Release Notes for Cisco Clean Access Version 3.5(11)

Revised: January 4, 2008, OL-7564-01

Contents

These release notes provide cumulative late-breaking and release information for Cisco® Clean Access (CCA), release 3.5(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 Releases

Cisco Clean Access Release	Availability
3.5.11.1 GD	January 19, 2007
3.5(11) GD	June 26, 2006
3.5(10) GD	March 7, 2006
3.5(9) GD	January 30, 2006
3.5(8) GD	November 29, 2005
3.5(7) ED	October 27, 2005
3.5.6.1 ED	October 12, 2005
3.5(6) ED	September 28, 2005
3.5.5.1 ED	October 12, 2005
3.5(5) ED	August 31, 2005
3.5.4.1 ED	September 6, 2005
3.5(4) ED	August 10, 2005
3.5.3.2 ED	September 6, 2005
3.5.3.1 ED	July 27, 2005
3.5(3) ED	July 20, 2005
3.5.2.2 ED	September 6, 2005
3.5.2.1 ED	June 15, 2005
3.5(2) ED	June 2, 2005
3.5(1)ED	May 20, 2005
3.5(0) ED	April 14, 2005

Cisco NAC Appliance Service Contract/Licensing Support

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

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

System and Hardware Requirements

This section describes the following:

- Hardware Supported
- VPN Components Supported for Single Sign-On
- Supported Switches for Cisco Clean Access

Hardware Supported

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

- Supported server hardware configurations
- Custom installation instructions
- Clean Access Manager System Requirements
- Clean Access Server System Requirements
- Clean Access Agent System Requirements

VPN Components Supported for Single Sign-On

Table 1 lists VPN components supported for SSO with Cisco Clean Access. Elements in the same row are compatible with each other.

Table 1 VPN Concentrators/Clients Supported By Cisco® Clean Access 3.5(3) (and above)

Cisco Clean Access Version	VPN Concentrator/Wireless Controller	VPN Clients

3.5(11)
3.5(10)
3.5(9)
3.5(8)
	Cisco Airespace Wireless LAN Controllers	• Cisco SSL VPN Client (Full Tunnel)
		• Cisco VPN Client (IPSec)

3.5(11)
3.5(10)
3.5(9)
3.5(8)
3.5(7)
3.5.6.1
3.5(6)
3.5.5.1
3.5(5)
3.5.4.1
3.5(4)
3.5.3.2
3.5.3.1
3.5(3)
	Cisco ASA 5500 Series Adaptive Security Appliances	

	Cisco VPN 3000 Series Concentrators, Release 4.7	

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

For further details, see:

- Multi-Hop L3 In-Band Deployment Support, page 34
- VPN Integration and Single Sign-On (SSO), page 35
- VPN/L3 Access for Clean Access Agent (3.5.3+), page 56

Supported Switches for Cisco Clean Access

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

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 Agent Enhancements, page 52
- Clean Access Supported Antivirus Product List, page 64

Software Compatibility Matrixes

This section describes the following:

- Release 3.5(x) Upgrade Compatibility Matrix
- Release 3.5(x) Compatibility Matrix
- Clean Access Agent Feature Compatibility Matrix

Release 3.5(x) Upgrade Compatibility Matrix

Table 2, "Release 3.5(x) Upgrade Compatibility Matrix" shows 3.5 upgrade compatibility. You can upgrade from the release(s) shown to the latest 3.5 release.

Table 2 Release 3.5(x) Upgrade Compatibility Matrix

Clean Access Manager		Clean Access Server		Clean Access Agent	
Upgrade From:	**To:**	**Upgrade From:**	**To:**	**Upgrade From:**	**To:**

3.5(11)
3.5(10)[1]
3.5(9)
3.5(8)
3.5(7)
3.5.6.1
3.5(6)
3.5.5.1
3.5(5)
3.5(4)
3.5.3.1
3.5(3)
3.5.2.1[2]
3.5(2)
3.5(1)
3.5(0)
	3.5.11.1[3]	3.5(11)
		3.5(10)[1]
		3.5(9)
		3.5(8)
		3.5(7)
		3.5.6.1
		3.5(6)
		3.5.5.1
		3.5(5)
		3.5.4.1[4]
		3.5(4)
		3.5.3.2[4]
		3.5.3.1
		3.5(3)
		3.5.2.2[4]
		3.5(2)
		3.5(1)
		3.5(0)
			3.5.11.1[3]	3.5.12[5,7,8,9,10]
				3.5.11[6,7,8,9]
				3.5.10[7,8,9,10]
				3.5.9[7,8,9,10]
				3.5.8[7,8,9,10]
				3.5.7[7,8,9,10]
				3.5.6[7,8,9,10]
				3.5.5[8,9]
				3.5.4[8,9]
				3.5.3[8,9]
				3.5.2[9]
				3.5.1[9]
				3.5.0[11,12]
					3.5.13[7,8,9,10]

3.4(x)
3.3(x)
3.2(6)
		3.4(x)
		3.3(x)
		3.2(6)
				3.4.1[12,13]
				3.4.0[12,13]
				3.3.0[12,13,14]
				3.2.3[12,13,14]
				3.2.2[12,13,14]	

1. If planning to migrate to CCA 3.6(x), you can migrate from release 3.5(10) only to release 3.6(2) or above.
2. Upgrade to 3.5.2.1 patch is only performed on the CAM. Version 3.5.2.1 is compatible with release 3.5(2) on the CAS.
3. 3.5.11.1 patch can only be applied to 3.5(x) CAM/CAS. See Enhancements for Release 3.5.11.1, page 10 and Resolved Caveats - Release 3.5.11.1, page 78 for details.
4. Upgrade to 3.5.4.1/3.5.3.2/3.5.2.2 patch is only performed on the CAS.
5. If planning to migrate to CCA 3.6(x), upgrade the 3.5.12 Agent directly to 3.6.2.0 or above Agent.
6. If planning to migrate to CCA 3.6(x), upgrade the 3.5.11 Agent directly to 3.6.1.0 or above Agent.
7. 3.5.5+ Agents only support multi-hop L3 operation starting with 3.5(5) CAM/CAS. L3 discovery will not work with prior CAM/CAS versions.
8. Only 3.5(3) and above CAM/CAS/Agent support VPN/L3 access. Agent must be installed from CAS (via Download CCA Agent or Auto-Upgrade). See VPN/L3 Access for Clean Access Agent (3.5.3+), page 56.
9. Only 3.5.1+ Agents support Agent Auto-Upgrade. See Clean Access Agent Auto-Upgrade (3.5.1+), page 57 for details.
10. 3.5.6+ Agents are only compatible with 3.5(5) or greater CAM/CAS, or 3.5.2.2 / 3.5.3.2/ 3.5.4.1 patches of the CAS. See Web Browser Compatibility for details.
11. 3.5.0 Agent supports Supported Antivirus Product List, but does not support "ANY" vendor/product AV rules/requirements.
12. 3.5.0 and below Agents do not support Agent Auto-Upgrade.
13. 3.4.1 Agent and below do not support AV Rule integration features nor the Supported Antivirus Product List.
14. 3.3.0 Agent and below do not support network policy URL page and 3.3 clients will not work if CAM/CAS have it enabled.

Caution You cannot upgrade to 3.5 directly from 3.1. In this case, upgrade from 3.1 to 3.2.6 then upgrade to 3.5.

Release 3.5(x) Compatibility Matrix

Table 3, "Release 3.5(x) Compatibility Matrix" shows release 3.5.x CAM/CAS/Agent compatibility for the latest version of the Clean Access Agent (3.5.6 and above). Releases listed in the same row are compatible with one another. Cisco recommends synchronizing your software images to match the latest shown as compatible in the table

Table 3 Release 3.5(x) Compatibility Matrix

Clean Access Manager	Clean Access Server	Clean Access Agent
3.5.11.1 GD	3.5.11.1 GD	3.5.13
3.5(11) GD	3.5(11) GD	
3.5(10) GD	3.5(10) GD	
3.5(9) GD	3.5(9) GD	
3.5(8) GD	3.5(8) GD	
3.5(7) ED	3.5(7) ED	
3.5.6.1 ED	3.5.6.1 ED	
3.5(6) ED	3.5(6) ED	
3.5.5.1 ED	3.5.5.1 ED	
3.5(5) ED	3.5(5) ED	
3.5(4) ED	3.5.4.1 ED	
3.5.3.1 ED 3.5(3) ED	3.5.3.2 ED	
3.5.2.1 ED 3.5(2) ED	3.5.2.2 ED	

Clean Access Agent Feature Compatibility Matrix

Table 2, "Agent Compatibility Matrix" shows general feature compatibility of Agent versions for release 3.5.

Table 4 Agent Compatibility Matrix

Clean Access Manager	Clean Access Server	Clean Access Agent
3.5(x) GD	3.5(x) GD	3.5.13 [3,4,5,6] 3.5.12 [1,3,4,5,6] 3.5.11 [2,3,4,5,6] 3.5.10 [3,4,5,6] 3.5.9 [3,4,5,6] 3.5.8 [3,4,5,6] 3.5.7 [3,4,5,6] 3.5.6 [3,4,5,6] 3.5.5 [5,6] 3.5.4 [5,6] 3.5.3 [5,6] 3.5.2 [6] 3.5.1 [6] 3.5.0 [7,8] 3.4.1 [8,9] 3.4.0 [8,9] 3.3.0 [8,9,10]

[1] If planning to migrate to CCA 3.6(x), upgrade the 3.5.12 Agent directly to 3.6.2.0 or above Agent.

[2] If planning to migrate to CCA 3.6(x), upgrade the 3.5.11 Agent directly to 3.6.1.0 or above Agent.

[3] 3.5.6+ Agents are only compatible with 3.5(5) or greater CAM/CAS, or 3.5.2.2 / 3.5.3.2/ 3.5.4.1 patches of the CAS. See Web Browser Compatibility for details.

[4] 3.5.5+ Agents only support multi-hop L3 operation starting with 3.5(5) CAM/CAS. L3 discovery will not work with prior CAM/CAS versions.

[5] Only 3.5(3) and above CAM/CAS/Agent support VPN/L3 access. Agent must be installed from CAS (via Download CCA Agent or Auto-Upgrade). See VPN/L3 Access for Clean Access Agent (3.5.3+), page 56.

[6] Only 3.5.1+ Agents support Agent Auto-Upgrade. See Clean Access Agent Auto-Upgrade (3.5.1+), page 57 for details.

[7] 3.5.0 Agent supports Supported Antivirus Product List, but does not support "ANY" vendor/product AV rules/requirements.

[8] 3.5.0 and below Agents do not support Agent Auto-Upgrade.

[9] 3.4.1 Agent and below do not support AV Rule integration features nor the Supported Antivirus Product List.

[10] 3.3.0 Agent does not support network policy URL accept page and 3.3 clients will not work if CAM/CAS have it enabled.

Web Browser Compatibility

- The 3.5(x) Clean Access Manager web admin console supports the Internet Explorer 6.0 browser.
- The CAM web console requires high encryption (64 or 128 bit) and does not accept 56-bit encryption (release 3.5(7) and above)
- High encryption is also required for client browsers for web login and Agent authentication (release 3.5(7) and above).
- Release 3.5(x) does not support IE 7.0.

Note Cisco NAC Appliance does not support beta versions of third-party software.

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** (3.5.1 and above)
- 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**.

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 Agent Enhancements, page 52 and Clean Access Supported Antivirus Product List, page 64.

Enhancements for Release 3.5.11.1

Release 3.5.11.1 is a general and important bug fix release for the Clean Access Manager and Clean Access Server that resolves the caveats listed in Resolved Caveats - Release 3.5.11.1, page 78. No new features are added.

Note

- Release 3.5.11.1 is an upgrade-only patch applied to the CAM and CAS, and is a mandatory upgrade for 3.5(x) systems.
- Your CAM/CAS must already be running 3.5(x) to apply the 3.5.11.1 patch upgrade. CD installation is not supported. If running 3.4(x) or below, you must upgrade to 3.5(x) first before you can apply the 3.5.11.1 patch.

For additional details refer to the following sections:

- Upgrade Instructions for 3.5.11.1
- Resolved Caveats - Release 3.5.11.1, page 78
- Web Browser Compatibility, page 8

Upgrade Instructions for 3.5.11.1

To upgrade your CAM/CAS to 3.5.11.1, perform the following steps.

Step 1 Download the **cca_upgrade_3.5.x.tar.gz** upgrade file to your local computer from the http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.5.11 folder.

Step 2 Upgrade your 3.5(x) Clean Access Manager and Clean Access Servers using the instructions in Installing or Upgrading to a New Software Release, page 97.

Step 3 If upgrading high-availability (failover) CAM or CAS pairs, refer to Upgrading High Availability Pairs, page 107

Enhancements for Release 3.5(11)

Release 3.5(11) is a general and important bug fix release for the Clean Access Manager and Clean Access Server, which also includes the following enhancements:

- New “service perfigo maintenance” CLI Command for CAS
- Clean Access Agent
- Supported AV Product List (Version 42)

See Resolved Caveats - Release 3.5(11), page 79 for caveats that are resolved with this release.

See Installing or Upgrading to a New Software Release, page 97 for upgrade instructions.

New "service perfigo maintenance" CLI Command for CAS

Release 3.5(11) 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

The version of the Clean Access Agent remains at 3.5.13 for Cisco Clean Access release 3.5(11) See Clean Access Agent Enhancements (3.5.13), page 12.

See Supported AV Product List Versions, page 72 and Enhancements per Agent Version, page 52 for additional details.

Supported AV Product List (Version 42)

- See Supported AV Product List Versions, page 72 for details on each version of the list.
- See Clean Access Supported Antivirus Product List, page 64 for the Supported AV Product List as of the latest release.

Enhancements for Release 3.5(10)

Release 3.5(10) is a general and important bug fix release for the Clean Access Manager and Clean Access Server, and which adds AV support for the Clean Access Agent:

- Upgrade Enhancements, page 11
- CAS HA (Failover) UI Enhancements, page 12
- CAS IP Page UI Enhancement, page 12
- Supported AV Product List (Version 31), page 12
- Clean Access Agent Enhancements (3.5.13), page 12
- Clean Access Agent Enhancements (3.5.12), page 12

See also Resolved Caveats - Release 3.5(10), page 80.

Upgrade Enhancements

With SSH upgrade to release 3.5(10) and above, when upgrading the CAM, the 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 3.5.12 for release 3.5(10)). 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 105 for details.

Note Once release 3.5(10) is installed on the CAM/CAS, an "Upgrade Agent" checkbox option will be displayed on the CAM/CAS web consoles when performing web upgrade to a future release.

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**

Supported AV Product List (Version 31)

- See Supported AV Product List Versions, page 72 for details on each version of the list.
- See Clean Access Supported Antivirus Product List, page 64 for the Supported AV Product List as of the latest release.

Clean Access Agent Enhancements (3.5.13)

Version 3.5.13 of the Clean Access Agent resolves caveat CSCsd84272, page 80. See also Supported AV Product List Versions, page 72 and Enhancements per Agent Version, page 52 for details.

Clean Access Agent Enhancements (3.5.12)

Version 3.5.12 of the Clean Access Agent provides additional AV product support (Windows XP/2000). See Supported AV Product List Versions, page 72 for details.

See also Enhancements per Agent Version, page 52.

Note If planning to migrate to CCA release 3.6(x), you can upgrade the 3.5.12 Agent directly to 3.6.2.0 or above Agent only.

Enhancements for Release 3.5(9)

This section details enhancements to existing features delivered with release 3.5(9) of the Cisco Clean Access Manager and Cisco Clean Access Server.

