannot be added to Managed CAS through Clean Access Manager This issue was found in 3.5.8 in Real-IP Gateway mode. When setting up the DCHP options on a Managed CAS, the options show up in the GUI, but are not reflected in the dhcpd.conf file on the CAS. Example: 'option netbios-node-type 2;' shows up in the CAM's GUI, but not in the dhcpd.conf file of the CAS.
CSCsc75627	Yes	SNMP trapsink settings lost with v3.6 upgrade All SNMP traps [including trapsink IP, community & description] configured on CAM v3.5.x are lost with the upgrade.
CSCsc78387	Yes	This affects machines performing an upgrade and using proxy server for CCA Agent updates, i.e. under Device Management > Clean Access > Clean Access Agent > Updates, the option “Use an HTTP proxy server to connect to the update server” option is checked. If CCA Agent updates are run on 3.5 prior to upgrade, upgrade from 3.5 to 3.6 is performed, then updates are run after upgrade to 3.6, some Cisco Updates may fail until the cache clears from the proxy servers along the HTTP request/response chain between the CAM and the Cisco Servers.

Table 22 List of Closed Caveats (continued)

DDTS Number	Software Release 3.6(1) Corrected	Caveat
CSCsc80264	Yes	CCA agent crashes when run by user with restricted access The admin user (logged as Administrator) installs the CCA Agent, logs off and the user with restricted access logs back on and launches CCA agent. The agent when run by a user with restricted access crashes on following actions: 1. Click “Popup Login Windows” 2. Select / Deselect checkbox “Remember Me” on the CCA Agent Login Window 3. Login for the very first time after install (admin never login after install) 4. Change the “Discovery Host” under Agent Properties (only applicable to agent v3.6.0.0 and up)
CSCsc82506	Yes	Default user agreement page doesn't show correctly through proxy
CSCsc85316	Yes	Firefox has problems with the scan reports link The “user info” box is checked for the successfully authenticated users. When a Firefox client clicks on the Scan Report link on the page that opens with the Logout button, a Javascript error message appears.
CSCsc85405	Yes	Obsolete JSPs could allow DoS attack on CAM. **Note** Security patch-CSCsc85405 resolves this caveat, and the patch is included in 3.6.0.1, and 3.6(1) or above upgrade. The security patch does not need to be re-applied after upgrade to 3.6.0.1 or 3.6(1) or above. (CAM upgrade to 3.6.0.1 or above is required). The patch is required for 3.6(0), and 3.5(8) and below. For further details, see : http://www.cisco.com/en/US/products/ps6128/products_security_notice09186a00805b87a7.html
CSCsc85588	Yes	Obsolete JSPs need to be removed from build
CSCsc88240	Yes	User can login using CCA Agent and is allowed on the network without accepting the “Network Usage Terms & Conditions”. Steps to reproduce: 1. Configure the CAM to check the software and run nessus scans on clients. 2. Launch CCA Agent and perform the login. 3. When the “Accept/Reject” Dialog box for network usage policy shows up, right click on CCA Agent icon in tray and click “Exit” 4. Launch CCA Agent again and perform the login. The user is not shown the “Network Usage Terms & Conditions” and does by-passes the “Accept/Reject” these terms. Technically, the user never accepted the “Network Usage Terms & Conditions” and was allowed to access the network.
CSCsc89288	Yes	Client machines who have SpyBot anti spyware installed will be logged out immediately showing Invalid DMReport in the logs. (CAS patch and Agent patch required; see Enhancements for Release 3.6.0.1, page 34).

Table 22 List of Closed Caveats (continued)

	Software Release 3.6(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsc89894	Yes	Button “Verify and Install Uploaded Certificates” does not work
CSCsc91332	Yes	Spaces not stripped from username/password while creating new local user Spaces [left and right] are not stripped from username / password while creating or modifying local users. However, the [left & right] spaces are stripped from the username/password entered into the CCA agent or in the web form.
CSCsc97952	Yes	H+BEDV AntiVir/XP 6.32.x def date/version couldn't be detected
CSCsd01069	Yes	JSP execution should only be allowed in selective web directories
CSCsd03329	Yes	Import certificate does not work on CAM running in standby mode
CSCsd03955	Yes	Header file perfigo_header.jsp should display version of CCA Server Header file perfigo_header.jsp should display the CCA version information of the CAS. Currently, the version information is being displayed only on CAM running in Standalone or HA-Primary mode. CAM running in HA-Standby mode should also display the version information in top header using admin_header.jsp
CSCsd05095	Yes	Button “Update Time Zone” does not work on CAM The CAM does not return any HTTP response and does not log any entry in the tomcat access_log file.
CSCsd06458	Yes	500 Internal Server Error on changing the admin username On page Administration > Admin Users > Admin Users > List > Edit, changing the “Admin User Name” and clicking button “Save Admin” causes 500 Internal Server Error

Table 22 List of Closed Caveats (continued)

DDTS Number	Software Release 3.6(1)	
	Corrected	**Caveat**
CSCsd08348	Yes	Network/VLAN-related issues with 3.6.0 on Clean Access Servers running on machines with Broadcom NIC controllers **Note** You do not have to apply the workaround below if upgrading to 3.6(1) or above. Servers with Broadcom NIC controllers, upon upgrading to 3.6.0 or installing 3.6.0, will demonstrate issues with networks where VLAN tags are of importance. Symptoms can include failure of DHCP (because the VLAN tags are lost) or failure to route traffic appropriately. This behavior is not consistent and is due to a feature known as IPMI on the Broadcom NICs. **Workaround if not Upgrading to 3.6(1):** To alter the IPMI-asf setting on Broadcom controllers, you must download a utility from Broadcom: http://www.broadcom.com/support/ethernet_nic/driver-sla.php?driver=570x-diag. Follow the instructions on the web page to start the download. Then, follow the instructions below: 1. Save the **user_diag-8.30.zip** utility to your workstation, and unzip the file. 2. Copy the contents of the **user_diag** folder onto a bootable DOS floppy or CD-ROM. 3. Boot the machine into DOS. 4. At the DOS prompt, type: `b57udiag -cmd` Wait for a prompt to appear. It might take a while. 5. At the prompt, type: `setasf -d @` 6. After this is done, at the prompt, type: `exit` 7. Eject the CD-ROM and reboot the machine.
CSCsd17858	Yes	Agent login pops up after user assigned to quarantine role Assigned quarantine role when agent failed network scan, CAM side online user show user login as quarantine role, but Agent side login window pops up.
CSCsd20418	Yes	HA problem with both servers being active when switch is rebooted HA state of power cycled standby unit comes up as active if the switch it is connected to is down during its reboot. When the switch comes up, both CAS units are then active, and stay active.