- OOB Port Profile Page Enhancement

- Supported AV Product List (Version 26)
- Clean Access Agent Enhancements (3.5.11)

See also Resolved Caveats - Release 3.5(9), page 80.

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**

Supported AV Product List (Version 26)

- See Supported AV Product List Versions, page 72 for details on each version of the list.
- See Clean Access Supported Antivirus Product List, page 64 for the Supported AV Product List as of the latest release.

Note For 3.5(x), if you have auto-updates enabled on your CAM, and have downloaded Version 26 of the Supported AV List prior to downloading version 3.5.11 of the CCA Agent Upgrade Patch, make sure to perform a **Clean Update** to enable the latest product support for the 3.5.11 Agent.

Clean Access Agent Enhancements (3.5.11)

Version 3.5.11 of the Clean Access Agent provides the following enhancements:

- Additional AV product support (Windows XP/2000). See Supported AV Product List Versions, page 72 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 Clean Access 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 112 for details.

See also Enhancements per Agent Version, page 52, and Resolved Caveats - Release 3.5(9), page 80.

Known Issue for Symantec/Norton Products (3.5.11)

When AV definition updates are performed from the 3.5.11 Clean Access Agent, Symantec/Norton Products will launch their own update UI to perform the update, instead of performing the update behind the scenes as in previous versions of the Agent. When the Symantec/Norton Product UI is launched and is updating, any more clicks on the Update button of the CCA Agent will create a considerable load on the machine to launch more windows and cause the update process to fail. With a higher number of clicks, this can also cause the updater to fail. Cisco advises waiting until the Symantec/Norton UI launched completes its update and closes on its own.

Enhancements for Release 3.5(8)

This section details enhancements to existing features delivered with release 3.5(8) of the Cisco Clean Access Manager and Cisco Clean Access Server.

- API Enhancements
- Support for Single Sign-on (SSO) with Cisco Airespace Wireless LAN Controller
- Cisco Clean Access OOB Support for Catalyst 4000
- Clean Access Agent Enhancements (3.5.10)
- Supported AV Product List

See also Resolved Caveats - Release 3.5(8), page 82.

API Enhancements

With release 3.5(8), the Cisco Clean Access API utility script, cisco_api.jsp, provides three new functions that will allow administrators to create, delete, and view local user accounts on the CAM (local users are those internally validated by the CAM as opposed to an external authentication server):

- getlocaluserlist —Returns a list of local users with user name and role name.
- addlocaluser —Takes user name, password, and role name. Returns success or failure.
- deletelocaluser—Takes user name or "ALL" (to delete entire list). Returns success or failure.

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**.

These APIs are intended to support guest access for dynamic token user access generation, providing the ability to:

- Use a webpage to access Cisco Clean Access API to insert a visitor username/password (for example, jdoe@visitor.com, jdoe112805), and assign a role (for example, guest1day).
- Delete all guest users associated with that role for that day (for example, guest1day)
- List all usernames associated with that role (for example, all users for guest1day)

These APIs will support most implementations of guest user access dynamic token/password generation and allow the removal of those users for a guest role.

Note You will still need to create the front end generation password/token. For accounting purposes, Cisco Clean Access provides RADIUS accounting functionality only.

Support for Single Sign-on (SSO) with Cisco Airespace Wireless LAN Controller

Cisco Clean Access release 3.5(8) extends RADIUS Accounting support for Single Sign-On (SSO) to include the Cisco Airespace Wireless LAN Controller. The Clean Access Server can acquire the client's IP address from either Calling_Station_ID or Framed_IP_address RADIUS attributes for SSO purposes.

For SSO to work with Cisco Clean Access, the Cisco Airespace Wireless LAN Controller must send the Calling_Station_IP attribute as the client's IP address (as opposed to the Framed_IP_address attribute that the VPN concentrator uses).

Cisco Clean Access OOB Support for Catalyst 4000

Release 3.5(8) adds out-of-band switch management support for the Cisco Catalyst 4000.

Clean Access Agent Enhancements (3.5.10)

Version 3.5.10 of the Clean Access Agent resolves caveats CSCsc44051 (antivirus) and CSCsc44335 (uninstall). See Resolved Caveats - Release 3.5(8), page 82 for details or Enhancements per Agent Version, page 52.

Supported AV Product List

The Supported AV Product List remains at Version 20. There are no enhancements for release 3.5(8).

See Clean Access Supported Antivirus Product List, page 64 and Supported AV Product List Versions, page 72 for information on previous versions.

Enhancements for Release 3.5(7)

This section details enhancements to existing features delivered with release 3.5(7) of the Cisco Clean Access Manager and Cisco Clean Access Server.

- OOB Support for Cisco Catalyst 5500, 2960 Series Switches
- OOB Virtual Gateway Enhancements
- NAT Gateway Notification
- Enhanced Security
- Clean Access Agent Enhancements (3.5.9)
- Supported AV Product List (Version 20)

See also Resolved Caveats - Release 3.5(7), page 83.

OOB Support for Cisco Catalyst 5500, 2960 Series Switches

Release 3.5(7) adds out-of-band switch management support for the following switches:

- Cisco Catalyst 5500
- Cisco Catalyst 2960

Note Cisco Catalyst 5500 does not support mac-notification SNMP traps.

See also Supported Switches for Cisco Clean Access, page 4.

OOB Virtual Gateway Enhancements

For OOB Virtual Gateway mode, there is a new option in the Port Profile to prevent the switch port from being bounced when:

- Users are removed from the Out-of-Band Online Users List, or
- Devices are removed from the Certified Devices list

Instead, the port VLAN will be changed to the Authentication VLAN.

This option is intended to prevent bouncing of a switch port when a client machine is connected to the switch port through a VoIP phone. The feature allows Cisco Clean Access to authenticate/assess/quarantine / remediate a client machine (laptop/desktop) without affecting the operation of a VoIP phone connected to the switch port. This enhancement results in a new option "**Remove Out-of-Band online user without bouncing the port**" added to following pages:

- **Switch Management > Profiles > Port > New** or **Edit**

Discovery Host Field

The "CAS Discovery Host" field is renamed to **Discovery Host** on the following web console page:

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

NAT Gateway Notification

Administrators will be shown the following notification when choosing **NAT Gateway** or **Out-of-Band NAT Gateway** for the operating mode of a CAS: "NAT Gateway is only recommended for demo/testing purposes. For production deployments, Virtual or Real-IP Gateway is recommended." This affects the following web console page:

- **Device Management > CCA Servers > New Server**

Enhanced Security

Starting with release 3.5(7), the Clean Access Manager web console requires high encryption (64 or 128 bit) and does not accept 56-bit encryption. See Web Browser Compatibility, page 8.

Clean Access Agent Enhancements (3.5.9)

For in-band configurations, release 3.5(7) of Cisco Clean Access with version 3.5.9 of the Agent provides a new option to enable/disable the Clean Access Agent from logging the user off the Clean Access system when the user logs off from the Windows domain or shuts down the Windows workstation. This allows the administrator to configure whether or not logged-in users remain logged into the network when the machine is shut down/restarted. Note that:

- 3.5.7 and below Agent will leave the Agent logged in when machine is shut down.
- 3.5.8 Agent will log out the user when machine is shutdown or user logs off.
- 3.5.9 Agent combined with 3.5(7) CAM/CAS will make this option configurable.

Note

- This feature only applies to new Agent logins. For example, if the administrator checks the option to force users to log off at Windows shutdown, this will not apply to users who are already logged in. The feature only immediately applies to new user logins after the option is checked in the web console.
- This Agent logout feature does not apply to OOB deployments.
- If the Agent is terminated by Windows prior to successfully logging off from the Clean Access environment, the Clean Access logoff attempt may not succeed.

This enhancement results in a new checkbox for "**Logoff Clean Access Agent users from network on their machine logoff or shutdown**" added to the following web console page:

- **Device Management > Clean Access > General Setup**

See also Clean Access Agent Enhancements (3.5.8), page 21 and Enhancements per Agent Version, page 52.

Supported AV Product List (Version 20)

- See Clean Access Supported Antivirus Product List, page 64 for the Supported AV Product List as of the latest release.
- See Supported AV Product List Versions, page 72 for details on each version of the list.

Enhancements for Release 3.5.6.1

Release 3.5.6.1 is a general and important bug fix release and patch for the Clean Access Manager and Clean Access Server. No new features are added.

Warning **Because this patch is related to database syncing on the CAM, please carefully follow the upgrade instructions. A CAM upgrade that is not performed correctly may result in configuration loss.**

Note

- The 3.5.6.1 patch is a mandatory patch for all 3.5(6) systems. All customers on 3.5(6) should apply this patch.
- This patch will run only on 3.5(6) systems.
- The patch is a tar ball that must be applied to both the CAS and the CAM.
- Instead of rebooting the machine, you may simply restart the service by issuing the **service perfigo restart** command.

Information for the 3.5.6.1 patch is in the following sections:

- Upgrade Instructions for 3.5.6.1
- Resolved Caveats - Release 3.5.6.1

Upgrade Instructions for 3.5.6.1

Please execute the steps for the following patch update procedures on your CAM and CAS.

- 3.5.6.1 Patch Upgrade Procedure for CAM
- 3.5.6.1 Patch Upgrade Procedure for CAS

3.5.6.1 Patch Upgrade Procedure for CAM

Carefully execute the following patch update procedure on your CAMs. After the steps are completed, the database of the current active CAM will be propagated to both CAMs, and the CAMs will be in sync.

Step 1 Log into Cisco Secure Software and download the **cca-3.5.6-to-3.5.6.1-upgrade.tar.gz** patch file to your local computer from the 3.5.6 folder under http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.5.6

Step 2 Open an SSH terminal to the Inactive (Standby) CAM and login as the `root` user with root **password** (default password is `cisco123`)

Step 3 Copy the **cca-3.5.6-to-3.5.6.1-upgrade.tar.gz** file to the /store directory:

Step 4 Untar the tar file:

```
tar -xzf cca-3.5.6-to-3.5.6.1-upgrade.tar.gz
```

Step 5 Change directory to the patch folder:

```
cd cca_upgrade_3.5.6.1
```

Step 6 Execute the upgrade:

```
./UPGRADE.sh
```

Step 7 **Do NOT restart the perfigo service on the inactive machine.**

Step 8 SSH to the Active CAM, and login as the `root` user with root **password** (default password is `cisco123`).

Step 9 Repeat steps 3 through 6 on the Active CAM.

Step 10 Restart the service on the Active CAM:

```
service perfigo restart
```

Step 11 After the Active CAM is restored and functioning properly, go to the SSH terminal of the Inactive CAM and restart the service on the Inactive CAM:

```
service perfigo restart
```

Step 12 Follow the 3.5.6.1 Patch Upgrade Procedure for CAS to upgrade each CAS.

3.5.6.1 Patch Upgrade Procedure for CAS

Step 1 Download the **cca-3.5.6-to-3.5.6.1-upgrade.tar.gz** patch file to your local computer from the 3.5.6 folder under http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.5.6

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

- Upgrade CAS from CAS Management Pages (3.5.5 and above), page 102
- Upgrade CAS from CAS Web Console (3.5.3/3.5.4), page 103
- Upgrade via Console/SSH, page 105

Enhancements for Release 3.5(6)

This section details enhancements to existing features delivered with release 3.5(6) of the Cisco Clean Access Manager and Cisco Clean Access Server.

- Case Insensitivity for Max Sessions per User Account
- API Enhancements
- Nessus Plugin Default View
- Clean Access Agent Distribution Enhancements
- Clean Access Agent Enhancements (3.5.8)
- Supported AV Product List (Version 18)

For additional details, see also Clean Access Agent Enhancements, page 52 and Clean Access Supported Antivirus Product List, page 64. For configuration details, refer to the product documentation.

Case Insensitivity for Max Sessions per User Account

The Max Sessions per User Account feature adds a new option for case insensitivity. The Case-Insensitive checkbox (3.5.6 and above) allows the administrator to allow/disallow case-sensitive user names towards the max session count. For example, if the administrator chooses to allow case-sensitivity (box unchecked; default), then jdoe, Jdoe, and jDoe are all treated as different users. If the administrator chooses to disable case-sensitivity (box checked), then jdoe, Jdoe, and jDoe are treated as the same user.

This enhancement results in a new "**Case-Insensitive**" checkbox added to these web console pages:

- **User Management > User Roles > New Role** or **Edit Role**

API Enhancements

With release 3.5(6), the Cisco Clean Access API utility script, cisco_api.jsp, provides two new functions and enhances an existing function.

- `kickoobuser` —(New) Removes the OOB user session and bounces the port if the user is currently connected to the port
- `getcleanuserinfo` —(New) Gets the certified device(s) information.
- `removecleanmac`—(Enhanced) Removes certified device from Certified List, and enhanced to remove out-of-band users from the Online Users list in addition to in-band users.

In addition, the descriptions for `addcleanmac`, `removecleanmac`, and `removemac` have been updated on the cisco_api.jsp page itself, which describes all the available API functions. 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

Nessus Plugin Default View

With release 3.5(6), the default view on the Nessus plugin page is changed from "All" to "**Selected**." Note that if Nessus plugins have not yet been checked and updated for the user role, the default view (i.e. Selected Plugins) shows no plugins. To select plugins, the administrator must choose one of the other views (for example, "All," "Backdoors," etc.) from the "Show...Plugins" dropdown.

This enhancement results in changes to the following web console page:

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

Clean Access Agent Distribution Enhancements

With release 3.5(6), the Clean Access Agent Distribution page of the CAM web console provides a new option to disable upgrade notifications (mandatory or optional) to 3.5.1+ Agent users, even when a newer Agent update becomes available on the CAM.

Note After CAM/CAS upgrade to 3.5(6), this feature is available for all 3.5.1 and above Clean Access Agents.

Prior to this feature, if an Agent update was available, the user was always shown a prompt, whether the upgrade was optional or mandatory. This additional Distribution option will cause the user not to be informed of an Agent upgrade even if an Agent update is available. Enabling this option in effect prevents distribution of the Agent Patch upgrade to users when a newer Agent is downloaded to the CAM.

This enhancement results in the following change to the web console:

- **Device Management > Clean Access > Clean Access Agent > Distribution** -- new checkbox for "**Do not offer current Clean Access Agent Patch to users for upgrade**"

See also Clean Access Agent Enhancements, page 52 for additional details

Clean Access Agent Enhancements (3.5.8)

For in-band configurations, version 3.5.8 of the Clean Access Agent now attempts to log the user off the Clean Access system prior to Windows user logout or Windows shutdown. This enhancement takes effect when the user logs off from the Windows domain (i.e. Start->Shutdown->Log off current user) or shuts down the machine (Start->Shutdown->Shutdown machine). Prior to the 3.5.8 Agent, a logged-in user remained logged into the network when the machine was shut down/restarted.

Note that the attempt to log off from the Clean Access environment may be unsuccessful if the Agent is terminated by Windows prior to successfully logging off from the Clean Access system.

Note This Agent logout feature does not apply to OOB deployment.

See Clean Access Agent Enhancements, page 52 for additional details on version 3.5.6 and 3.5.7 of the Clean Access Agent (released post 3.5(5)).

Supported AV Product List (Version 18)

- See Clean Access Supported Antivirus Product List, page 64 for the Supported AV Product List as of the latest release.
- See Supported AV Product List Versions, page 72 for details on each version of the list.

Enhancements for Release 3.5.5.1

Release 3.5.5.1 is a general and important bug fix release and patch for the Clean Access Manager and Clean Access Server. No new features are added.

Warning **Because this patch is related to database syncing on the CAM, please carefully follow the upgrade instructions. A CAM upgrade that is not performed correctly may result in configuration loss.**

Note

- The 3.5.5.1 patch is a mandatory patch for all 3.5(5) systems. All customers on 3.5(5) should apply this patch.
- This patch will run only on 3.5(5) systems.
- The patch is a tar ball that must be applied to both the CAS and the CAM.
- Instead of rebooting the machine, you may simply restart the service by issuing the **service perfigo restart** command.

Information for the 3.5.5.1 patch is in the following sections:

- Upgrade Instructions for 3.5.5.1
- Resolved Caveats - Release 3.5.5.1

Upgrade Instructions for 3.5.5.1

Please execute the steps for the following patch update procedures on your CAM and CAS.

- 3.5.5.1 Patch Upgrade Procedure for CAM
- 3.5.5.1 Patch Upgrade Procedure for CAS

3.5.5.1 Patch Upgrade Procedure for CAM

Carefully execute the following patch update procedure on your CAMs. After the steps are completed, the database of the current active CAM will be propagated to both CAMs, and the CAMs will be in sync.

Step 1 Log into Cisco Secure Software and download the **cca-3.5.5-to-3.5.5.1-upgrade.tar.gz** patch file to your local computer from the 3.5.5 folder under http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.5.5

Step 2 Open an SSH terminal to the Inactive (Standby) CAM and login as the `root` user with root **password** (default password is `cisco123`)

Step 3 Copy the **cca-3.5.5-to-3.5.5.1-upgrade.tar.gz** file to the /store directory:

Step 4 Untar the tar file:

```
tar -xzf cca-3.5.5-to-3.5.5.1-upgrade.tar.gz
```

Step 5 Change directory to the patch folder:

```
cd cca_upgrade_3.5.5.1
```

Step 6 Execute the upgrade:

```
./UPGRADE.sh
```

Step 7 **Do NOT restart the perfigo service on the inactive machine.**

Step 8 SSH to the Active CAM, and login as the `root` user with root **password** (default password is `cisco123`).

Step 9 Repeat steps 3 through 6 on the Active CAM.

Step 10 Restart the service on the Active CAM:

```
service perfigo restart
```

Step 11 After the Active CAM is restored and functioning properly, go to the SSH terminal of the Inactive CAM and restart the service on the Inactive CAM:

```
service perfigo restart
```

Step 12 Follow the 3.5.5.1 Patch Upgrade Procedure for CAS to upgrade each CAS.

3.5.5.1 Patch Upgrade Procedure for CAS

Step 1 Download the **cca-3.5.5-to-3.5.5.1-upgrade.tar.gz** patch file to your local computer from the 3.5.5 folder under http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.5.5

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

– Upgrade CAS from CAS Management Pages (3.5.5 and above), page 102

– Upgrade CAS from CAS Web Console (3.5.3/3.5.4), page 103

– Upgrade via Console/SSH, page 105

Important Notes for Release 3.5(5)

OOB Switch Management MAC Address Table Aging Time

The MAC address table aging-time must be set to a minimum of 3600 seconds on the switch when mac-notification SNMP traps are used for switch management. For details, see “Example Switch Configuration Steps” in the *Cisco Clean Access Manager Installation and Administration Guide, Release 3.5*.

Enhancements for Release 3.5(5)

This section details enhancements to existing features delivered with release 3.5(5) of the Cisco Clean Access Manager and Cisco Clean Access Server.

- New Enable/Disable L3 Option on CAS
- CAS Discovery Host Enhancements
- Clean Access Agent Enhancement (3.5.5)
- OOB Switch Management SNMP Receiver Enhancements
- OOB Switch Management MAC Address Table Aging Time
- OOB Switch Management Respects Device Filters
- Automatic Update of Default Host Policies
- Supported AV Product List (Version 17)
- System Upgrade Enhancements
- Event Log Enhancements

For additional details, see also Clean Access Agent Enhancements, page 52 and Clean Access Supported Antivirus Product List, page 64. For configuration details, refer to the product documentation.

New Enable/Disable L3 Option on CAS

Release 3.5(3) introduced support for multi-hop L3 in-band deployments, and with release 3.5(3) and 3.5(4), this feature was enabled by default. With release 3.5(5), the administrator has the option of enabling or disabling the L3 feature at the CAS level. L3 capability will be disabled by default after upgrade or new install of 3.5(5), and enabling the feature will require an update and reboot of the Clean Access Server.

To Enable L3 Capability:

1. Go **Device Management** > **CCA Servers** > **Manage [IP address]** > **Network** and click the checkbox for “**Enable L3 support for Clean Access Agent**.”
2. Click **Update**.
3. Click **Reboot**.

Note The **CAS Discovery Host** field still automatically populates with the IP address of the CAM by default after new install or upgrade to 3.5(5).

To Disable L3 Capability:

To disable L3 discovery of the Clean Access Server at the CAS level for all Clean Access Agents:

1. Go **Device Management > CCA Servers > Manage [IP address] > Network** and uncheck the option for "**Enable L3 support for Clean Access Agent**."
2. Click **Update**.
3. Click **Reboot**.

To disable L3 discovery of the Clean Access Server for NEW installs of the Clean Access Agent (3.5.3+)

1. Go **Device Management > Clean Access > Clean Access Agent > Distribution**.
2. Change the **CAS Discovery Host** field from your CAM's IP address to **127.0.0.1**.
3. Click **Update**.

Note To disable L3 discovery for releases prior to 3.5(5), the CAS Discovery Host field should be set to either 127.0.0.1 or to a hostname/IP in your network that is behind the CAS (on the trusted side).

This feature results in the following enhancements to the web console:

- **Device Management > CCA Servers > Manage [IP address] > Network** (new checkbox for "**Enable L3 support for Clean Access Agent**."

See Clean Access Agent Enhancements, page 52 for additional details.

CAS Discovery Host Enhancements

With release 3.5(5), the Clean Access Agent will now send use a proprietary, encrypted, UDP-based protocol, instead of HTTP, to the Clean Access Manager to discover the Clean Access Server. This changes the behavior of the 3.5.5 Clean Access Agent, but does not affect the web console interface or Agent dialogs. See Software Compatibility Matrixes, page 4 and Clean Access Agent Enhancements, page 52 for further details.

Clean Access Agent Enhancement (3.5.5)

With release 3.5(5), the Clean Access Agent installer now installs by default for all users on a client machine, as opposed to only the current user.

Note that 3.5.5 Agent will only support multi-hop L3 operation with the 3.5(5) CAM/CAS. L3 discovery will not work with older CAM/CAS versions. See Software Compatibility Matrixes, page 4 and Clean Access Agent Enhancements, page 52 for further details.

OOB Switch Management SNMP Receiver Enhancements

Release 3.5(5) enhances the Clean Access Manager SNMP Receiver to support simultaneous use of different versions of SNMP (V1, V2c, V3) when controlling groups of switches in which individual switches may use different versions of SNMP.

This enhancement results in changes to the following web console page:

- **Switch Management > Profiles > SNMP Receiver > SNMP Trap**

OOB Switch Management Respects Device Filters

With release 3.5(5), the Clean Access Manager now respects the global Device Filters list (under **Device Management > Filters > Devices > New**) for Out-of-Band deployments. In OOB, the rules configured for MAC addresses on the global Device Filter list will have the highest priority for user/device processing (just as for In-Band deployments). For OOB, the priority of rule processing is as follows:

1. Device Filters (if configured with a MAC address, and if enabled for OOB under **Switch Management > Profiles > Port > New** or **Edit)**
2. Certified Devices List
3. Out-of-Band Online User List

MAC address device filters configured for OOB have the following options and behavior:

- allow—The device is put in the Default Access VLAN.
- deny—The device is put in the Default Auth VLAN.
- use role—The device is put in the Access VLAN configured for the user role.

This enhancement results in changes to the following web console page:

- **Switch Management > Profiles > Port > New** or **Edit** (UI is clarified, and new option "**Switch VLAN if the device is in the global device filter list**" is added)

Automatic Update of Default Host Policies

As a convenience for administrators, Cisco Clean Access will provide updates to default host-based traffic policies for the Unauthenticated, Temporary, and Quarantine user roles.

Note Administrators always have the option of creating their own host-based traffic policies for any update sites via **User Management > User Roles > Traffic Control > Host**.

Updates to default host-based policies for default system user roles will be distributed when an Update or Clean Update is performed from **Device Management > Clean Access > Clean Access Agent > Updates**. Note that default host policies are disabled by default, and you must enable them for each role. The following default allowed hosts are provided with release 3.5(5):

Microsoft Windows Update

- microsoft.com
- windowsupdate.com

Symantec AntiVirus Update

- liveupdate.symantecliveupdate.com (HTTP)
- liveupdate.symantec.com (HTTP)
- update.symantec.com (FTP)

McAfee AntiVirus Update

- update.nai.com (HTTP)
- ftp.nai.com (FTP)

TrendMicro AntiVirus Update

- pccreg.antivirus.com
- activeupdate.trendmicro.com

This enhancement results in the following changes in the web console:

- **Device Management > Clean Access > Clean Access Agent > Updates** (new entry "Current Version of Default Host Policies")
- **User Management > User Roles > Traffic Control > Host** (for 3.5.5, default host policies are added for TrendMicro AntiVirus Update)

Supported AV Product List (Version 17)

- See Supported AV Product List Versions, page 72 for details on each version of the list.
- See Clean Access Supported Antivirus Product List, page 64 for the latest Supported AV Product List as for the latest release.

System Upgrade Enhancements

Release 3.5(4) introduced the capability of upgrading the CAM via the CAM web console and the CAS via the CAS web console, as follows:

- CAM web admin console: **Administration > CCA Manager > System Upgrade**
- CAS (direct access) web admin console: **Administration > Software Update**

Release 3.5(5), installed, will additionally allow for web console upgrade of the CAS via the CAS management pages for future upgrades (e.g. 3.5.6), as follows:

- CAM web admin console: **Device Management > CCA Servers > Manage [IP address] > Misc > Update**

Event Log Enhancements

Starting with release 3.5(5), Switch Management events for notifications received by the CAM from switches are no longer written to the event log. They will instead be written only to the logs on the file system (/perfigo/logs/perfigo-log0.log.0). Furthermore, these events are written to disk only when the log level is set to INFO or finer (using the loglevel utility found in /perfigo/control/bin).

Enhancements for Release 3.5.4.1

Release 3.5.4.1 is a general, important bug fix release and patch for the CAS. No new features are added.

The 3.5.6 Clean Access Agent uncovered a hidden bug in the SWISS (CAS discovery) implementation on the Clean Access Server which caused the 3.5.6 Agent not to be able to log into 3.5(4) and prior CASes. This patch resolves this issue and allows 3.5.6 and above Agents to log in. See Resolved Caveats - Release 3.5.4.1, page 86, and Clean Access Agent Enhancements, page 52 for details.

Note

- The 3.5.4.1 patch is a mandatory patch for all 3.5(4) systems. All customers on 3.5(4) should apply this patch to their Clean Access Servers.
- This patch will run only on 3.5(4) systems.
- The patch is a tar ball that must be applied to the CAS(es) only.
- You must reboot the machine after applying the patch.

Upgrade Instructions for 3.5.4.1

Use the steps below to apply the 3.5.4.1 patch to each Clean Access Server in your system.

Step 1 Download the **cas-3.5.4-to-3.5.4.1-upgrade.tar.gz** patch file to your local computer from the 3.5.4 folder under http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.5.4.

Step 2 Use one of the following sets of instructions to upgrade your CAS(es):

- To upgrade via web console (from 3.5(3) and above only), see Upgrade CAS from CAS Web Console (3.5.3/3.5.4), page 103.
- To upgrade an HA CAS pair, see Upgrading High Availability Pairs, page 107.
- To upgrade via SSH, use Upgrade Instructions for 3.5.4.1 CAS Patch via SSH, page 28.

Upgrade Instructions for 3.5.4.1 CAS Patch via SSH

Step 1 Open an SSH terminal and copy the `cas-3.5.4-to-3.5.4.1-upgrade.tar.gz` patch file into the /store directory on each Clean Access Server.

Step 2 Change directory to /store on each machine:

```
cd /store
```

Step 3 Untar the patch file on each machine:

```
tar xzvf cas-3.5.4-to-3.5.4.1-upgrade.tar.gz
```

Step 4 Cd to the upgrade directory:

```
cd cca_upgrade_3.5.4.1
```

Step 5 Execute the patch on each machine:

```
./UPGRADE.sh
```

Step 6 Reboot each machine:

```
reboot
```

Enhancements for Release 3.5(4)

This section details enhancements to existing features delivered with release 3.5(4) of the Cisco Clean Access Manager and Cisco Clean Access Server.

- OOB Support for Cisco Catalyst 3500 XL, 2900 XL, 2940 Series Switches
- OOB Switch Management Ports Configuration Enhancements
- API Support Enhancement
- Agent-AV Support Info Page Enhancements
- Supported AV Product List (Version12)
- Clean Access Agent (3.5.4) Auto-Upgrade
- System Upgrade Enhancements
- Logging Enhancements

For additional details, see also Clean Access Agent Enhancements, page 52 and Clean Access Supported Antivirus Product List, page 64. For configuration details, refer to the product documentation.

OOB Support for Cisco Catalyst 3500 XL, 2900 XL, 2940 Series Switches

Release 3.5(4) adds out-of-band switch management support for the following switches:

- Cisco Catalyst 3500 XL
- Cisco Catalyst 2900 XL
- Cisco Catalyst 2940

See Supported Switches for Cisco Clean Access, page 4 for details.

OOB Switch Management Ports Configuration Enhancements

Release 3.5(4) provides a new button option from the web console to make switch configuration changes permanent on the switch. Prior to 3.5(4), the web console only allowed changing the running configuration of the switch and saving the switch configuration had to be done on the switch itself.

This enhancement results in the following modifications to the **Switch Management** > **Devices** > **Switch [IP address]** > **Ports** page of the web admin console:

- New **Save** button for “Save the switch running configuration into non-volatile memory:”
- **Setup** button replaces “Update Switch Running Configuration” button for “Set up mac-notification on managed switch ports:”
- The following buttons are renamed and moved to the top of the page for “Set the initial VLANs for the ports to the current VLAN settings of the switch:”
  - **Reset All** button replaces “Reset initial VLANs for ALL ports”
  - **Set New Ports** button replaces “Set initial VLANs for NEW ports”

API Support Enhancement

Cisco Clean Access provides a utility script called cisco_api.jsp that allows you to perform certain operations using HTTPS POST. The Clean Access API for your Clean Access Manager is accessed via: https://<cam-ip-or-name>/admin/cisco_api.jsp

This API was originally designed to provide unauthenticated access. However, due to information available through this API, this API will be protected by authentication starting with release 3.5.4. Release 3.5.4 will require authentication over SSL for access to the API. (Note that this also resolves caveat CSCsb48572).

Since it is now necessary to authenticate before accessing the API, this enhancement results in two new authentication methods:

- Authentication by Session

  This method requires the administrator to create an authentication shell script that will set a cookie with the session ID to be accessed for the rest of the admin session. If a session ID cookie is not set, the user will be prompted to login. This method results in two new functions being added: *adminlogin* and *adminlogout*. The administrator login function returns a session ID which has to be set as a cookie for usage of any API. The *adminlogout* function should then be used to terminate the session. However, if *adminlogout* is not used, the session will still be terminated by admin session timeout.