Table 22 List of Closed Caveats (continued)

	Software Release 3.6(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsd28300	Yes	CCA Agent exits on login submission when upgraded from 3.5.11 to 3.6.0.1. If a client upgrades from the 3.5.11 to 3.6.0.0/3.6.0.l Agent, 3.6 AV support is not fully installed , and uninstalling 3.6.0.0/3.6.0.1 Agent does not fully uninstall the old 3.5 AV support. Workaround 1: Have 3.5.11 Agent clients upgrade to 3.6.**1**.0 or above Agent only. Do not upgrade 3.5.11 Agent (released 30-JAN-2006) to 3.6.0.0 or 3.6.0.1 Agent (released December 2005). Workaround 2: If the 3.5.11 Agent has already been upgraded to 3.6.0.0/3.6.0.1, you must reinstall the 3.5.11 Agent manually on the client. Then , either uninstall the 3.5.11 Agent from Add/Remove programs to fully clean the machine of the old 3.5 files, and have the client Download the new 3.6.1.0 Agent. Or, leave the 3.5.11 Agent on the client, and have the client auto-upgrade to the 3.6.1.0 Agent .
CSCsd35643	Yes	Incorrect message when using the Update button in Agent In 3.6.0.0 and 3.6.0,1, if vendor name is configured as “ANY” in the AV Definition type of requirement, for several AV products, the agent will report incorrect message saying that no product could be found when clicking on the “Update” button.

Resolved Caveats - Release 3.6.0.1

Table 23 List of Closed Caveats

	Software Release 3.6.0.1	
DDTS Number	**Corrected**	**Caveat**
CSCsc82522	Yes	Network scanner report page does not display correctly to the user, although the administrator report is displayed under Device Management > Clean Access > Network Scanner > Reports. **Note** Affects network scanning users only. Steps to reproduce: 1. Select plugins in OS:WINDOWS_ALL, 2. If those plugins are not selected in OS:ALL as well, end-users will see an empty report when they try to login Workaround: Enable the same plugins in the “ALL” OS category (and deselect “Enable scanning with selected plugins” for the “ALL” OS category, if applicable).

Table 23 List of Closed Caveats (continued)

DDTS Number	Software Release 3.6.0.1	
	Corrected	**Caveat**
CSCsc85405	Yes	Obsolete JSPs could allow DoS attack on CAM. **Note** Security patch-CSCsc85405 resolves this caveat, and the patch is included in 3.6.0.1, and 3.6(1) or above upgrade. The security patch does not need to be re-applied after upgrade to 3.6.0.1 or 3.6(1) or above. (CAM upgrade to 3.6.0.1 or above is required). The patch is required for 3.6(0), and 3.5(8) and below. For further details, see : http://www.cisco.com/en/US/products/ps6128/products_security_notice09186a00805b87a7.html
CSCsc89288	Yes	Client machines which have SpyBot anti spyware installed will be logged out immediately showing Invalid DMReport in the logs. (CAS patch and Agent patch required; see Enhancements for Release 3.6.0.1, page 34).
CSCsc89894	Yes	Button “Verify and Install Uploaded Certificates” does not work

Resolved Caveats - Release 3.6(0)

All caveats resolved for release 3.5(8) are also resolved for release 3.6(0). For additional details, see http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cca/cca35/35rn.htm#wp168744.

Known Issues for Cisco Clean Access

This section describes known issues when integrating Cisco Clean Access with the following:

- Known Issues with Broadcom NIC 5702/5703/5704 Chipsets
- Known Issue with Windows 98/ME/2000 and Windows Script 5.6

Known Issues with Switches

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

Known Issues with Broadcom NIC 5702/5703/5704 Chipsets

Customers running CCA release 3.6(2), 3.6(1), or 3.6(0) on servers with 57xx Broadcom NIC cards may be impacted by caveat CSCsd74376, page 74. 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. Versions 3.6(2), 3.6(1), 3.6(0) of the CCA software are impacted by this bug.

Solution

Note If upgrading from 3.5(x) to 3.6(3) or above and your system uses the 5702/5703/5704 Broadcom NIC chipsets, you will still need to perform step 2a. However, none of the other steps are necessary. Note that you can apply the firmware upgrade from HP before or after upgrading to CCA 3.6(3)+.

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 need to perform two steps:
   a. Apply the firmware upgrade from HP: http://h18023.www1.hp.com/support/files/networking/us/download/24056.html
   b. Upgrade to the latest CCA release (3.6(3) or above). See New and Changed Information, page 8.
3. If your machine has another 57xx Broadcom chipset, you only need to upgrade to the latest CCA release (3.6(3) or above). See New and Changed Information, page 8.

For additional history on this caveat, see also Resolved Caveats - Release 3.6.2.1, page 74 and Enhancements for Release 3.6.2.1, page 22.

For further details, see the *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 Cisco Clean Access Agent in release 3.6(x). 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 3.6(x)

If you purchased and are performing a first installation of Cisco Clean Access, use the following steps.

For New Installation:

1. If you have 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 85.
2. Follow the instructions on your welcome letter to obtain a license file for your installation. See *Cisco NAC Appliance Service Contract/Licensing Support* 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 3.6 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, download the 3.6.x.ISO from http://www.cisco.com/public/sw-center/ciscosecure/cleanaccess.shtml and burn it to 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).
6. At the admin login prompt, login with the default user name and password **`admin/cisco123`** or with the username and password you configured when you installed the Clean Access Manager.
7. In the web console, navigate to **Administration > CCA Manager > Licensing** if you need to install any additional FlexLM license files for your Clean Access Servers.
8. For detailed software installation steps and further steps for adding the Clean Access Server(s) to the Clean Access Manager and performing basic configuration, refer to the following guides:
   – *Cisco Clean Access (NAC Appliance) Manager Installation and Administration Guide, Release 3.6*
   – *Cisco Clean Access (NAC Appliance) Server Installation and Administration Guide, Release 3.6*

Note Cisco Clean Access Manager 3.6.4.4 is bundled with Cisco Clean Access Agent 3.6.5.0.

Upgrading to 3.6(x)

This section covers the following topics:

General Preparation for Upgrade

Caution Please review this section carefully before commencing any Cisco Clean Access upgrade.

- **Homogenous Clean Access Server Software Support**

  You must upgrade your Clean Access Manager and all your Clean Access Servers concurrently. The Clean Access architecture is not designed for heterogeneous support (i.e., some Clean Access Servers running 3.6 software and some running 3.5 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. 3.6.3 to 3.6.4), 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 For the 3.5 (x) to 3.6(x) migration process, allow considerably more time 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 safekeeping, it is recommended to back 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 3.5(x) database should you encounter problems during upgrade. Backing up immediately following upgrade preserves your upgraded tables and provides a baseline of your 3.6(x) 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 95.

Warning **You cannot restore a 3.5 or earlier database to a 3.6 Clean Access Manager.**

- **Software Downgrade**

  Once you have upgraded your software to 3.6, if you wish to revert to 3.5, you will need to reinstall 3.5 from the CD and recover your configuration based on the backup you performed prior to upgrading to 3.6.

OOB Switch Trunk Ports and 3.6(x) Upgrade

Because Cisco Clean Access can control switch trunk ports for OOB (starting from release 3.6(1) and above), please ensure the uplink ports for controlled switches are configured as "uncontrolled" ports before or after upgrade. This can be done in one of two ways:

- Before upgrading, change the **Default Port Profile** for the entire switch to "uncontrolled" under **Switch Management > Devices > Switches > List > Config[Switch_IP] > Default Port Profile | uncontrolled**, or
- After upgrading, change the **Profile** to "uncontrolled" for the applicable uplink ports of the switch under **Switch Management > Devices > Switches > List > Ports [Switch_IP] | Profile**

This will prevent unnecessary issues when the Default Port Profile for the switch has been configured as a managed/controlled port profile.

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

Migrating/Upgrading from 3.5(7)/3.5(8)/3.5(9)/3.5(10)/3.5(11) to 3.6(x)

This section contains the following topics:

Notes on Migration

Cisco Clean Access recommends performing new installation of the latest 3.6(x) release if you have an immediate need for a new installation or new deployment of Cisco Clean Access NAC Appliance. (See New Installation of Release 3.6(x), page 84 for details.)

If planning to migrate from release 3.5(x) to release 3.6(x), Cisco Clean Access provides a migration procedure from release 3.5(7)/3.5(8)/3.5(9)/3.5(10)/3.5(11) only. Before upgrading to 3.6(x) ED, please ensure you understand the following:

- The underlying kernel is changed with release 3.6(x) and you can only perform migration to the latest 3.6(x) release from release 3.5(7)/3.5(8)/3.5(9)/3.5(10)/3.5(11).
- **Read and review the installation or upgrade/migration procedure completely before starting. The 3.6(x) upgrade/migration process differs considerably from minor release upgrades and requires physical CD installation, in addition to an upgrade file.**
- **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 box before upgrading your production Clean Access environment, you will need to get a trial license for your test servers. For details, see "How to Obtain Evaluation Licenses" in *Cisco NAC Appliance Service Contract/Licensing Support*.

- Do not upgrade to release 3.6(x) if you are currently using Monitoring > SNMP traps from the Clean Access Manager.
- **OOB Deployments:** Because Cisco Clean Access can control switch trunk ports for OOB (starting from release 3.6(1) and above), please ensure the uplink ports for controlled switches are configured as "uncontrolled" ports either before or after upgrade. See OOB Switch Trunk Ports and 3.6(x) Upgrade, page 86 for details.
- DHCP configuration is preserved for each CAS in the configuration during upgrade.
- When migrating/upgrading between major versions, such as from 3.5(x) to 3.6(x), Clean Access Agent Setup/Patch installation files are automatically upgraded with the CAM for compatibility with the new release.
- **5702/5703/5704 Broadcom NIC chipsets**: If upgrading from 3.5(x) to 3.6(x) and your system uses 5702/5703/5704 Broadcom NIC chipsets, you will need to perform a firmware upgrade from HP. See Known Issues with Broadcom NIC 5702/5703/5704 Chipsets, page 82 for details.
- If you need further assistance, contact TAC as described in Obtaining Documentation and Submitting a Service Request, page 115.

Summary of Migration Procedure

The Cisco Clean Access 3.6 upgrade differs considerably from previous upgrades. The Cisco Clean Access 3.6 upgrade will create a complete snapshot of the configuration of your existing deployment, including failover information. This snapshot will be automatically copied to a remote server. The remote server must not be a Cisco Clean Access Server or Manager.

After the upgrade is run, you will be required to install from the provided 3.6 CDs. After this install, the snapshot created here must be copied back to the Clean Access Manager, un-tarred and the RESTORE.pl script run to restore your systems' previous configuration information.

The following is a general summary of the upgrade/migration steps:

1. For safekeeping, BACKUP your 3.5(x) Clean Access Manager using **Administration > Backup** and save the snapshot on a local computer (as described in Create CAM DB Backup Snapshot, page 95).
2. From your existing CAM, run the upgrade script to generate a backup tarball of your entire system and send the file off the CAM (by SCP (default) or FTP) to another machine. For users whose networks do not have convenient SSH servers available for SCP, the configuration snapshot can be transferred automatically via FTP to any Windows (IIS) FTP server.

Warning **The 3.6(x) upgrade script must only be run immediately prior to the CD re-install. The script assumes that the hard drive will be destroyed shortly after the upgrade script is run.**

Note For users whose networks do not have convenient SSH servers available for SCP, the configuration snapshot can be transferred automatically via FTP to any Windows (IIS) FTP server.

3. You must then perform CD-ROM install (.iso files) of release 3.6(x) on all CAM and CAS boxes.
4. After installation is complete on all boxes, copy the system backup tarball back to the CAM.
5. Untar the system backup file and execute the restore command.
6. You must then reboot each CAM and CAS machine in your system. For CAM or CAS failover (high-availability) configurations, the Primary machine must be rebooted first, then the Standby machine.
7. After reboot, your Cisco Clean Access configuration will be propagated to all your CASes and Standby machines.
8. After performing 3.5(x)-to-3.6(x) migration, the very first time you log into the 3.6(x) 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.

Migration Procedure Steps

Warning **Please make sure you have thoroughly reviewed General Preparation for Upgrade, page 85, Migrating/Upgrading from 3.5(7)/3.5(8)/3.5(9)/3.5(10)/3.5(11) to 3.6(x), page 87, before proceeding.**

The sequence of steps is described as follows:

1. Download the Upgrade File
2. Run the Upgrade File on the CAM and Perform System Backup
3. Perform CD Installation
4. Copy System Backup File Back to CAM
5. Restore System Backup File
6. Reboot All Machines

Download the Upgrade File

Step 1 Log into Cisco Downloads (http://www.cisco.com/public/sw-center/ciscosecure/cleanaccess.shtml) and click the link for Cisco Clean Access Software. On the Cisco Secure Software page for Cisco Clean Access, click the link for the appropriate 3.6 release. Download the following file to a local computer:

cca_upgrade_3.5.x-to-3.6.4.tar.gz

Step 2 Copy the file to the Clean Access Manager only using WinSCP, SSH File Transfer or PSCP, as described below.

If using WinSCP or SSH File Transfer:

a. Copy **cca_upgrade_3.5.x-to-3.6.4.tar.gz** to the /store directory on the Clean Access Manager.

If using PSCP:

a. Open a command prompt on your Windows computer.

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

c. Enter the following command to copy the file to the Clean Access Manager:

```
pscp cca_upgrade_3.5.x-to-3.6.4.tar.gz root@ipaddress_manager:/store
```

Run the Upgrade File on the CAM and Perform System Backup

Note Before running the upgrade, please document the eth0 IP addresses of your CAM and CAS (including Primary and Standby eth0 IP addresses for HA systems). These must be given during the system backup procedure, and are needed for the CD install and to SCP the backup file back to the system after the CD upgrade.