- Authentication by Function

  If the administrator does not want to create a shell script using cookies, this method is provided as an alternative. With this method, authentication is performed every time a function is used. This results in two new optional parameters added to every function: *admin*, and *password*. If authenticating by function, you will need to add the *admin* and *password* parameters to all functions that you are using in your existing script. In this case, you do not use the *adminlogin* and *adminlogout* functions.

Agent-AV Support Info Page Enhancements

Release 3.5(4) further integrates the dynamic AV checking provided with release 3.5(3) (see Dynamic AV Definition Checks, page 37) to make this process more transparent for the administrator. Starting with version 3.5.3 and 3.5.4 of the Clean Access Agent, the Agent automatically returns its version number to the Clean Access Manager. This allows the CAM to determine on-the-fly the method of AV checking to perform (version or date) when sending the requested AV definition checks to the Agent.

Note

- The CAM always attempts to first use the virus definition version for AV checks. If version is not available, the CAM uses the virus definition date instead.
- The 3.5.0, 3.5.1, and 3.5.2 Agents do not send their version information to the CAM (as this is a new feature for 3.5.3 and above). If the CAM does not know the Agent version, the CAM always selects support for the earliest Agent as the baseline for AV checks. For example, if using a 3.5.2 Agent with an AV product that has a Minimum Agent version of 3.5.0 for Def Date and 3.5.1 for Def Version, the CAM will use the Def Date to perform the check. If a 3.5.3/3.5.4 Agent is used, the CAM uses the Def Version.

This enhancement modifies the following page of the web admin console:

- **Device Management > Clean Access Agent > Rules > Agent-AV Support Info**

  The “Support AV Products for Agent Version []” portion of the page, added for release 3.5(3), is removed for release 3.5(4) as this function is now automatically performed by the CAM going forward.

See also Supported AV Product List Versions, page 72.

Supported AV Product List (Version12)

- See Clean Access Supported Antivirus Product List, page 64 for the Supported AV Product List as of the latest release.
- See Supported AV Product List Versions, page 72 for details on each version of the list.

Clean Access Agent (3.5.4) Auto-Upgrade

With release 3.5(4), the Clean Access Agent will no longer check for newer Agent versions at application startup, and will instead check for Agent updates at every login request. Note that 3.5.1/3.5.2/3.5.3 Agents will still check for Agent updates only at application restart or on client machine reboot.

Note New installs of 3.5.4 or above automatically set the "Current Clean Access Agent Patch is a mandatory upgrade" option by default under Device Management > Clean Access > Clean Access Agent > Distribution. If the option is disabled in a system being upgraded, then the current setting (disabled) will be carried over to the upgraded system.

See Clean Access Agent Enhancements, page 52 for further details.

System Upgrade Enhancements

Release 3.5(3) introduced the ability to perform software upgrade on the CAM and CAS by uploading the upgrade file in .tar.gz format via the web console. This means with release 3.5(4), you can now upgrade to 3.5(4) via the web console UI. For upgrade instruction details via the web console, see Installing or Upgrading to a New Software Release, page 97.

The Clean Access Manager will automatically perform all the upgrade tasks that are currently done manually (for example, create snapshots before and after upgrade, untar file, cd to /store, run upgrade script).

Note You must have 3.5(3) installed and running before you can use this feature to upgrade to 3.5(4).

In addition the upgrade process has been enhanced as follows:

- You can now upload upgrade .tar.gz files (with date/version information) before applying them to the CAM or CAS. You will also have the ability to upload multiple patch files at the same time.
- Once the .tar.gz upgrade files are uploaded to the CAM, you can manage them by viewing their attached Notes (if any), deleting the files from the CAM, or clicking **Apply** to perform the upgrade.
- The new **Apply** button performs the upgrade then automatically reboots the server machine after upgrade is complete. This new feature is only available by using the **Apply** button from the web console.
- Upgrades for future releases will now check a table of contents file to ensure that all pieces of the build are there.
- A Notes file can now be attached with the upgrade file to provide important information about the upgrade.

- The **Shutdown** button shuts down the service on the box without shutting down the box itself (equivalent to the **service perfigo stop** command). To restart the service, you must use the **service perfigo restart** or **reboot** CLI command from a command shell (since stopping the service stops the web console).

These enhancements result in modifications to the following pages in the web admin console:

- CAM web admin console: **Administration > CCA Manager > System Upgrade**
- CAS (direct access) web admin console: **Administration > Software Update**

Logging Enhancements

Logging enhancements have been made to support Agent AV check implementation.

Enhancements for Release 3.5.3.2

Release 3.5.3.2 is a general, important bug fix release and patch for the CAS. No new features are added.

The 3.5.6 Clean Access Agent uncovered a hidden bug in the SWISS (CAS discovery) implementation on the Clean Access Server which caused the 3.5.6 Agent not to be able to log into 3.5(4) and prior CASes. This patch resolves this issue and allows 3.5.6 and above Agents to log in. See Resolved Caveats - Release 3.5.3.2, page 88, and Clean Access Agent Enhancements, page 52 for details.

Note

- The 3.5.3.2 patch is a mandatory patch for all 3.5.3.1 systems. All customers on 3.5.3.1 should apply this patch to their Clean Access Servers.
- This patch will run only on 3.5.3.1 systems.
- The patch is a tar ball that must be applied to the CAS(es) only.
- You must reboot the machine after applying the patch.

Upgrade Instructions for 3.5.3.2

Use the steps below to apply the 3.5.3.2 patch to each Clean Access Server in your system.

Step 1 Download the **cas-3.5.3.1-to-3.5.3.2-upgrade.tar.gz** patch file to your local computer from the 3.5.3 folder under http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.5.3.

Step 2 Use one of the following sets of instructions to upgrade your CAS(es):

- To upgrade via web console (from 3.5(3) and above only), see Upgrade CAS from CAS Web Console (3.5.3/3.5.4), page 103.
- To upgrade an HA CAS pair, see Upgrading High Availability Pairs, page 107.
- To upgrade via SSH, use Upgrade Instructions for 3.5.3.2 CAS Patch via SSH, page 33.

Upgrade Instructions for 3.5.3.2 CAS Patch via SSH

Step 1 Open an SSH terminal and copy the `cas-3.5.3.1-to-3.5.3.2-upgrade.tar.gz` patch file into the /store directory on each Clean Access Server.

Step 2 Change directory to /store on each machine:

```
cd /store
```

Step 3 Untar the patch file on each machine:

```
tar xzvf cas-3.5.3.1-to-3.5.3.2-upgrade.tar.gz
```

Step 4 Cd to the upgrade directory:

```
cd cca_upgrade_3.5.3.2
```

Step 5 Execute the patch on each machine:

```
./UPGRADE.sh
```

Step 6 Reboot each machine:

```
reboot
```

Enhancements for Release 3.5.3.1

Release 3.5.3.1 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 3.5.3.1 patch is a mandatory patch for all 3.5.3 systems. All customers on 3.5.3 should apply this patch.
- This patch will run only on 3.5.3 systems.
- The patch is a tar ball that must be applied to both the CAS and the CAM.
- Instead of rebooting the machine, you may simply restart the service by issuing the **service perfigo restart** command.

Without the 3.5.3.1 patch, systems running Cisco Clean Access 3.5.3 might experience service outages with very little load on the systems. Information for the 3.5.3.1 patch is in the following sections:

- Upgrade Instructions for 3.5.3.1
- Resolved Caveats - Release 3.5.3.1

Upgrade Instructions for 3.5.3.1

Use the following steps to apply the 3.5.3.1 patch to the CAM and CAS:

Step 1 Download the **cca-3.5.3-to-3.5.3.1-upgrade.tar.gz** patch file to your local computer from the 3.5.3 folder under http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.5.3.

Step 2 Open an SSH terminal and copy the `cca-3.5.3-to-3.5.3.1-upgrade.tar.gz` patch file into the /store directory on the Clean Access Manager and each Clean Access Server.

Step 3 Change directory to /store on each machine:

```
cd /store
```

Step 4 Untar the patch file on each machine:

```
tar xzvf cca-3.5.3-to-3.5.3.1-upgrade.tar.gz
```

Step 5 Execute the patch on each machine:

```
./cca-3.5.3-to-3.5.3.1-upgrade.sh
```

Step 6 Restart the service on each machine:

```
service perfigo restart
```

New Features in Release 3.5(3)

This section details the new additional features delivered with release 3.5(3) of the Cisco Clean Access Manager and Cisco Clean Access Server.

- Multi-Hop L3 In-Band Deployment Support
- VPN Integration and Single Sign-On (SSO)
- System Upgrade via Web Console (3.5(3) and Above)
- Automated Daily Database Backups
- Database Recovery Tool
- Support Logs

See also Enhancements for Release 3.5(3), page 37 for additional details. For configuration details, refer to the product documentation.

Multi-Hop L3 In-Band Deployment Support

Release 3.5(3) of Cisco Clean Access enables administrators to deploy the Clean Access Server (CAS) in-band behind a VPN concentrator, or router, or multiple routers. Prior to 3.5(3), Clean Access Server(s) needed to be deployed either as a bridge (Virtual Gateway) or first-hop default gateway with Layer 2 proximity to users, in order for user MAC addresses to be visible to the CAS. Release 3.5(3) adds the capability of multi-hop Layer 3 in-band deployment by allowing the Clean Access Manager (CAM) and CAS to track user sessions by unique IP address when users are separated from the CAS by one or more routers. Note that you can have a CAS supporting both L2 and L3 users. With layer 2-connected users, the CAM/CAS continue to manage these user sessions based on the user MAC addresses, as before.

For users that are one or more L3 hops away, note the following considerations:

- User sessions are based on unique IP address rather than MAC address.
- If the user’s IP address changes (for example, the user loses VPN connectivity), the client must go through the Clean Access certification process again.
- In order for clients to discover the Clean Access Server when they are one or more L3 hops away, the 3.5.3 (or above) Clean Access Agent must be initially installed by being downloaded from the CAS (via Download Agent button (i.e. web login), or client auto-upgrade). Acquiring and installing the 3.5.3 Agent by any means other than direct download from the CAS (for example, Cisco Downloads) will not provide the necessary CAM information to the Agent and will not allow those Agent installations to operate in a multi-hop Layer 3 deployment. See Clean Access Agent (3.5.3), page 39 and Clean Access Agent Enhancements, page 52 for details.
- Since the Certified List tracks L2 users by MAC address, multi-hop L3 users do not appear on the Certified Devices List and the Certified Devices Timer does not apply to these users. The L3 users will only be on the Online User list (In-Band).

- All other user audit trails, such as network scanner and Clean Access Agent logs, are maintained for multi-hop L3 users.
- The Session Timer will work the same way for multi-hop L3 In-Band deployments and L2 (In-Band or Out-of-Band) deployments.

  Note that when the Single Sign-On (SSO) feature is configured for multi-hop L3 VPN concentrator integration, if the user's session on the CAS times out but the user is still logged in on the VPN concentrator, the user session will be restored without providing a username/password.
- The Heartbeat Timer will not function in L3 deployments, and does not apply to Out-of-Band deployments.

  Note that the HeartBeat Timer will work if the CAS is the first hop behind the VPN concentrator. This is because the VPN concentrator responds to the ARP queries for the IP addresses of its current tunnel clients.

This new feature results in the following enhanced page in the web admin console:

- **Device Management > Clean Access > Clean Access Agent > Distribution** (new "CAS Discovery Host" field)

VPN Integration and Single Sign-On (SSO)

In addition to being deployable with VPN concentrators, Cisco Clean Access provides the best user experience possible for Cisco VPN concentrator users through Single Sign-On (SSO). Users logging in through the VPN Client do not have to login again to Cisco Clean Access. Cisco Clean Access leverages the VPN login and any VPN user group/class attributes to map the user to a particular role.

This level of integration is achieved using RADIUS Accounting with the Clean Access Server acting as a RADIUS accounting proxy.

Release 3.5(3) of Cisco Clean Access supports the following VPN clients for the purposes of Single Sign-On:

- Cisco SSL VPN Client (Full Tunnel)
- Cisco VPN Client (IPSec)

See VPN Components Supported for Single Sign-On, page 3 for details.

This new feature results in the following new pages or enhancements in the web admin console:

- **User Management** > **Auth Servers** > **New Server** (new "Cisco VPN Server" Authentication Type)
- **Device Management** > **CCA Servers** > **IPaddress** > **Authentication** (new tab)
- **Device Management** > **CCA Servers** > **IPaddress** > **Authentication** > **VPN Auth** (incorporates new configuration subpages: General, VPN Concentrators, Accounting Servers, Accounting Mapping)

System Upgrade via Web Console (3.5(3) and Above)

Going forward from version 3.5(3) of the Cisco Clean Access software, administrators will be able to perform software upgrade on the CAM and CAS by uploading the upgrade file in .tar.gz format via the web console. The Clean Access Manager will automatically perform all the upgrade tasks that are currently done manually (for example, create snapshots before and after upgrade, untar file, cd to /store, run upgrade script).

Note You will need to have 3.5(3) installed and running before you can use this feature for your next upgrade.

The software upgrade pages have a new **Shutdown** button that shuts down the service on the box without shutting down the box itself (equivalent to the **service perfigo stop** command). To restart the service, use the **service perfigo restart** or **reboot** command from a command shell. The software upgrade pages now also display how many upgrades have been done, and the list of upgrades and logs from each. Upgrade Logs are the same as a stdout from a manual upgrade, and Upgrade Details display a list of actions performed by the upgrade for the purpose of customer support troubleshooting.

This new feature results in the following enhanced pages in the web admin console:

- CAM web admin console: **Administration > CCA Manager > System Upgrade**
- CAS (direct access) web admin console: **Administration** > **Software Update**

Automated Daily Database Backups

Starting with 3.5(3), Cisco Clean Access automatically creates daily snapshots of the Clean Access Manager database and preserves the most recent from the last 30 days. It also automatically creates snapshots before and after software upgrades, and before and after failover events. For upgrades and failovers, only the last 5 backup snapshots are kept.

Database Recovery Tool

The Database Recovery tool is a new command line utility (3.5.3+) that can be used to restore the database from the following types of backup snapshots:

- Automated daily backups (the most recent 30 copies)
- Backups made before and after software upgrades
- Backups made before and after failover events
- Manual snapshots created by the administrator via the web console

Although the web console already allows you to manually create and upload snapshots (via **Administration** > **Backup**), the CLI tool presents additional detail. The tool provides a menu that lists the snapshots from which to restore, and the uncompressed size and table count. Note that a file which is corrupt or not in the proper format (e.g. not .tar.gz) will show a remediation warning instead of an uncompressed size and a table count.

Once the administrator confirms the restore, the database is replaced with the chosen snapshot.

Caution The CAM must be stopped before you can run this utility and must be rebooted after the utility is run.

To run the command utility:

1. Access your Clean Access Manager by SSH.
2. Login as user `root` with the root password (default password is `cisco123`)
3. Cd to the directory of the database recovery tool: `cd /perfigo/dbscripts`
4. Run `service perfigo stop` to stop the Clean Access Manager.
5. Run `./dbbackup.sh` to start the tool.
6. Follow the prompts to perform database restore.

7. Run `reboot` to reboot the Clean Access Manager after running the utility.

Support Logs

There are two new **Support Logs** web console pages for the CAM and CAS to facilitate TAC support when a customer has issues. The **Support Logs** page allows 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 these support logs when sending their customer support request.

This feature results in the following new pages in the web admin console:

- **Administration** > **CCA Manager** > **Support Logs**
- **Device Management** > **CCA Servers** > **IPaddress** > **Misc** > **Support Logs**

Enhancements for Release 3.5(3)

This section details enhancements to existing features delivered with release 3.5(3) of the Cisco Clean Access Manager and Cisco Clean Access Server.