Warning **The 3.6(x) upgrade script must only be run immediately prior to the CD re-install. The script assumes that the hard drive will be destroyed shortly after the upgrade script is run.**

Step 3 Connect to the Clean Access Manager to upgrade using Putty or SSH.

a. SSH to the Clean Access Manager.

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

c. Change directory to /store:

```
cd /store
```

d. Uncompress the downloaded file:

```
tar xzvf cca_upgrade_3.5.x-to-3.6.4.tar.gz
```

7. Change directory to the upgrade folder:

```
cd cca_upgrade_3.5.x-to-3.6.4
```

Step 4 Run the upgrade file:

```
./UPGRADE-3.6.4.pl
```

Step 5 You will see the following banner:

```
./UPGRADE-3.6.4.pl
############################################################
# Welcome to Cisco Clean Access 3.6 upgrade #
############################################################
The Cisco Clean Access 3.6 upgrade.
The 3.6 upgrade is different from previous upgrades. Please
be sure to read the documentation before proceeding.
The Cisco Clean Access 3.6 upgrade will create a complete
snapshot of the configuration of your existing deployment,
including failover information. This snapshot will be auto-
matically copied to a remote server. The remote server must
not be a Cisco Clean Access server or manager.
After the upgrade is run, you will be required to install from
the provided 3.6 CDs. After this install, the snapshot created
here must be copied back to the Clean Access Manager, un-tarred
and the RESTORE.pl script run to restore your systems' previous
configuration information.
Upgrading TCL RPM
Upgrading expect RPM
It is strongly recommended that the snapshot be automatically transferred to a non-CCA
machine via SCP or FTP.
```

Step 6 At the following prompt, type **y** or press Enter:

```
Perform the transfer automatically? [y] y
```

Step 7 Type the method of transfer to send the backup file off the CAM or press Enter for the default (**scp**):

```
Transfer using SCP or FTP? [scp] scp
```

Note For users whose networks do not have convenient SSH servers available for SCP, the configuration snapshot can be transferred automatically via FTP to any Windows (IIS) FTP server.

Step 8 Type the IP address of the machine on which to save the system backup file:

```
Please enter the IP address of the destination (non-CCA) machine: 10.201.2.40
```

Step 9 Type the destination directory:

```
Please choose a directory on the destination machine that the configuration snapshot will
be placed in. A small test file will be copied into that directory to verify connectivity.
Please enter the destination directory now: /store
```

Step 10 Type the username account and password for the destination machine:

```
Please enter the username to be used for the transfer: root
What is the password for account root at 10.201.2.40?
```

Step 11 At the following prompt, type **y** or press Enter to start the system backup:

```
Backup entire system? [y] y
```

Note Typically, the entire system should be backed up. If you enter **n** (no) at this prompt, only the CAM is backed up and it is expected that you will run the upgrade/migration script on each of your individual CAS systems to back up each CAS system individually.

Step 12 This starts the backup of the first Clean Access Server. At the next prompt, type the **root** user password for the CAS and press Enter to continue:

```
Backing up Clean Access Server 10.201.200.214
Please enter the root password for Clean Access Server at 10.201.200.214:
```

Step 13 You will see a status message corresponding to the number of machines in your deployment. For failover (HA) pairs, the script will locate the Service IP first, followed by the real IP address of each machine in the failover pair. In the example deployment below, two failover CAS machines and two failover CAM machines are backed up. When finished, the `Backup complete` prompt indicates the system backup file (i.e. **cam-<cam_ip_address>-backup.tar.gz**) has been successfully created and transferred to the external machine.

```
Clean Access Server ip 10.201.200.214 is a service IP, adding real IP at 10.201.200.212
and proceeding
Backing up Clean Access Server 10.201.200.212
Located Clean Access Server peer at 10.201.200.213, adding to list
Backing up Clean Access Server 10.201.200.213
Locating Clean Access Manager standby server
Backing up Clean Access Manager at 10.201.200.211
Backing up Clean Access Manager 10.201.200.209
File "cam-10.201.200.209-backup.tar.gz" successfully transferred to 10.201.2.40:/store
Backup complete
```

Note Cisco recommends performing automatic transfer of the backup configuration file. If you do not select automatic transfer at step 6, the following warning message will appear:

```
########################
#       WARNING        #
########################

File "cam-<cam_ip_address>-backup.tar.gz" MUST be transferred safely off this machine
before the 3.6.x install is run.
Failure to do this will result in complete loss of configuration information for this
deployment.
```

Perform CD Installation

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 14 Install 3.6(x) on each CAS and CAM machine. Connect to each server machine directly or via serial connection using terminal emulation software (such as HyperTerminal or SecureCRT) and insert the 3.6(x) product CD in the CD-ROM drive. Follow the auto-run procedures.

Step 15 At the first screen 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:
```

Caution With release 3.6(x), only **one** CD is used for installation of the Clean Access Server **or** Clean Access Manager software. The installation script does **NOT** automatically detect or select CAS or CAM installation for the target server. You **MUST** select the appropriate type, **either** CAS **or** CAM, for the target machine on which you are performing installation. Do NOT select either both packages or no packages.

Step 16 Release 3.6(x) presents an additional screen prompt for selection of CCA Manager software installation or CCA Server software installation. At the following screen prompt, you must select EITHER **`CCA Manager`** or **`CCA Server`** and select **`OK`** to begin the installation. Use the space bar and the "+" and "-" keys to select the appropriate type. Use the Tab key to tab to the OK field, and press the Enter key when done to start the installation of the package type selected.

```
Welcome to Cisco Clean Access

                        ++ Package Group Selection ++
                        |                           |
                        | Total install size: 606M  |
                        |                           |
                        |    [ ] CCA Manager #      |
                        |    [ ] CCA Server  #      |
                        |                    #      |
                        |                    #      |
                        |                    #      |
                        |                    #      |
                        |                    #      |
                        |                    #      |
                        |                           |
                        |   +-----+     +-------+   |
                        |   | OK |      | Back |    |
                        |   +-----+     +-------+   |
                        |                           |
                        |                           |
                        +---------------------------+

<Space>,<+>,<-> selection   |   <F2> Group Details   |   <F12> next screen
```

Note Do not select the "Back" option from the Package Group Selection screen (known issue).

Step 17 After the CCA Manager or CCA Server type is chosen and before the prompts appear to configure the IP address of the server, a warning message may be displayed:

```
Initial RAM disk image
Turning off some packages…
Initializing JDK links...
CCA has detected a change in your network hardware configuration. Please switch the
network cables between eth0 and eth1
Press [ENTER] to continue…
```

This message is displayed when 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. 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.

Step 18 For step-by-step CD installation instructions, refer to the installation chapters of the *Cisco Clean Access (NAC Appliance) Manager Installation and Administration Guide, Release 3.6* and the *Cisco Clean Access (NAC Appliance) Server Installation and Administration Guide, Release 3.6*.

Step 19 When CD installation on all target server machines is complete, continue to the next step.

Copy System Backup File Back to CAM

Step 20 After CD installation is completed on all machines, copy the system backup file to your Primary Clean Access Manager using WinSCP, SSH File Transfer or PSCP, as described below. The name of the system backup file will reflect the name and IP address of your Clean Access Manager and will be in the form **cam-<cam_ip_address>-backup.tar.gz.**

If using WinSCP or SSH File Transfer (replace <cam_ip_address> with the actual IP of your CAM)

a. Copy **`cam-<cam_ip_address>-backup.tar.gz`** to the `/store` directory on your Primary Clean Access Manager.

If using PSCP:

a. Open a command prompt on your Windows computer.

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

c. Enter the following command to copy the file (replace <cam_ip_address> with the actual IP of your CAM) to the Clean Access Manager:

```
pscp cam-<cam_ip_address>-backup.tar.gz root@ipaddress_manager:/store
```

Restore System Backup File

Step 21 Cd to the `/store` directory on your Primary CAM or the directory in which you copied the system backup file (**cam-<cam_ip_address>-backup.tar.gz)**

Step 22 Uncompress the backup file (replace **`<cam_ip_address>`** with the actual IP of your CAM):

```
tar xzvf cam-<cam_ip_address>-backup.tar.gz
```

Step 23 Execute the RESTORE command:

```
./RESTORE.pl
```

Step 24 This starts the configuration restoration utility. The configuration information for the Primary CAM is restored first:

```
[root@cam1 store]#./RESTORE.pl
Welcome to the Clean Access 3.6 configuration restoration utility.
This utility will restore configuration information from a previous system.
Restoring Clean Access Manager 10.201.200.9
Stopping Perfigo Service
```

Step 25 At the next prompt, type **`y`** or press Enter to continue the rest of the system restore:

```
Restore the rest of the system? [y]
Restoring Clean Access Manager at 10.201.200.14
```

Step 26 At the next prompted, type the **`root`** password of the Standby CAM (for an HA deployment) and press Enter to continue the rest of the system restore:

```
Please enter the root password for Clean Access Manager at 10.201.200.14:
Done
Restoring Clean Access Server at 10.201.200.16
Restoring Clean Access Server at 10.201.200.18
Restoring Clean Access Server at 10.201.200.217
Done!
Please reboot your systems and the upgrade will be complete.
```

Reboot All Machines

Step 27 After restore is complete, you MUST reboot all server machines to complete the upgrade and restoration of the backup configuration to all machines. For failover (HA) deployments, reboot the Primary CAM or CAS first, then reboot the Standby CAS.