- Upgrade Script Enhancements
- Dynamic AV Definition Checks
- Supported AV Product List (Version 9)
- Clean Access Agent (3.5.3)

See also New Features in Release 3.5(3), page 34 for additional details. For configuration details, refer to the product documentation.

Upgrade Script Enhancements

The upgrade script for release 3.5(3) now enables direct upgrades to 3.5(3) from 3.2(x) and 3.3(x) in addition to 3.4(x), and previous 3.5(x) releases. See Installing or Upgrading to a New Software Release, page 97 for specific instructions.

Dynamic AV Definition Checks

Cisco Clean Access flexibly allows multiple versions of the Clean Access Agent to be used on the network. Each new version of the Clean Access Agent adds support for the latest AV products as these products are released. With release 3.5(3) of Cisco Clean Access, the system picks the best method to execute AV definition checks based on the AV product support at the time of execution.

This dynamic AV definition checking means the Clean Access Manager will now decide at runtime, based on the supported AV product list, whether to use the virus definition date or version to execute AV Rule checks. This frees the customer from having to reconfigure AV rules when the check method changes based on updates to the AV support chart.

Previous to 3.5(3), the use of virus definition date or version in executing checks for AV Definition Rules was determined at the time of rule configuration. This required customer reconfiguration of AV Rules when checking methods changed with the supported AV product list updates.

Because Cisco Clean Access allows concurrent use of multiple Agent versions, a new page has been added to web console that details AV product/version support per Clean Access Agent version. It is intended to help the administrator pinpoint AV product version support in order to troubleshoot failed AV definition requirements on clients in environments where multiple Agent versions are deployed.

Note that you must configure Mandatory Agent upgrade on clients to ensure latest AV product support.

Warning **For 3.5(3), to ensure proper functioning of enhanced features such as AV product support, Clean Access Agent Auto-update must be set to Mandatory (i.e. "Current Clean Access Agent Patch is a mandatory upgrade") under Device Management > Clean Access > Clean Access Agent > Distribution. Failure to do so may cause these features to fail.**

The dynamic AV definition check feature results in the following enhancements to the web admin console:

- **Device Management** > **Clean Access Agent** > **Rules** > **Agent-AV Support Info** (new page)
- **Device Management** > **Clean Access Agent** > **Rules** > **New AV Rule** (version/date information previously on this page is moved to new **Agent-AV Support Info** page)

AV Support Changes

Note New installations or upgrades to release 3.5(3) do not have the following issue.

Customers running release 3.5(0), 3.5(1), or 3.5(2) who configured AV Definition Update Rules for the following products will need to perform a Clean Update to get the latest AV product list and reconfigure any existing AV definition rules based on these products:

- Computer Associates eTrust EZ Antivirus 6.1.x (Windows XP/2000/ME/98)
- Computer Associates eTrust EZ Armor 6.1.x (Windows XP/2000/ME/98)
- Panda Antivirus 6.0 Platinum (Windows XP/2000)
- Sophos Anti-Virus version3.80 (Windows XP/2000)

You can perform a **Clean Update** under **Device Management** > **Clean Access** > **Clean Access Agent** > **Updates** to get the latest Supported AV Product list.

AV virus definition rules are not supported for Computer Associates eTrust EZ Antivirus 6.1.x and eTrust EZ Armor 6.1.x products (although AV installation rules are supported). AV virus definition rules for the specified Panda and Sophos products are supported but require a Clean Update of the supported AV list to correct the version numbering information and a reconfiguration of any existing rules for these products.

See Supported AV Product List Versions, page 72 for details.

Supported AV Product List (Version 9)

Version 9 of the Supported AV list resolves a number of bugs including McAfee Engine 9.x version fix (CSCei46351) and BitDefender definition date issue (CSCei46336). See the following for details:

- Resolved Caveats - Release 3.5(3), page 89
- Clean Access Supported Antivirus Product List, page 64 for the Supported AV Product List as of the latest release.

- Supported AV Product List Versions, page 72 for details on each version of the list.

Clean Access Agent (3.5.3)

Version 3.5.3 of the Clean Access Agent incorporates support for the multi-hop L3 deployment feature.

VPN/L3 access from the Clean Access Agent is only supported with the 3.5.3 (or above) Agent.

In order for clients to discover the Clean Access Server when they are one or more L3 hops away, the 3.5.3 (or above) Clean Access Agent must be initially installed by being downloaded from the CAS. This can be done in two ways:

- From the Download Clean Access Agent web page (i.e. via web login)
- By client auto-upgrade to the 3.5.3 Agent. For this work, you must be running 3.5(3) on your CAM and CAS, and clients must have the 3.5.2 or 3.5.1 Agent already installed.

Either method provides clients with the CAM information needed for subsequent logins when users are one or more L3 hops away from the CAS. Acquiring and installing the 3.5.3 Agent by other means than direct download from the CAS (for example, Cisco Downloads) will not provide the necessary CAM information to the Agent and will not allow those Agent installations to operate in a multi-hop Layer 3 deployment.

See Clean Access Agent Enhancements, page 52 for further details.

Note In 3.5.3, the “Current Clean Access Agent Patch is a mandatory upgrade” option under **Device Management > Clean Access > Clean Access Agent > Distribution** is enabled by default.

Warning **To ensure proper functioning of enhanced features such as AV product support, Clean Access Agent Auto-update must be set to Mandatory (i.e. “Current Clean Access Agent Patch is a mandatory upgrade“) under Device Management > Clean Access > Clean Access Agent > Distribution. Failure to do so may cause these features to fail.**

Enhancements for Release 3.5.2.2

Release 3.5.2.2 is a general and important bug fix release and patch for the Clean Access Server. No new features are added.

The 3.5.6 Clean Access Agent uncovered a hidden bug in the SWISS (CAS discovery) implementation on the Clean Access Server which caused the 3.5.6 Agent not to be able to log into 3.5(4) and prior CASes. This patch resolves this issue and allows 3.5.6 and above Agents to log in. See Resolved Caveats - Release 3.5.2.2, page 91, and Clean Access Agent Enhancements, page 52 for details.

Note

- The 3.5.2.2 patch is a mandatory patch for all 3.5(2) systems. All customers on 3.5(2) should apply this patch to their Clean Access Servers.
- This patch will run only on 3.5(2) systems.
- The patch is a tar ball that must be applied to the CAS(es) only.
- You must reboot the machine after applying the patch.

Upgrade Instructions for 3.5.2.2

Use the steps below to apply the 3.5.2.2 patch to each Clean Access Server in your system.

Step 1 Download the **cas-3.5.2-to-3.5.2.2-upgrade.tar.gz** patch file to your local computer from the 3.5.2 folder under http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.5.2.

Step 2 Use one of the following sets of instructions to upgrade your CAS(es):

- To upgrade via SSH, use Upgrade Instructions for 3.5.2.2 CAS Patch via SSH, page 40.
- To upgrade an HA CAS pair, see Upgrading High Availability Pairs, page 107.

Upgrade Instructions for 3.5.2.2 CAS Patch via SSH

Use the following steps to apply the 3.5.2.2 patch to each Clean Access Server in your system:

Step 1 Open an SSH terminal and copy the `cas-3.5.2-to-3.5.2.2-upgrade.tar.gz` patch file into the /store directory on each Clean Access Server.

Step 2 Change directory to /store on each machine:

```
cd /store
```

Step 3 Untar the patch file on each machine:

```
tar xzvf cas-3.5.2-to-3.5.2.2-upgrade.tar.gz
```

Step 4 Cd to the upgrade directory:

```
cd cca_upgrade_3.5.2.2
```

Step 5 Execute the patch on each machine:

```
./UPGRADE.sh
```

Step 6 Reboot each machine:

```
reboot
```

Enhancements for Release 3.5.2.1

This section describes enhancements for the 3.5.2.1 release and patch for the Cisco Clean Access Manager:

- Overview
- 3.5.2.1 Update/Upgrade Matrix
- Supported AV Product List (Version 8)
- Upgrading from 3.5(2) to 3.5.2.1

For additional details, see also Clean Access Agent Enhancements, page 52 and Supported AV Product List Versions, page 72. For configuration details, refer to the product documentation.

Overview

Release 3.5.2.1 is a general and important bug fix release and patch for the Clean Access Manager. No new features are added. If you are running release 3.5(2) and using ANY AV definition rules, install the 3.5.2.1 patch. Without the patch, you will not be able to get updates of vendors' definition version/date for ANY definition rules by Update or Auto-Update. You will only be able to get the definition version/date update for ANY definition rules by performing periodic Clean Updates. Note that version-specific (non-ANY) AV definition rules and other checks and rules are not affected.

For further details, see:

- 3.5.2.1 Update/Upgrade Matrix, page 42—for details on the upgrade.
- Resolved Caveats - Release 3.5(3), page 89—for a description of the issue fixed with this release.
- Upgrade via Web Console (from 3.5.3 and Above Only), page 101—for general upgrade instructions. Note the following:
  - You can only upgrade to 3.5.2.1 from 3.5(2).
  - Download the **cam-3.5.2-to3.5.2.1-upgrade.tar.gz** patch file from the 3.5.2 folder under http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.5.2
  - The **cam-3.5.2-to3.5.2.1-upgrade.tar.gz** patch is applied only to the Clean Access Manager.
  - Instead of rebooting the machine, you may simply restart the service by issuing the **service perfigo restart** command.
- Known Issues for Release 3.5(2), page 44—If, prior to updating to Version 8 of the supported AV list, you created AV Definition Update Rules in release 3.5(0), 3.5(1), 3.5(2) (or 3.5.2.1) for Symantec ME/98 and Computer Associates XP/2000/ME/98, you must update to Version 8 of the supported AV list and reconfigure these rules before they can be used. It is recommended to do this prior to upgrading to 3.5.2.1. Note that this issue does not affect **new** AV Definition Update rules that are created **after** updating to Version 8 of the supported AV list.

3.5.2.1 Update/Upgrade Matrix

Table 5 explains what action is needed depending on the version of Clean Access being run.

Table 5 Software Release and AV Definition Rule Matrix

If Running Release	And Using AV Definition Rules for	Required Action
3.5(1)	ANY Antivirus Vendor	**Action:** Upgrade to 3.5(2) to fix issue CSCei10529. ANY Antivirus Vendor definition rules will always fail for AV products for which "version" is used in the virus definition check. **Note** This issue does not affect ANY AV *installation* rules. This issue does not affect Symantec (Norton) products or AV products for which "date" is used in the virus definition file check. For these products, the ANY Antivirus Vendor definition rule successfully detects virus definition updates on the client.
	Specific product version of: • Symantec (ME/98) • Computer Associates (XP/2000/ME/98)	**Action:** Update to Version 8 of the supported AV list to get the correct definition checks for these products, then reconfigure vendor-specific AV definition rules you created for Symantec ME/98 (if created prior to AV list Version 7) or Computer Associates XP/2000/ME/98 (if created prior to AV list Version 8). This affects 3.5(0), 3.5(1), 3.5(2), 3.5.2.1.
3.5(2)	ANY Antivirus Vendor or ANY product version for a specific vendor	**Action:** Upgrade to 3.5.2.1 if using or planning to use ANY AV definition rules.
	Specific product version of: • Symantec (ME/98) • Computer Associates (XP/2000/ME/98)	**Action:** Update to Version 8 of the supported AV list to get the correct definition checks for these products, then reconfigure vendor-specific AV definition rules you created for Symantec ME/98 (if created prior to AV list Version 7) or Computer Associates XP/2000/ME/98 (if created prior to AV list Version 8). This affects 3.5(0), 3.5(1), 3.5(2), 3.5.2.1.

Supported AV Product List (Version 8)

- See Clean Access Supported Antivirus Product List, page 64 for the Supported AV Product List as of the latest release.
- See Supported AV Product List Versions, page 72 for details on each version of the list.

Upgrading from 3.5(2) to 3.5.2.1

Release 3.5.2.1 was a general and important interim bug fix release and patch to be installed on the 3.5(2) Clean Access Manager only. If running release 3.5(2), and using ANY AV definition rules, install the 3.5.2.1 patch. See Enhancements for Release 3.5.2.1, page 41 and 3.5.2.1 Update/Upgrade Matrix, page 42 for further details.

Note

- You can only upgrade to 3.5.2.1 from 3.5(2).
- The **cam-3.5.2-to3.5.2.1-upgrade.tar.gz** patch is applied only to the Clean Access Manager.
- Instead of rebooting the machine, you may simply restart the service by issuing the **service perfigo restart** command.

To upgrade from Cisco Clean Access Manager 3.5(2) to 3.5.2.1 follow the instructions below:

Step 1 Download the **cam-3.5.2-to3.5.2.1-upgrade.tar.gz** patch file to your local computer from the 3.5.2 folder under http://www.cisco.com/cgi-bin/tablebuild.pl/cleanaccess-3.5.2.

Step 2 Copy the .tar.gz file to the /store directory on the Clean Access Manager.

Step 3 Unzip the file with the following command:

```
tar zxvf <filename>
```

Step 4 Run the following command:

```
sh ./<filename.sh>
```

Step 5 After this has completed, issue the following command:

```
service perfigo restart
```

Enhancements for Release 3.5(2)

This section describes enhancements for the 3.5(2) release:

- Licensing Changes
- AV Enhancements
- Supported AV Product List (Version 7)
- Clean Access Agent (3.5.2)

Licensing Changes

As of release 3.5(2), customers with Out-of-Band (OOB) licenses can add In-Band (IB) Clean Access Servers to the Clean Access Manager. Note that you must have an OOB license to enable Out-of-Band features and Clean Access Servers.

AV Enhancements

If an AV Definition Update requirement with “ANY” vendor is used, then only the first AV product in the discovered AV list is updated. Hence, if a machine has multiple AV products installed, all the AV products are detected but only the first AV product will be updated. Note that the “ANY” feature is mainly intended to support the validation of machines with a single AV product installed where the vendor is unknown (e.g. guest access, visitor access), as opposed to situations with a single machine having more than one AV installed.

In 3.5(1) when mapping AV Definition Update requirements to rules on the Rules-Requirement page, only AV definition rules for the applicable vendor were shown. This meant AV definition rules could only be mapped to the AV Definition Update requirement type. The AV Definition Update requirement allows the user to update client virus definition files via the Clean Access Agent by clicking the "Update" button when the requirement is not met (virus definition files are not up-to-date). In 3.5(2), the Rules-Requirement page displays all rules by applicable client operating system only and does not filter out non-AV definition rules for the AV Definition Update requirement type. This allows mapping AV definition rules to other requirement types (such as File or Link Distribution) in cases where AV definition update will not be performed directly via the Agent on the client. Note that AV installation rules continue to be mapped to Link Distribution, File Distribution, or Local Check requirement types.

See also Supported AV Product List Versions, page 72 for further details.

Supported AV Product List (Version 7)

- See Clean Access Supported Antivirus Product List, page 64 for the Supported AV Product List as of the latest release.
- See Supported AV Product List Versions, page 72 for details on each version of the list.

Clean Access Agent (3.5.2)

Version 3.5.2 of the Clean Access Agent clarifies some messages in the installation setup dialogs from 3.5.1. The 3.5.2 Clean Access Agent also incorporates the auto-upgrade feature (available as of release 3.5.1). When Auto-Upgrade is configured in the Clean Access Manager, clients running the 3.5.1 Agent can automatically upgrade to the 3.5.2 Agent. See Clean Access Agent Enhancements, page 52 for additional details.