```
[root@cam1 store]# reboot
```

Step 28 This completes the 3.6(x) upgrade/migration.

Note **For OOB Deployments:** Because Cisco Clean Access can control switch trunk ports for OOB (starting from release 3.6(1) and above), please ensure the uplink ports for controlled switches are configured as "uncontrolled" ports either before or after upgrade. See OOB Switch Trunk Ports and 3.6(x) Upgrade, page 86 for details.

Upgrade Instructions for 3.6(x) Minor Releases and Patches

Warning **Your CAM/CAS must already be running 3.6(0) or above to perform minor release upgrades to a later 3.6(x) release. If your system is on 3.5(x), refer to the instructions in Migrating/Upgrading from 3.5(7)/3.5(8)/3.5(9)/3.5(10)/3.5(11) to 3.6(x), page 87.**

This section describes how to upgrade an existing standalone 3.6(x) system to a new minor release (e.g. 3.6(4)) or patch release (e.g. 3.6.4.4). In most cases, web upgrade is recommended for minor releases.

Note When upgrading from 3.6(x) to 3.6.4.4, you can perform **web console** upgrade of standalone 3.6(x) CAM/CAS machines if the following conditions are met:

- 3.6(x) CAM machines have already been patched for caveat CSCsg24153, page 69.
- 3.6(x) CAS machines have already been patched for caveat CSCsg24153, page 69 **and** the CAS web console password is NOT cisco123.

If the system has not already been patched, upgrade both your machines using the Upgrading via Console/SSH, page 101 procedure. For details on Patch-CSCsg24153, download the README-CSCsg24153 file from http://www.cisco.com/cgi-bin/tablebuild.pl/cca-patches.

Note **For OOB Deployments:** Because Cisco Clean Access can control switch trunk ports for OOB (starting from release 3.6(1) and above), please ensure the uplink ports for controlled switches are configured as "uncontrolled" ports either before or after upgrade. See OOB Switch Trunk Ports and 3.6(x) Upgrade, page 86 for details.

Before performing any upgrade, refer to General Preparation for Upgrade, page 85 for general information, then follow the instructions below.

- Create CAM DB Backup Snapshot
- Download the Upgrade File
- Upgrade via Web Console
- Upgrading via Console/SSH (alternate instructions if not performing web console upgrade)

For details on upgrading failover pairs, see:

- Upgrading High Availability Pairs, page 103

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 Type a name for the snapshot in the **Database Snapshot Tag Name** field.

Step 3 The field automatically populates with a name incorporating the current time and date (such as 07_20_06-14:43_snapshot). To facilitate backup file identification, it is recommended to insert the release version in the snapshot, for example, 07_20_06-14:43_**3.6.3**_snapshot. You can also either accept the default name or type another.

Step 4 Click **Create Snapshot**. The CAM generates a snapshot file, which is added to the snapshot list.

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 5 To download the snapshot to another computer, click the tag name of the snapshot to be downloaded.

Step 6 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 Clean Access 3.6 minor release upgrades, a single file, **cca_upgrade_3.6.x-to-3.6.y.tar.gz**, is downloaded to each Clean Access Manager (CAM) and Clean Access Server (CAS) installation machine. The upgrade script automatically determines whether the machine is a CAM or CAS.
For Cisco Clean Access 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/public/sw-center/ciscosecure/cleanaccess.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 (replace the .x and .y in the file name with the version number to which you are upgrading, for example, **cca_upgrade_3.6.x-to-3.6.4.4.tar.gz**):

- **cca_upgrade_3.6.x-to-3.6.y.tar.gz** (CAM/CAS release upgrade file)
- **cca-3.6.x-to-3.6.x.y-upgrade.tar.gz** (CAM/CAS patch upgrade file)
- **cam-3.6.x-to-3.6.x.y-upgrade.tar.gz** (CAM-only patch upgrade file)
- **cas-3.6.x-to-3.6.x.y-upgrade.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.

Upgrade via Web Console

Note In most cases, web upgrade is recommended for 3.6(x) minor release upgrades.

Administrators have the option of performing software upgrade on the CAS and CAM via web console:

- CAM web console: **Administration > Clean Access Manager > System Upgrade**
- CAS management pages (in CAM web console): **Device Management > CCA Servers > Manage [CAS_IP_address] > Misc**
- CAS direct web console: **https://<CAS_eth0_IP>/admin**

For web console upgrade, you will need your CAM web console **admin** user password (and, if applicable, CAS direct access console **admin** user password).

Note

- For web upgrade, you must **upgrade each CAS first, then the CAM**.
- Release 3.6(0) or above must be installed and running on your CAM/CAS(es) before you can upgrade to a later 3.6(x) release via web console.
- If upgrading failover pairs, refer to Upgrading High Availability Pairs, page 103.
- Alternatively, you can always upgrade using the instructions in Upgrading via Console/SSH, page 101.

With web upgrade, the CAM and CAS automatically perform all the upgrade tasks that are done manually for 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

Once release 3.6(x) is installed on the CAS, minor release web upgrades to the CAS can be performed via the CAS management pages as described below, or if preferred, using the instructions for Upgrade CAS from CAS Direct Access Web Console, page 98.

Step 1 Create CAM DB Backup Snapshot, page 95.

Step 2 Download the Upgrade File, page 96.

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 (replace the .x and .y in the filename with the upgrade version):

cca_upgrade_3.6.x-to-3.6.y.tar.gz (CAM/CAS release upgrade file), or

cca-3.6.x-to-3.6.x.y-upgrade.tar.gz (CAM/CAS patch upgrade file), or

cas-3.6.x-to-3.6.x.y-upgrade.tar.gz (CAS-only patch upgrade file)

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.

Note For 3.6.0.1 patch upgrade via web console only, the machine (CAS or CAM) will NOT automatically reboot. The patch upgrade should complete in 2-5 minutes.

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 97.

Step 1 Create CAM DB Backup Snapshot, page 95.

Step 2 Download the Upgrade File, page 96.

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 (replace the .x and .y in the file name with the upgrade version):

cca_upgrade_3.6.x-to-3.6.y.tar.gz (CAM/CAS release upgrade file), or

cca-3.6.x-to-3.6.x.y-upgrade.tar.gz (CAM/CAS patch upgrade file), or

cas-3.6.x-to-3.6.x.y-upgrade.tar.gz (CAS-only patch upgrade file)

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.

Note For 3.6.0.1 patch upgrade via web console only, the machine (CAS or CAM) will NOT automatically reboot. The patch upgrade should complete in 2-5 minutes.

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 CAM as described below.

Step 1 Create CAM DB Backup Snapshot, page 95.

Step 2 Download the Upgrade File, page 96.

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 (replace the .x and .y in the file name with the upgrade version):

cca_upgrade_3.6.x-to-3.6.y.tar.gz (CAM/CAS release upgrade file)

cca-3.6.x-to-3.6.x.y-upgrade.tar.gz (CAM/CAS patch upgrade file), or

cam_upgrade-3.6.x.y.tar.gz (CAM-only patch upgrade file)

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 Once the upgrade file appears in the list, click the checkbox under "**Upgrade Agent?**" to ensure the Setup and Patch installation files for the Clean Access Agent are upgraded to the latest release, (e.g. Agent 3.6.5.0 for CCA release 3.6.4.4).

Step 7 Click the **Apply** button for the upgrade file, and click **OK** in the confirmation dialog that appears. This will start the CAM upgrade in 2 minutes. After upgrade completes, the CAM automatically reboots.

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

Note For 3.6.0.1 patch upgrade via web console only, the machine (CAS or CAM) will NOT automatically reboot. The patch upgrade should complete in 2-5 minutes.

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

Step 9 Access the CAM web console again. You should now see the new version, "Cisco Clean Access Manager Version 3.6.x", 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.

Note **For OOB Deployments:** Because Cisco Clean Access can control switch trunk ports for OOB (starting from release 3.6(1) and above), please ensure the uplink ports for controlled switches are configured as "uncontrolled" ports either before or after upgrade. See OOB Switch Trunk Ports and 3.6(x) Upgrade, page 86 for details.

Upgrading via Console/SSH

Warning **Your CAM/CAS must already be running 3.6(0) or above to perform minor release upgrades to a later 3.6(x) release. If your system is on 3.5(x), refer to the instructions in Migrating/Upgrading from 3.5(7)/3.5(8)/3.5(9)/3.5(10)/3.5(11) to 3.6(x), page 87.**

In most cases, web upgrade is recommended for 3.6(x) minor release upgrades of standalone systems (as described Upgrade via Web Console, page 97). However, you can always perform SSH upgrade if necessary or if preferred.

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

Note The default username/password for SSH/console login is `root/cisco123`.

A single file, **cca_upgrade_3.6.x-to-3.6.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 Cisco Clean Access patch upgrades, the upgrade file can be for the CAM only, CAS only, or for both CAM/CAS, depending on the patch upgrade required.

Steps are as follows:

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

Download the Upgrade File and Copy to CAM/CAS

Step 1 Create CAM DB Backup Snapshot, page 95.

Step 2 Download the Upgrade File, page 96.

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 (replace the .x and .y in the file name with the upgrade version number)

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

a. Copy **cca_upgrade_3.6.x-to-3.6.y.tar.gz** to the /store directory on the Clean Access Manager.

b. Copy **cca_upgrade_3.6.x-to-3.6.y.tar.gz** to the /store directory on **each** Clean Access Server.

If using PSCP (replace .y 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 minor upgrade version number) to the CAM:

```
pscp cca_upgrade_3.6.x-to-3.6.y.tar.gz root@ipaddress_manager:/store
```

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

```
pscp cca_upgrade_3.6.x-to-3.6.y.tar.gz root@ipaddress_server:/store
```

Perform SSH Upgrade on the CAM

Step 4 Connect to the Clean Access Manager to upgrade using Putty or SSH.

a. SSH 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 .y with upgrade version number):

```
tar xzvf cca_upgrade_3.6.x-to-3.6.y.tar.gz
```

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

```
cd cca_upgrade_3.6.x-to-3.6.y
sh ./UPGRADE.sh
```

Note When upgrading the CAM from a 3.6(x) release to 3.6(3) and above, the script provides an additional prompt to choose whether or not to upgrade the Clean Access Agent files inside the CAM. Choosing **Yes** upgrades the Agent Setup Installation and Patch Installation files to the latest Agent version bundled with the release (for example, Agent 3.6.5.0 for release 3.6.4.4). Choosing **No** leaves the original Agent Setup and Patch Installation files that were on your CAM prior to upgrade.

5. At the following prompt enter **Y** to upgrade the Agent on your CAM to the version bundled with the CCA release, or enter **N** to keep the version of the Agent currently on your CAM.