Known Issues for Release 3.5(2)

If you created AV Definition Update Rules in release 3.5(0) or 3.5(1) (whether ANY or vendor-specific) for the following vendors and client operating systems, after upgrading to release 3.5(2), you will need to edit and save such rules before they can be used. This issue does not affect **new** AV Definition Update rules that are created **after** updating to version 8 of the supported AV list.

Note that this only affects AV definition updates for the specified vendor and client OS.

- Computer Associate AV Definition Update Rules (Windows XP/2000/ME/98)
- Norton AV Definition Update Rules (Windows ME/98 only)

See caveat CSCei10529, page 93 for details. See also Supported AV Product List Versions, page 72

New Features in Release 3.5(1)

This section details new additional features delivered with release 3.5(1) of the Cisco Clean Access Manager and Cisco Clean Access Server.

- Clean Access Agent Auto-Upgrade (3.5.1)
- Clean Access Agent Displays VPN Information (3.5.1)
- Login Session Limit
- Ability to Assign Original VLAN to Authenticated/Certified Devices on Out-of-Band Ports

- Ability to Specify Complex Auth Server Mapping Rules

For configuration details, refer to the product documentation.

Clean Access Agent Auto-Upgrade (3.5.1)

With release 3.5(1), Cisco Clean Access introduces easy, on-the-fly auto-upgrade of deployed Clean Access Agent client software. Whenever a newer version of the Agent is available, the running Clean Access Agent informs the user and automatically performs the upgrade, relieving the administrator and end-user of the chore of manually downloading the new Agent, uninstalling the previous Agent, and installing the new Agent. The Clean Access Manager (CAM) automatically fetches new Agent updates (or Agent patches, bug fixes, and so on) from a centralized remote site and automatically deploys the updated Agent to all the managed Clean Access Servers (CASs) without administrator intervention. In addition, administrators can make the Agent upgrades mandatory (end-user has no choice but to update) or optional (end-user can choose to upgrade immediately or later).

Note Cisco Clean Access 3.5(1) must be installed on the CAM and CAS, and Cisco Clean Access Agent 3.5.1 must be installed on the client to start using the Auto-Upgrade feature. Although 3.5.0 and prior Clean Access Agent versions are compatible with release 3.5(1) of Cisco Clean Access, the Auto-Upgrade feature is not enabled until the 3.5.1 Clean Access Agent is installed on the client.

Once version 3.5.1 of the Clean Access Agent is installed on clients, it will automatically detect when a Agent upgrade is available (3.5.2 or above), download the Agent upgrade from the Clean Access Server, and upgrade itself on client systems. Users will see a confirmation prompt to start the auto-upgrade — OK (mandatory upgrade), or Yes (non-mandatory upgrade)

To upgrade from 3.5.0 or below, users must manually install the Agent. However, the new installer for the 3.5.1 Agent makes the process simpler for users than before and does not need to be executed twice (once to remove, second time to install). The 3.5.1 installer auto-detects if a previous version of the Clean Access Agent is installed, removes the old version and installs the new version in one pass. It is also capable of shutting down the previous version of the application if it is running on the client during upgrade. See Upgrading Agent to 3.5.1 for further details.

The new Auto-Upgrade feature results in the following enhancements to the web admin console:

- The **Device Management > Clean Access > Clean Access Agent > Distribution** page now displays the mandatory/optional client auto-upgrade option.
- The **Device Management > Clean Access > Clean Access Agent > Updates** now displays the Clean Access Agent version and the “check for automatic update” option.

The Clean Access Agent installs to C:\Program Files\Cisco Systems\Clean Access Agent\ on the client.

See Clean Access Agent Enhancements, page 52 for additional details.

Clean Access Agent Displays VPN Information (3.5.1)

The Clean Access Agent now displays the same VPN information that is currently available to VPN-connected web login users via the logout page. When an Optional or Enforce VPN Policy is configured for the Clean Access Server (CAS) and/or user role, VPN information appears in a separate dialog to Clean Access Agent users. The VPN Info dialog is available both from a link in the Successful Login dialog, and by right-clicking the “Show VPN Info” option from the system tray taskbar menu.If available, VPN server, IPSec Key, PPP ID, and PPP Key information will be displayed.

Login Session Limit

This new feature allows administrators to limit the number of login sessions per user ID to a configured maximum for the user role. If the user exceeds this limit, the user is alerted on the web login page or Clean Access Agent dialog and prompted to remove the oldest session before re-logging in. A warning message “Too many users using this account” appears and the user can either log in as a different user or check an option to remove the oldest user login session.

This new feature results in the following enhancements to the web admin console:

- The “Max Sessions per User Account” option is now available from **User Management > User Roles > New Role** or **Edit Role**.

Ability to Assign Original VLAN to Authenticated/Certified Devices on Out-of-Band Ports

This new feature allows administrators to switch Out-of-Band clients back to the initial VLAN after authentication and certification of a device. The initial VLAN is the value saved for the port by the Clean Access Manager when the switch is added. Instead of specifying an Access VLAN, the client is switched from the initial VLAN to an Auth VLAN for authentication and certification, then switched back to the initial VLAN when the client is certified.

This new feature results in the following enhancements to the web admin console:

- “Switch Initial VLAN” is now a dropdown option under **Switch Management > Profiles > Port > New** and **Edit** pages and appears under the **Access VLAN** column on the **List** page when selected.
- The **Switch Management > Devices > Switches > List > Ports** configuration page now displays Initial VLAN and Current VLAN columns, as well as “Reset initial VLANs for ALL ports” and “Set initial VLANs for NEW ports” buttons at the bottom of the page.

Ability to Specify Complex Auth Server Mapping Rules

This new feature allows the administrator to specify complex boolean expressions when defining mapping rules for Kerberos, LDAP, and RADIUS authentication servers. You can use boolean expressions to combine multiple user attributes and multiple VLAN IDs to map users to user roles. Mapping rules can be created for a range of VLAN IDs, and attribute matches can be made case-insensitive. This allows multiple conditions to be flexibly configured for a mapping rule.

This new feature results in the following enhancements to the web admin console:

- The Add Mapping Rule / Edit Mapping Rule pages are considerably changed under **User Management > Auth Servers > Mapping Rules**.

Enhancements for Release 3.5(1)

This section describes enhancements for release 3.5(1) of the Cisco Clean Access Manager and Cisco Clean Access Server.

- Upgrade Script Enhancement
- Event Log Simplified for Rule Auto-Updates
- Clean Access Agent Rule Categorization
- Enhancement to AV Definition Rules and Requirements
- Supported AV Product List (Version 6)
- Supported Out-of-Band Switches List Updated

Upgrade Script Enhancement

The 3.5 upgrade script is now modified to perform 3.5(1) upgrades and 3.4(x) upgrades. The upgrade script also incorporates a DHCP script which regenerates all ARP entries upon upgrade. This DHCP script is an upgrade-time enhancement to account for a resolved caveat (CSCeh31769) that might have caused deletion of some DHCP-related ARP entries from the database in certain cases.

Event Log Simplified for Rule Auto-Updates

With 3.5(1), checks and rules modified from auto-update are condensed into a single event log entries. This enhancements results in following modification to the web admin console:

- **Monitoring > Event Logs > View Logs**

Clean Access Agent Rule Categorization

Display and usability is improved by categorizing the display of rules on the Clean Access Agent rule and requirement configuration pages. The UI is made more intelligent by only showing AV definition rules when displaying AV definition requirements.

Enhancement to AV Definition Rules and Requirements

Starting with version 3.5.1 of the Clean Access Agent, there is a new “ANY” Antivirus Vendor category available on the configuration pages for New/Edit AV Rule and New/Edit AV Definition Update Requirement. This enhancement allows the administrator to create a single AV definition rule to check for antivirus definition files for any supported vendor. Additionally, you can now select “ANY” Antivirus Vendor when configuring an AV Definition Update requirement. When mapping AV definition rules to an AV Definition Update requirement configured for ANY vendor, this displays the “ANY” vendor AV definition rules as well as those configured for individual vendors and products. Note that while AV definition rules are mapped to AV Definition Update requirements, AV installation rules are mapped to requirements of type Link Distribution, File Distribution, or Local Check.

This enhancement results in the following modifications to the web admin console:

- On **Device Management > Clean Access > Clean Access Agent > Rules > New AV Rule**, there is now an **ANY** option on the Antivirus Vendor dropdown, and under “Checks for Selected Operating System” when a particular AV Vendor is chosen.

- On **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement**, there is now an **ANY** option in the Antivirus Vendor Name dropdown list for the AV Definition Update requirement type.
- On **Device Management > Clean Access > Clean Access Agent > Requirements > Requirements-Rules**, when choosing an AV Definition Update requirement for which "ANY" Antivirus Vendor is configured, all supported AV definition rules for the selected OS will display.

See also Clean Access Supported Antivirus Product List, page 64.

Supported AV Product List (Version 6)

- See Clean Access Supported Antivirus Product List, page 64 for the Supported AV Product List as of the latest release.
- See Supported AV Product List Versions, page 72 for details on each version of the list.

Supported Out-of-Band Switches List Updated

Support for the Cisco Catalyst 3560 switch is now added for release 3.5(1) OOB. See Supported Switches for Cisco Clean Access, page 4.

New Features in Release 3.5(0)

This section details the new features delivered with release 3.5(0) of the Cisco Clean Access Manager and Cisco Clean Access Server.

- Switch Control-Based Out-of-Band (OOB) Product Module
- Anti-Virus Software Integration
- SNMP Agent Monitoring Services
- FlexLM Integration

For configuration details, refer to the product documentation.

Switch Control-Based Out-of-Band (OOB) Product Module

With release 3.5, Cisco Clean Access expands its capabilities to provide a choice of out-of-band deployment and/or traditional in-band deployment. The Cisco Clean Access Manager (CAM) can manage both in-band Clean Access Servers and out-of-band Clean Access Servers at the same time, as well as switches used for out-of-band deployment.

This is a new product offering that requires the purchase of an Out-of-Band (OOB) Clean Access Server (CAS). When you import an OOB CAS license following the purchase of an OOB CAS, the CAM web admin console automatically displays an additional module menu for **Switch Management**.

In the Cisco Clean Access in-band solution, the CAS is deployed inline with user traffic. The CAS can be deployed in Virtual Gateway configuration between the layer 2 and layer 3 devices on the network edge, or in Real-IP Gateway or NAT Gateway configuration as the first layer-3 hop at the network edge. Inline deployment has the advantage of providing fine-grained control of user traffic, access, and bandwidth.

If it is preferable not to deploy the CAS inline with user traffic after client assessment and certification, the new Cisco Clean Access Out-of-Band (OOB) product provides customers with three additional deployment modes: out-of-band Virtual Gateway, out-of-band Real-IP Gateway, and out-of-band NAT Gateway. With out-of-band deployment, user traffic is directed to the CAS only during the process of initial authentication, posture assessment, and remediation. Following the certification of the device based on the network access policy, user traffic no longer flows through the CAS until the time that the user machine needs to be authenticated/certified again.

Out-of-band deployment is achieved by using the CAM to control switches on the network edge using SNMP. SNMP v1, v2c and v3 are supported for maximum compatibility and security. The CAM uses SNMP to assign/change the VLAN setting on switch ports thereby routing the traffic to the CAS or away from the CAS as needed.

Currently, the OOB product includes support for the following Cisco switches:

- Catalyst 2950
- Catalyst 3550
- Catalyst 3750
- Catalyst 450x
- Catalyst 650x

For further details, see Supported Switches for Cisco Clean Access, page 4.

In addition to the new **Switch Management** module, the new OOB product results in the addition of the following three new Server Types in the Add New Server page of the web admin console (**Device Management > CCA Servers > New Server**):

- Out-of-Band Virtual Gateway
- Out-of-Band Real-IP Gateway
- Out-of-Band NAT Gateway

The new OOB product also results in the addition of an Out-of-Band Users list in the **Monitoring > Online Users > View Online Users > Out -of-Band** page on the web admin console. The Out-of-Band Users list contains a list of all the users that authenticated to the network through an Out-of-Band Clean Access Server.

For details, see Chapter 4, “Switch Management and Cisco Clean Access Out-of-Band (OOB)” of the *Cisco Clean Access Manager Installation and Administration Guide, Release 3.5*.

Anti-Virus Software Integration

With release 3.5, Cisco Clean Access expands and adds new Clean Access Agent-based support for the detection of Anti-Virus (AV) software and subsequent checking of AV application status and virus definition status. This is achieved through communicating with the installed AV software (if there is any installed AV software) through an API on the client device.

This new mode of direct communication between the Clean Access Agent and the AV software allows Cisco Clean Access to support many more AV vendors and versions and also enables the Agent to perform auto-update of AV virus definitions for several supported AV products. The hourly updates of Cisco Clean Access checks/rules now reflects the latest published virus definitions of most AV vendors including Symantec, McAfee, TrendMicro, Sophos Panda, Softwin (BitDefender) and others. For further details, see Clean Access Supported Antivirus Product List, page 64.

The new AV integration results in the following enhancements to the web admin console:

- The Rule Updates link is removed and replaced by the **Device Management** > **Clean Access** > **Clean Access Agent** > **Updates** page.
- There is a **New AV Rule** page under **Device Management** > **Clean Access** > **Clean Access Agent** > **Rules** > **New AV Rule**.
- There is a new Requirement Type, **AV Definition Update**, under **Device Management** > **Clean Access** > **Clean Access Agent** > **Requirements** > **New Requirement** or **Edit Requirement**.

For details, see the “Clean Access Agent” chapter of the *Cisco Clean Access Manager Installation and Administration Guide, Release 3.5*.

SNMP Agent Monitoring Services

New SNMP monitoring support in release 3.5 (**Monitoring** > **SNMP**) enables the Cisco Clean Access Manager to be monitored from an existing SNMP manager such as HP OpenView, Sun Enterprise Manager, and others. It also provides the capability for the Clean Access Manager to alert the SNMP manager through SNMP traps. However, note that for non-basic monitoring / reporting / configuration / management, the administrator will still have to use the web admin console of the Clean Access Manager.

For details, see the “Monitoring” chapter of the *Cisco Clean Access Manager Installation and Administration Guide, Release 3.5*.

FlexLM Integration

Release 3.5 introduces a new licensing mechanism based on the industry leading FlexLM license manager product. This allows for the support of flexible licensing schemes.

Release 3.5 also introduces a new license status page in the web admin console (**Administration** > **CCA Manager** > **Licensing**) which allows administrators to install licenses, view the set of features associated with FlexLM licenses, and remove all FlexLM licenses.

For details, see the “Introduction” and “Administration” chapters of the *Cisco Clean Access Manager Installation and Administration Guide, Release 3.5*.

Enhancements from Release 3.4

This section describes enhancements to features from release 3.4 that are delivered with release 3.5(0) of the Cisco Clean Access Manager and Cisco Clean Access Server.

- RADIUS Accounting Enhancements
- Network Scanning Enhancements
- Clean Access Agent Configuration Enhancements
- Clean Access Agent Dialog Enhancements (3.5.0)
- Clean Access Server Proxy Settings

RADIUS Accounting Enhancements

RADIUS Accounting is modified in release 3.5 so that the Clean Access Manager sends a Start accounting message on user login and a Stop accounting message on user logout (instead of sending Accounting-on and Accounting-off messages).

RADIUS Accounting has been made highly configurable in release 3.5 (**User Management** > **Auth Servers** > **Accounting**). Prior to this release, RADIUS accounting was limited both in the information that was sent to the accounting server, and the formatting of that information. Release 3.5 greatly improves this by allowing the administrator to configure the kinds of events/data to be sent to the accounting server on user login/logout. It also allows the administrator to customize the formatting of that information to suit specific needs.

For details, see the "User Management: Auth Servers" chapter of the *Cisco Clean Access Manager Installation and Administration Guide, Release 3.5*.

Network Scanning Enhancements

The **Device Management** > **Network Scanner** > **Scan Setup** > **Test** page is enhanced with a **Show Log** button that brings up a debug log for the target computer tested (sourced from /var/nessus/logs/nessusd.messages). The log shows which plugins were executed, the results of the execution, which plugins were skipped and the reason (dependency, timeout, etc). Administrators can check this log to debug why a scan result is not as expected.

The "Automatic Update" option under **Device Management** > **Network Scanner** > **Plugin Updates** is removed. Due to a licensing requirement by Tenable, Cisco will no longer be able to bundle pre-tested Nessus plugins or automated plugin updates to Cisco Clean Access, effective Release 3.3.6/3.4.1. Customers can still download Nessus plugins selectively and manually through http://www.nessus.org. For details on Nessus plugin feeds, see http://www.nessus.org/plugins/index.php?view=feed.

For details, see the "Network Scanning" chapter of the *Cisco Clean Access Manager Installation and Administration Guide, Release 3.5*.

Clean Access Agent Configuration Enhancements

The Clean Access Manager automatically publishes the Clean Access Agent to all Clean Access Servers. As a result, the "Select Clean Access Servers to Publish the Clean Access Agent" checkbox is removed from **Device Management** > **Clean Access** > **Clean Access Agent** > **Distribution.**

Verification of Clean Access Agent rules and requirements is now performed automatically and the "Verify All" button and "Verify" icon next to each entry in the Clean Access Agent Rule List and Requirement List have been removed and replaced with a **Validity** column which displays the integrity status of the rule or requirement. Blue checks in the column indicate the rule or requirement is valid and red crosses indicate the rule or requirement needs to be reconfigured. Highlighting either icon with the mouse pointer displays the validity message.

The following pages of the web administration console are modified accordingly:

- **Device Management** > **Clean Access** > **Clean Access Agent** > **Rules** > **Rule List**
- **Device Management** > **Clean Access** > **Clean Access Agent** > **Requirements** > **Requirement List**

For details, see the "Clean Access Agent" chapter of the *Cisco Clean Access Manager Installation and Administration Guide, Release 3.5*.

Clean Access Agent Dialog Enhancements (3.5.0)

The taskbar menu for the Clean Access Agent is modified to enable the **Login** option only if a Clean Access Server is detected by the Agent. If a CAS is not detected, the Agent does not allow the user to attempt a login.

For details, see Clean Access Agent Enhancements, page 52 and 3.5.0 Agent and Below, page 62. See also the "Clean Access Agent" chapter of the *Cisco Clean Access Manager Installation and Administration Guide, Release 3.5*.

Clean Access Server Proxy Settings

You can configure additional ports (for example, 3128, 8080, 8000, 6588, 3382, 3127) from which to redirect proxied HTTP requests to the login page from **Device Management** > **Clean Access Servers** > **IPaddress** > **Advanced** > **Proxy**.

For details, see Chapter 4, "Clean Access Server Managed Domain" of the *Cisco Clean Access Server Installation and Administration Guide, Release 3.5*.

Clean Access Agent Enhancements

This section provides information for the Clean Access Agent client software:

- Enhancements per Agent Version
- VPN/L3 Access for Clean Access Agent (3.5.3+)
- Clean Access Agent Auto-Upgrade (3.5.1+)
- Agent Setup vs. Agent Upgrade Files
- Auto-Upgrade Compatibility
- Upgrading Agent to 3.5.1
- Manually Uploading the Agent to the CAM

Enhancements per Agent Version

Table 6 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 later versions. See also Software Compatibility Matrixes, page 4 for additional details.

Table 6 Clean Access Agent Versions

Agent Version	Feature / Enhancement
3.5.13	• Resolves caveat CSCsd84272 (Trend Micro). See Resolved Caveats - Release 3.5(10), page 80. • Enhancements for AV Rule (XP/2000) support. See Supported AV Product List Versions, page 72. See also Clean Access Agent Enhancements (3.5.13), page 12.
3.5.12	• Resolves caveat CSCsd53315 (F-Secure). See Resolved Caveats - Release 3.5(10), page 80. • Enhancements for AV Rule (XP/2000) support. See Supported AV Product List Versions, page 72. See also Clean Access Agent Enhancements (3.5.12), page 12.

Table 6 Clean Access Agent Versions

Agent Version	Feature / Enhancement
3.5.11	• Resolves a variety of caveats. • 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 Resolved Caveats - Release 3.5(9), page 80, Enhancements for Release 3.5(9), page 12, and Known Issue for Symantec/Norton Products (3.5.11), page 13
3.5.10	Resolves caveats CSCsc44051 (antivirus) and CSCsc44335 (uninstall) See Resolved Caveats - Release 3.5(8), page 82 and Enhancements for Release 3.5(8), page 14.
3.5.9	• Enhancements for AV Rule support • With 3.5(7) CAM/CAS, 3.5.9 Agent can enable/ disable Agent logging off from the Clean Access network when a user logs off from the Windows domain or shuts down a Windows workstation. This feature does not apply for OOB deployments. **Important Notes:** • 3.5.7 and below Agent will leave the Agent logged in when machine is shut down. • 3.5.8 A gent will log out user when machine is shutdown or user logs off. • 3.5.9 Agent combined with 3.5(7) CAM/CAS will make this option configurable. See also Enhancements for Release 3.5(7), page 16.
3.5.8	• Enhancements for AV Rule support • For in-band configurations, the Agent now attempts logoff from Clean Access network prior to Windows user logout (Start->Shutdown->Log off current user) or Windows shutdown (Start->Shutdown->Shutdown machine). This feature does not apply to OOB deployment. **Note** The Clean Access system log-off attempt may be unsuccessful if the Agent is terminated by Windows prior to successfully logging off from Clean Access . **Important Notes:** • 3.5.8 A gent will log out user when machine is shutdown or user logs off. • Release 3.5(6) provides a new disable to prevent upgrade notifications (mandatory or optional) to 3.5.1+ Agent users when an Agent update becomes available on the CAM. See Disabling Agent Patch Upgrade Distribution to Users, page 57. See also Enhancements for Release 3.5(6), page 20.
3.5.7	Enhancement for AV Rule support (McAfee Enterprise 8.0 virus def updates; see caveat CSCsb79391, page 86). **Important Notes:** • 3.5.6/3.5.7 Agents are only compatible with 3.5.5/3.5.4.1/3.5.3.2/3.5.2.2 CAM/CAS. • 3.5.7 and below Agents leave the Agent logged in when machine is shut down. See Clean Access Agent Feature Compatibility Matrix, page 7.

Table 6 Clean Access Agent Versions

Agent Version	Feature / Enhancement
3.5.6	3.5.6 Agent optimizes discovery in multi-hop L3 deployments for release 3.5(5) **Important Notes:** 3.5.6/3.5.7 Agents are only compatible with 3.5.5/3.5.4.1/3.5.3.2/3.5.2.2 CAM/CAS. For further details, see: • Clean Access Agent Feature Compatibility Matrix, page 7 • Enhancements for Release 3.5.4.1, page 28 • Enhancements for Release 3.5.3.2, page 32 • Enhancements for Release 3.5.2.2, page 40
3.5.5	• Agent behavior is changed to send proprietary encrypted UDP-based protocol to the CAM (instead of HTTP) to discover the CAS. • CAM web console now has enable/disable L3 option for the CAS (requires update and reboot) • Agent installer now installs by default for all users on a client PC instead of only the current user. See Enhancements for Release 3.5(5), page 24 and VPN/L3 Access for Clean Access Agent (3.5.3+), page 56. **Important Notes:** 3.5.5+ Agents only support multi-hop L3 operation with 3.5(5)+ CAM/CAS. L3 discovery will not work with older CAM/CAS versions.
3.5.4	Agent now checks for newer Agent upgrades at every login request instead of at application startup. See Enhancements for Release 3.5(4), page 29.
3.5.3	• 3.5(3) and above CAM/CAS/Agent support multi-hop L3 deployment and VPN/L3 access with Single Sign-On (SSO). See VPN/L3 Access for Clean Access Agent (3.5.3+), page 56 for details. • 3.5(3)+ CAM/CAS new installs set mandatory Agent Auto-Upgrade by default (software upgrades maintain previous settings). See Enabling Mandatory Auto-Upgrade on the CAM, page 58. **Important Notes:** 3.5.1/3.5.2/3.5.3 Agents check for auto-upgrade only at Agent restart or client reboot.
3.5.2	Agent clarifies some messages in the installation setup dialogs (from 3.5.1). See Enhancements for Release 3.5(2), page 43. **Important Notes:** 3.5.1/3.5.2/3.5.3 Agents check for auto-upgrade only at Agent restart or client reboot.

Table 6 Clean Access Agent Versions

Agent Version	Feature / Enhancement
3.5.1	- Agent supports Auto-Upgrade with 3.5(1) or above installed of CAM/CAS/Agent. See Clean Access Agent Auto-Upgrade (3.5.1+), page 57 - Agent displays available VPN information (VPN server, IPSec Key, PPP ID, and PPP Key) when an Optional or Enforce VPN Policy is configured for the CAS and/or user role. The VPN Info dialog is available both from a link in the Successful Login dialog, and by right-clicking the "Show VPN Info" option from the system tray taskbar menu. **Important Notes:** - Actual upgrade to 3.5.1 requires manual install of the Agent. See Upgrading Agent to 3.5.1 for further details. - 3.5.1/3.5.2/3.5.3 Agents check for auto-upgrade only at Agent restart or client reboot.
3.5.0	Agent taskbar menu only enables the **Login** option if a CAS is detected by the Agent. **Important Notes:** - Users upgrading to 3.5.0 Agent (or prior versions of the SmartEnforcer), must select **Remove** and not Repair when prompted by the installer. The user then needs to go back and double-click the Setup.exe file to install the newer version. See 3.5.0 Agent and Below, page 62 for further details. - SmartEnforcer 3.2.x is not supported with Cisco Clean Access release 3.5(x). You must upgrade to 3.5.x Agent to use it with CAM/CAS 3.5(x).

VPN/L3 Access for Clean Access Agent (3.5.3+)

Releases 3.5(3) and above of the CAM/CAS/Agent introduce support for multi-hop L3 deployment. VPN/L3 access from the Clean Access Agent is only supported with the 3.5.3+ Agent.

Starting with release 3.5(3)+ of the CAM/CAS/Agent, the Agent will:

1. Check the client network for the Clean Access Server (same as previous versions), and if not found,
2. Send IP traffic to the Clean Access Manager (new behavior for 3.5.3+) if the Agent has the runtime IP address information of the CAM.

In order for clients to discover the CAS when they are one or more L3 hops away, clients must initially download the 3.5.3+ Agent from the CAS (via download web page or auto-upgrade). Either method allows the Agent to acquire the IP address of the CAM in order to send traffic to the CAM/CAS over the L3 network. Once installed in this way, the Agent can be used for both L3/VPN concentrator deployments or regular L2 deployments.

Acquiring and installing the 3.5.3+ Agent on the client by means other than direct download from the CAS (e.g. from Cisco Downloads) will not provide the necessary CAM information to the Agent and will not allow those Agent installations to operate in a multi-hop Layer 3 deployment.

To support VPN/L3 Access, you must:

- Be running 3.5(3) or above CAM/CAS/Agent.
- For 3.5(**5**) or above CAM/CAS, you must check the option for “Enable L3 Support for Clean Access Agent” and perform an Update and Reboot under **Device Management > CCA Servers > Manage [IP address] > Network > IP**. See New Enable/Disable L3 Option on CAS, page 24 for additional details.

Note 3.5.5+ Agents only support multi-hop L3 operation with 3.5(5)+ CAM/CAS. L3 discovery will not work with older CAM/CAS versions.

- There must be a valid **CAS Discovery Host** under **Device Management > Clean Access > Clean Access Agent > Distribution** (set by default to the trusted IP address of the CAM).
- Clients must initially download the 3.5.3+ Agent from the CAS, in one of two ways:
  - “Download Clean Access Agent” web page (i.e. via web login)
  - Auto-Upgrade to 3.5.3 or above Agent. You must be running 3.5(3) or above CAM/CAS, and clients must have 3.5.1 or above Agent already installed (see Clean Access Agent Auto-Upgrade (3.5.1+), page 57 for details).
- SSO is only supported when integrating Cisco Clean Access with the Cisco VPN Concentrator (3000 series, release 4.7)

Note

- Uninstalling a 3.5.3+ Agent while still on the VPN connection does not terminate the connection.
- For VPN-concentrator SSO deployments, if the 3.5.3+ Agent is not downloaded from the CAS and is instead downloaded by other methods (e.g. Cisco Downloads), the Agent will not be able to get the runtime IP information of the CAM and will not pop up automatically nor scan the client.
- If a 3.5.0 or prior version of the Agent is already installed, or if the 3.5.3+ Agent is installed through non-CAS means (e.g. Cisco Downloads), you must perform web login to download the 3.5.3+ Agent setup files from the CAS directly and reinstall the Agent to get the L3 capability.

Clean Access Agent Auto-Upgrade (3.5.1+)

Auto-Upgrade of the Agent is available starting with release 3.5(1) of the CAM/CAS/Agent.

Once the 3.5.1+ Agent is installed on clients, it automatically detects when an Agent upgrade is available (3.5.2+), downloads the upgrade from the CAS, displays a user confirmation prompt, and upgrades itself on the client. Administrators can make Agent Auto-Upgrade mandatory or optional for users.

With upgrade to 3.5(6) CAM/CAS, the Clean Access Agent Distribution page provides a "**Do not offer current Clean Access Agent Patch to users for upgrade**" option to prevents upgrade notifications to all 3.5.1+ users (mandatory or optional), when an Agent update becomes available on the CAM. Enabling this option in effect prevents distribution of the Agent Patch upgrade to users when a newer Agent is downloaded to the CAM.

Note You must be running 3.5(1) or above on the CAM/CAS and the 3.5.1 Agent must be installed on the client to use the Auto-Upgrade feature. Although 3.5.0 and prior Agent versions are compatible with 3.5(1)+ CAM/CAS, Auto-Upgrade is not enabled until the 3.5.1+ Agent is installed on the client.

This section describes the following:

- Enabling Agent Auto-Upgrade on the CAM
- Disabling Agent Patch Upgrade Distribution to Users
- Enabling Mandatory Auto-Upgrade on the CAM
- User Experience for Auto-Upgrade
- Uninstalling the Agent

Enabling Agent Auto-Upgrade on the CAM

To enable Auto-Upgrade of the Clean Access Agent on clients, you must:

1. Be running 3.5(1) or above CAM/CAS/Agent.
2. Require use of the Clean Access Agent for the role and client OS (from **Device Management** > **Clean Access** > **General Setup**)
3. Retrieve the latest version of the Agent Upgrade patch from **Device Management** > **Clean Access** > **Clean Access Agent** > **Updates** (click **Update** to get the Agent Upgrade and all Cisco Updates)

Note For mandatory or optional auto-upgrade, the latest Agent patch (3.5.2+) must be downloaded to the CAM via Updates, or 3.5.1+ users will not be prompted to upgrade to the newer Agent.