```
Upgrade CCA Agent version to 3.6.x.x? (y/n)? [y]
```

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

```
reboot
```

Perform SSH Upgrade on the CAS

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

a. SSH 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 .y with upgrade version number):

```
tar xzvf cca_upgrade_3.6.x-to-3.6.y.tar.gz
```

6. Execute the upgrade process (replace .y with upgrade version number):

```
cd cca_upgrade_3.6.x-to-3.6.y
sh ./UPGRADE.sh
```

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

```
reboot
```

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

Note **For OOB Deployments:** Because Cisco Clean Access can control switch trunk ports for OOB (starting from release 3.6(1) and above), please ensure the uplink ports for controlled switches are configured as "uncontrolled" ports either before or after upgrade. See OOB Switch Trunk Ports and 3.6(x) Upgrade, page 86 for details.

Upgrading High Availability Pairs

Warning **Your CAM/CAS must already be running 3.6(0) or above to perform minor release upgrades to a later 3.6(x) release. If your system is on 3.5(x), refer to the instructions in Migrating/Upgrading from 3.5(7)/3.5(8)/3.5(9)/3.5(10)/3.5(11) to 3.6(x), page 87.**

This section describes the following:

- Accessing Web Consoles for High Availability
- Instructions for Upgrading High Availability CAM and CAS

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

Accessing Web Consoles for High Availability

CAM High Availability (failover) is configured in the CAM web console under **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-Standby** when you initially set up HA.

CAS High Availability (failover) is configured in the CAS direct access web console under **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-Standby-Mode** when you initially set up HA.

Determining Active and Standby Clean Access Manager

For a Clean Access Manager High-Availability pair:

- Access the Primary CAM by opening the web console for the Primary's IP address.
- Access the Secondary CAM by opening the web console for the Secondary's IP address.

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 Active and Standby Clean Access Server

For a Clean Access Server High-Availability pair:

- Access the primary CAS by opening the CAS direct access web console for the trusted-side (eth0) IP address of the primary CAS, as follows: **https://<primary CAS (eth0)IP>/admin**

  For example, `https://172.16.1.2/admin`

- Access the secondary CAS by opening CAS direct access web console for the trusted-side (eth0) IP address of the secondary CAS, as follows: **https://<secondary CAS (eth0)IP>/admin**

  For example, `https://172.16.1.3/admin`

For failover CAS pairs, **Device Management > CCA Servers > List of Servers** in the CAM web console displays the Service IP of the CAS pair first, followed by the IP address of the active CAS in brackets. When the 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.

Instructions for Upgrading High Availability CAM and CAS

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

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

Note For serial cable connection for HA, the serial cable must be a "null modem" cable. For details, refer to http://www.nullmodem.com/NullModem.htm.

Step 1 SSH into each machine in the failover pair. Login as the **`root`** user with the root password (default is **`cisco123`**)

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 101 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 and .y in the file name with the upgrade version number):

```
tar xzvf cca_upgrade_3.6.x-to-3.6.y.tar.gz
```

b. CD into the created "cca_upgrade_3.6.x-to-3.6.y" 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 always determine which box is active or standby by accessing the web console as described in Accessing Web Consoles for High Availability, page 103.

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

```
shutdown -h now
```

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

Step 6 CD into the created "cca_upgrade_3.6.x-to-3.6.y" directory on the active box.

```
cd cca_upgrade_3.6.x-to-3.6.y
```

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_3.6.x-to-3.6.y"), run the upgrade script on the active box:

```
./UPGRADE.sh
```

Note When upgrading the CAM from a 3.6(x) release to 3.6(3) and above, the script provides an additional prompt to choose whether or not to upgrade the Clean Access Agent files inside the CAM. Choosing `Yes` upgrades the Agent Setup Installation and Patch Installation files to the latest Agent version bundled with the release (for example, Agent 3.6.5.0 for release 3.6.4.4). Choosing `No` leaves the original Agent Setup and Patch Installation files that were on your CAM prior to upgrade.

Caution For HA-CAM upgrade, make sure to use the **same** upgrade option for the CCA Agent on **both** the HA-Primary and HA-Standby CAM.

7. At the following prompt enter `Y` to upgrade the Agent on your active CAM to the version bundled with the CCA release, or enter **N** to keep the current version of the Agent.

```
Upgrade CCA Agent version to 3.6.x.x? (y/n)? [y]
```

Step 9 After the upgrade is completed, shut down the active box by entering the following command via the 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_3.6.x-to-3.6.y
```

c. Run the upgrade script on the standby box:

```
./UPGRADE.sh
```

Caution For HA-CAM upgrade from a 3.6(x) release to 3.6(3) and above, make sure to use the **same** upgrade option for the CCA Agent on **both** the HA-Primary and HA-Standby CAM.

8. At the following prompt enter **`y`** to upgrade the Agent on the standby CAM to the version bundled with the CCA release, or enter **N** to keep the version of the Agent.

```
Upgrade CCA Agent version to 3.6.x.x? (y/n)? [y]
```

Step 13 Shut down the standby box by entering the following command via the 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.

Note **For OOB Deployments:** Because Cisco Clean Access can control switch trunk ports for OOB (starting from release 3.6(1) and above), please ensure the uplink ports for controlled switches are configured as "uncontrolled" ports either before or after upgrade. See OOB Switch Trunk Ports and 3.6(x) Upgrade, page 86 for details.

Troubleshooting

This section discusses the following:

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

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.

Creating CAM DB Snapshot

See the instructions in Create CAM DB Backup Snapshot, page 95 for details.

Downloading 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

- With release 3.6(2) and above, CAS-specific support logs are obtained from the CAS direct console only.
- For releases 3.6(0)/3.6(1) and 3.5(3) and above, 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.

See also Support Log and Log Level Enhancements, page 24 for additional details.

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

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

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

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

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

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

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

Recovering Root Password for CAM/CAS (Release 3.5.x or Below)

To recover the root password for CAM/CAS on release 3.5(x), you can use the Linux procedure to boot to single user mode and change the root password:

1. Connect to the CAM/CAS machine via console.
2. Power cycle the machine.
3. After power-cycling, the GUI mode displays. Press Ctrl-x to switch to text mode. This displays a "boot:" prompt.
4. At the prompt type: **`linux single`**. This boots the machine into single user mode.
5. Type: **`passwd`**.
6. Change the password.
7. Reboot the machine using the **`reboot`** command.

Agent AV/AS Rule Troubleshooting

To view administrator reports for the Clean Access Agent go to **Device Management > Clean Access > Clean Access Agent > Reports**. To view information from the client right-click the Agent taskbar icon and select **About** for the Agent version and **Properties** for AV/AS version.

When troubleshooting AV/AS Rules, please provide the following information:

1. Version of CAS, CAM, and Clean Access Agent.

2. Client OS version (e.g. Windows XP SP2)
3. Name and version of AV/AS vendor product.
4. What is failing—AV/AS installation check or AV/AS update checks? What is the error message?
5. What is the current value of the AV/AS def date/version on the failing client machine?
6. 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**)

Enable Debug Logging on the Clean Access Agent

Note For the 3.6.1.0 and above Agent:

- The registry key path changes from HKEY_LOCAL_MACHINE\Software\Cisco\Clean Access Agent\ to HKEY_CURRENT_USER\Software\Cisco\Clean Access Agent\.
- The event.log path changes from the installation directory (e.g. C:\Program Files\Cisco Systems\Clean Access Agent\event.log) to the user's home directory (e.g. C:\Documents and Settings\<username>\Application Data\CiscoCAA\event.log)

You can enable debug logging on the Clean Access Agent by adding a registry value on the client in HKCU\Software\Cisco\Clean Access Agent\LogLevel with value "debug."

The event log will be created in the directory <user home directory>\ Application Data\CiscoCAA\. You can copy this event log to include it in a customer support case.

To generate the Clean Access Agent debug log:

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

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`**.
5. Right-click **LogLevel** and select Modify. The **Edit String** dialog appears.
6. Type **`debug`** in the **Value data** field and click **OK** (this sets the value of the LogLevel string to "debug").
7. Restart the Clean Access Agent by double-clicking the desktop shortcut.
8. Re-login to the Clean Access Agent.
9. When a requirement fails, click the **Cancel** button in the Clean Access Agent.
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.

11. 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\.

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 24 Updates to Release Notes for Cisco Clean Access (NAC Appliance) Version 3.6(x)

Date	Description
4/16/08	• Enhancements for Release 3.6.4.4, page 9 (updated) • Resolved Caveats - Release 3.6.4.4, page 67 addresses a Cisco PSIRT issue involving caveat CSCsj33976 (new) • Updated trademarks (version 0804R)
4/1/08	Release 3.6.4.4: • Cisco Clean Access (NAC Appliance) Releases, page 2 (updated) • Release 3.6(x) Compatibility Matrix, page 4 (updated) • Release 3.6(x) CAM/CAS Upgrade Compatibility Matrix, page 5 (updated) • Enhancements for Release 3.6.4.4, page 9 (new) General: • Updated hypertext links to cisco.com documents throughout • Replaced “Obtaining Documentation” section with boilerplate Obtaining Documentation and Submitting a Service Request, page 115 text inset
1/30/08	Applied new template and updated trademark information
6/28/07	Added caveat CSCsd90433 to Open Caveats - Release 3.6.4.4, page 65
3/19/07	Moved Caveat CSCsi07595 to Open Caveats - Release 3.6.4.4, page 65.
3/9/07	Added Caveat CSCsi07595 to address the DST 2007 fix.
1/22/07	Updates for release 3.6.4.3: • Updated Software Compatibility Matrixes, page 4 • Added Enhancements for Release 3.6.4.3, page 10 • Updated Clean Access Agent Version Summary, page 63 • Updated all charts under Clean Access Supported AV/AS Product List, page 43 • Updated Open Caveats - Release 3.6.4.4, page 65 • Added Resolved Caveats - Release 3.6.4.3, page 68 • Updated template and boilerplate; Updated hypertext URLs for Cisco NAC Appliance installation and compatibility guides
9/19/06	• Added CSCsg07369 to Open Caveats - Release 3.6.4.4, page 65 • Updated URL for Troubleshooting, page 107.

Table 24 Updates to Release Notes for Cisco Clean Access (NAC Appliance) Version 3.6(x)

Date	Description
9/18/06	Updates for release 3.6.4.2: • Updated Software Compatibility Matrixes, page 4 • Added Enhancements for Release 3.6.4.2, page 13 • Updated Open Caveats - Release 3.6.4.4, page 65 • Added Resolved Caveats - Release 3.6.4.2, page 70 Also: • Updated VPN Components Supported for Single Sign-On (SSO), page 3 • Updated 3.6(4) feature list with Support for "Ignore" Global Device Filter for IP Phones in OOB Deployments, page 16 • Updated Troubleshooting, page 107 section.
8/24/06	Added root password recovery procedures to Troubleshooting, page 107.
8/18/06	Updated general Cisco support boilerplate.
8/4/06	Updates for release 3.6.4.1 • Updated Software Compatibility Matrixes, page 4 • Added Enhancements for Release 3.6.4.1, page 15 • Updated Open Caveats - Release 3.6.4.4, page 65 • Added Resolved Caveats - Release 3.6.4.1, page 71 • Updated Upgrading to 3.6(x), page 85 Also, reorganized links under System and Hardware Requirements, page 2.
8/2/06	Updates for release 3.6(4): • Updated Software Compatibility Matrixes, page 4 • Updated Web Browser Compatibility, page 7 • Updated all switch support information to point to *Switch Support for Cisco NAC Appliance*. • Added Enhancements for Release 3.6(4), page 16 • Updated Clean Access Supported AV/AS Product List, page 43 • Updated Clean Access Agent Version Summary, page 63 • Updated Open Caveats - Release 3.6.4.4, page 65 • Added Resolved Caveats - Release 3.6(4), page 71 • Updated Known Issues with Broadcom NIC 5702/5703/5704 Chipsets, page 82 • Updated Upgrading to 3.6(x), page 85 • Updated Troubleshooting, page 107
7/14/06	Moved CSCse53459 to Open Caveats table for 3.6(3)

Table 24 Updates to Release Notes for Cisco Clean Access (NAC Appliance) Version 3.6(x)

Date	Description
7/12/06	Updates for release of 3.6.3.1Agent (7/12/06): • Updated Software Compatibility Matrixes, page 4 • Added Clean Access Agent Enhancements (3.6.3.1), page 19 • Updated Clean Access Agent Version Summary, page 63 • Updated Resolved Caveats - Release 3.6(3), page 73 (CSCse72371, CSCse72384,CSCse72396, and CSCse53459)
6/27/06	Supported Switches for Cisco NAC Appliance, page 3 - updates for 4000/4500 and 6000/6500
6/22/06	• Updated Clean Access Supported AV/AS Product List, page 43 summary • Added CSCse60519 to Table 11 on page 65
6/21/06	3.6.(3) Release • Updated Supported Switches for Cisco NAC Appliance, page 3 • Updated Software Compatibility, page 4 • Updated Web Browser Compatibility, page 7 • Added Enhancements for Release 3.6(3), page 17 • Updated charts for Clean Access Supported AV/AS Product List, page 43 • Updated Clean Access Agent Version Summary, page 63 • Updated Open Caveats - Release 3.6.4.4, page 65 • Added Resolved Caveats - Release 3.6(3), page 73 • Added note to Known Issues with Broadcom NIC 5702/5703/5704 Chipsets, page 82 • Updated Upgrading to 3.6(x), page 85 • Updated Troubleshooting, page 107
3/29/06	3.6.2.2 Release
3/24/06	3.6.2.1 Release
3/20/06	3.6(2) Release
2/21/06	3.6.1.1 Release
2/15/06	3.6(1) Release
12/30/05	3.6.0.1 Release
12/9/05	3.6(0) Release

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 Clean Access (NAC Appliance) Manager Installation and Administration Guide, Release 3.6*
- *Cisco Clean Access (NAC Appliance) Server Installation and Administration Guide, Release 3.6*
- *Release Notes for Cisco Clean Access (NAC Appliance) Version 3.6(x)*
- *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)*
- *Switch Support for Cisco NAC Appliance*
- *Cisco NAC Appliance Service Contract / Licensing Support*

Obtaining Documentation and Submitting a Service Request

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

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

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

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