Disabling Agent Patch Upgrade Distribution to Users

With the 3.5(6)+ CAM/CAS, you can disable notification (therefore distribution) of the Agent Patch upgrade to users as follows:

1. Upgrade your CAM/CAS to release 3.5(6) or above.
2. Go to **Device Management** > **Clean Access** > **Clean Access Agent** > **Distribution**
3. Click the checkbox for "**Do not offer current Clean Access Agent Patch to users for upgrade**."
4. Click **Update**.

Enabling Mandatory Auto-Upgrade on the CAM

New installs of the 3.5(3)+ CAM/CAS automatically enable mandatory Auto-Upgrade by default. For CAM/CAS upgrades, the current setting (enabled or disabled) will be carried over to the upgraded system. To enable/disable mandatory Agent Auto-Upgrade for all users:

1. Make sure you have the latest Agent Upgrade patch (see Enabling Agent Auto-Upgrade on the CAM, page 57).
2. Go to **Device Management > Clean Access > Clean Access Agent > Distribution**. The page displays the most current Agent Setup and Agent Upgrade versions (see Agent Setup vs. Agent Upgrade Files, page 59 for details.)
3. Check (to enable) or uncheck (to disable) the option for "**Current Clean Access Agent Patch is a mandatory upgrade**."
4. Click **Update**.

⚠ **Caution** To ensure proper functioning of enhanced features such as AV product support, Clean Access Agent Auto-Upgrade must be set to Mandatory (i.e. "Current Clean Access Agent Patch is a mandatory upgrade“) under Device Management > Clean Access > Clean Access Agent > Distribution. Failure to do so may cause these features to fail.

User Experience for Auto-Upgrade

With Agent auto-upgrade (and patch distribution) enabled in the CAM, the user experience is as follows:

- New users download and install the newest version of the Agent after the initial one-time web login.
- In-Band (IB) users with 3.5.4+ Agent installed will be prompted to auto-upgrade at login.
- Out-of-Band (OOB) users with 3.5.4+ Agent installed must be on the Authentication VLAN to be prompted to auto-upgrade at login.
- IB users with 3.5.1/3.5.2/3.5.3 Agent installed must exit the application from the taskbar menu and restart the Agent from the Desktop shortcut to be prompted to auto-upgrade the Agent. When the user clicks OK (mandatory upgrade), or Yes (non-mandatory upgrade) the client will automatically install the newer version of the Agent.
- OOB users with 3.5.1/3.5.2/3.5.3 Agent installed must do the following to auto-upgrade the Agent:
  - Be on the Authentication VLAN
  - Exit the application from the taskbar menu and restart the Agent from the Desktop shortcut.
- For users with Agents older than 3.5.1, see Upgrading Agent to 3.5.1, page 61 for how to upgrade.

Uninstalling the Agent

The Clean Access Agent can be uninstalled on the client from either:

- Start Menu > Programs > Cisco Systems > Cisco Clean Access > Uninstall Clean Access Agent, or
- Start Menu > Control Panel > Add or Remove Programs > Clean Access Agent

The 3.5.1+ Agent installs to C:\Program Files\Cisco Systems\Clean Access Agent\ on the client.

The 3.5.0 Agent installs to C:\Program Files\Cisco\Clean Access\ on the client.

(Version 3.3 and below of the SmartEnforcer install to C:\Program Files\Perfigo\SmartEnforcer\)

Agent Setup vs. Agent Upgrade Files

Clean Access Agent Auto-Upgrade (3.5.1 and above) introduces a distinction between the Agent Setup version and the Agent Upgrade (or Patch) version of the client installation files. These reflect the two installers of the same Agent that are used under different conditions:

- Agent Setup Installer
  Used for fresh installs on clients that do not have a previous version of the Agent already installed. Users download the Agent Setup file from the “Download Clean Access Agent” page after an initial one-time web login.
- Agent Upgrade (or Patch) Installer
  Downloaded by an already-installed Clean Access Agent (i.e. older version) to upgrade itself. Users are prompted to download the Agent Upgrade file after user login (3.5.4+) or after restart of the Agent or PC reboot (3.5.1/3.5.2/3.5.3).

Loading Agent Installation Files to the CAM

The Agent Setup or Upgrade file is placed on the CAM as described below. Once either of these files is in the CAM, it can be published to the Clean Access Servers, then distributed to clients/users.

Agent Setup

The Agent Setup is the complete Agent Setup installation file that comes with the Clean Access Manager software release. It is not distributed by Internet updates. It can only be:

1. Installed from the CAM CD along with the CAM
2. Installed by a CAM Upgrade
3. Installed by manually uploading CCAAgentSetup.tar.gz to the CAM via the web console.
   For details, see Manually Uploading the Agent to the CAM, page 62.

Agent Upgrade

The Agent Upgrade (or Patch) can only be:

1. Installed from the CAM CD (from 3.5.3 onwards) along with the CAM
2. Installed by a CAM Upgrade (from 3.5.3 onwards)
3. Installed by Cisco Updates from the Internet (via **Device Management** > **Clean Access** > **Clean Access Agent** > **Updates**)

Auto-Upgrade Compatibility

The newest version of the Clean Access Agent Setup Installation file and Upgrade (Patch) installation file is automatically included with the CAM software for each Cisco Clean Access software release.

Every major and minor version of the Clean Access Agent is intended to have basic compatibility with the same major and minor version of the server product. For example:

- 3.5(x) Agent works with 3.5(x) CAS/CAM
- 3.4(x) Agent works with 3.4(x) CAS/CAM
- 3.3(x) Agent works with 3.3(x) CAS/CAM

Basic compatibility means the Agent is able to perform basic functions such as login, logout, look for configured requirements, and report vulnerabilities.

In addition, new versions of the Clean Access Agent may add additional functionality (e.g. L3 discovery) or additional AV Rule support in conjunction with updates to the Supported Antivirus Product List (e.g. support for new AV product ClamWin).

Note

- 3.5.5 and above Agents are only compatible with 3.5(5) and greater CAM/CAS or 3.5.2.2 / 3.5.3.2/ 3.5.4.1 patches of the CAS.
- 3.5.5+ Agents only support multi-hop L3 operation with the 3.5(5)+ CAM/CAS. L3 discovery will not work with older CAM/CAS versions. See Web Browser Compatibility, page 8.

Higher Versions

Release 3.5.1 and above of the CAM/CAS/Agent support Agent Auto-Upgrade, which allows the CAM to pull down the Agent Upgrade version via Updates from the Internet. In this case, any 3.5(1)+ CAS/CAM can pull down any latest 3.5.x Upgrade release of the Agent if it is also 3.5.1+.

By design, the system will typically support Agent versions that are higher than the CAM/CAS version as the result of Agent auto-upgrade, minus any added features that are non-AV related. For example, if the CAM/CAS are running 3.5(1), and a user auto-upgrades to the 3.5.3 Agent, the user would have support for the latest AV products (e.g. Symantec 10.x) but the L3/VPN feature would not be supported as this requires a 3.5(3) CAM/CAS.

Note Do not install a 3.6.x.x Agent on a 3.5(x) CAM/CAS.

Note that the 3.5.3 Agent user on the 3.5(1) CAM/CAS in this case will have the same AV support as if on a 3.5(3) CAM/CAS, because the AV support is tied to the version of the Supported AV Product List and Agent, rather than the CAM/CAS version.

Note AV Rule support may entail major and minor version compatibility restrictions. For example, the 3.5.0 Agent supports the Supported Antivirus Product List, but does not support “ANY” vendor/product AV rules/requirements, as this is a feature of 3.5.1 and above Agents.

Lower Versions

Where possible, some software releases may provide basic compatibility with older Agent versions, for example, release 3.5(3) supports the 3.4.1 Agent. In this case, the older Agent can perform the basic functions for the CAS/CAM on the new software release, but cannot support the new features such as AV Rules. Refer to the Software Compatibility Matrixes, page 4 for details on which Agent versions support which specific platform features.

Upgrading Agent to 3.5.1

To upgrade to 3.5.1 or above from 3.5.0 Agent and Below, users must manually install the Agent. However, the 3.5.1 installer does not need to be executed twice (once to remove, second time to install). The 3.5.1 installer auto-detects if a previous Agent version is installed, removes the old version and installs the new version in one pass. It also shuts down the previous version of the application if it is running on the client during upgrade.

You can have users upgrade from previous versions of the Clean Access Agent to version **3.5.1** in several ways, including:

- CD install
  Distribute the setup executable (.exe) to users via CD.
- Web login/ download Clean Access Agent
  Inform all users to perform web login, which will redirect users to the Clean Access Agent download page if Agent use is required for that user role and client OS.
- Create a File Distribution requirement that distributes the newest 3.5.x setup executable
  This last method is described in Agent Upgrade Through File Distribution Requirement.

Agent Upgrade Through File Distribution Requirement

The following steps show how to create a software package requirement to enforce download and installation of the Clean Access Agent (3.5.1+) for users in a specified user role. Users in the role will be required to download and install the required package (in this case, the Agent setup file) before they can log onto the network.

Note For this procedure (requirement for clients) the .exe file is uploaded.

Step 1 Log into the Clean Access Agent download page on http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml and download the CCAAgentSetup-3.5.x.tar.gz file to an accessible location on your machine (replace the *.x* in the filename with the applicable version number).

Note If you want to enable VPN/L3 capability for your users later via auto-upgrade to 3.5.3 or above, make sure you only download the 3.5.1 or 3.5.2 Agent here. Distributing a 3.5.3+ Agent downloaded from Cisco Downloads via File Distribution Requirement will not enable clients to acquire the CAM IP information that enables VPN/L3 capability.

Step 2 Untar the file (change the *.x* in the filename respectively):

```
> tar xzvf CCAAgentSetup-3.5.x.tar.gz
```

Step 3 The CCAA folder will contain the **CCAAgent_Setup.exe** file.

Step 4 On the CAM web admin console, go to **Device Management** > **Clean Access** > **Clean Access Agent** > **Rules** > **New Check**. Create a Registry Check (Type: Registry Value) that checks for a Version later than 3.5.(x-1) in the registry of the client (HKLM\SOFTWARE\Cisco\Clean Access Agent\). For example, if you want to distribute 3.5.1, make the registry check look for a Version later than 3.5.0. Make sure to select “Automatically create rule based on this check” in addition to a client OS for the check/rule.

Step 5 Go to **Device Management > Clean Access > Clean Access Agent > Requirements > New Requirement**. Create a File Distribution requirement, browse to the CCAA folder, and upload the untarred **CCAAgent_Setup.exe** file in the “File to Upload” field. Make sure to select a client OS, and type a requirement name and instructions for the user.

Step 6 Select your Agent upgrade requirement and map it your registry check rule under **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement-Rules**.

Step 7 Select your Agent upgrade requirement and map it to user roles under **Device Management > Clean Access > Clean Access Agent > Requirements >Role- Requirements**.

Step 8 Make sure to add traffic policies to the Temporary user role to allow HTTP and HTTPS access to only the IP address of your Clean Access Manager. This allows clients to download the setup executable file.

Step 9 Test as a user. If all is correctly configured, you will be able to download, install, and login with the 3.5.x Clean Access Agent.

3.5.0 Agent and Below

Users with new installs of the 3.5.0 Agent (from web download) will see the “Welcome to the Clean Access Agent Setup Wizard” dialog the first time they Run the Setup.exe file.

Users who upgrade to the 3.5.0 Clean Access Agent (from prior versions of the Agent or SmartEnforcer) must select the **Remove** option and not the Repair option when prompted by the installer. The user should then follow the installer dialogs to remove the old version. Once the old version is removed, the user needs to go back to the download location of the installer Setup.exe file and double-click this executable again to install the newer version of the Agent. At this point the upgrade user sees the “Welcome to the Clean Access Agent Setup Wizard” dialog.

The setup wizard installs the Clean Access Agent to C:\Program Files\Cisco\Clean Access\ on the client.

Note SmartEnforcer 3.2.x is not supported with Cisco Clean Access 3.5(x). If you are currently running SmartEnforcer 3.2.x, you will need to upgrade to the 3.5.x Agent to use it with the 3.5(x) CAM/CAS.

Manually Uploading the Agent to the CAM

When performing a software upgrade to the CAM and CAS, it is not necessary to upload the installation file for the Clean Access Agent since it is automatically included with the CAM software. However in certain cases, it is possible to manually upload the Clean Access Agent Setup installation file to the CAM directly, for example, if you are not performing a CAM/CAS software upgrade but need to upgrade the version of the Agent to be distributed to clients. (See Software Compatibility, page 4 for details.)

The CAM will automatically publish the Agent Setup file to the connected CAS(es) when the Agent Setup file is uploaded manually. There is no version check while publishing, so the Agent Setup can be downgraded or replaced.

The following steps describe how to manually upload the Agent setup file to the CAM.

Caution With release 3.5(1) and above, you must upload the Clean Access Agent installation setup file as a **tar.gz** file (without untarring it) to the CAM. Make sure you do NOT extract the .exe file before uploading.

Step 1 Log into the Clean Access Agent download page on http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml and download the CCAAgentSetup-3.5.x.tar.gz file to an accessible location on your machine (replace the .x in the filename with the applicable version number).

Step 2 Go to **Device Management** > **Clean Access** > **Clean Access Agent** > **Distribution**.

Step 3 In the **Clean Access Agent Setup to Upload** field, click **Browse**, and navigate to the folder where the Clean Access Agent installation file is located.

Step 4 Select the .tar.gz file and click **Open**. The name of the file should appear in the text field.

Step 5 In the **Version** field, type the version of the Agent to be uploaded (for example, 3.5.2). The Version you enter should be the same as the version for the .tar.gz file, and should be in the form "x.y.z".

Step 6 Click **Upload**.

Clean Access Supported Antivirus Product List

This section describes the Supported Antivirus Product List that is downloaded to the Clean Access Manager via **Device Management** > **Clean Access** > **Clean Access Agent** > **Updates** to support AV integration in release 3.5. The Supported Antivirus Product List is a versioned XML file distributed from a centralized update server that provides the most current matrix of supported AV vendors and product versions used to configure AV Rules and AV Definition Update requirements.

The Supported AV list contains information on which AV 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 list ensures your AV rule configuration pages list all the new products supported in the new Agent.

Note Cisco recommends that you keep your Supported Antivirus 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."

Note For 3.5(x), if you have auto-updates enabled on your CAM, and have downloaded the latest version of the Supported AV List prior to downloading the corresponding version of the CCA Agent Upgrade Patch, make sure to perform a **Clean Update** to enable the latest product support for that version of the Agent.

The following charts summarize the AV product/version support per client OS as of the latest Cisco Clean Access release:

- Supported AV Products (Windows XP / 2000), page 65
- Supported AV Products (Windows ME / 98), page 70

For details on what is added per version of the Supported AV Product List, see:

- Supported AV Product List Versions, page 72

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

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

Note Where possible, it is recommended to use AV Rules mapped to AV Definition Update Requirements when checking antivirus software on clients. In the case of a non-supported AV product, or if an AV product/version is not available through AV Rules, administrators always have the option of using Cisco provided pc_ checks and pr_rules for the AntiVirus 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 Manager Installation and Administration Guide, Release 3.5* for configuration details.

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

Supported AV Products (Windows XP / 2000)

Table 7 lists Windows XP/2000 Supported AV Products as of the latest release of the Cisco Clean Access software. (See Table 8 for Windows ME/98).

Table 7 Cisco Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 49, Release 3.5(11) and 3.5.13 Agent (Sheet 1 of 5)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Virus Definition	
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
ClamWin				
ClamWin Antivirus	0.x	yes (3.5.2)	yes (3.5.2)	yes
ClamWin Free Antivirus	0.x	yes (3.5.4)	yes (3.5.4)	yes
Computer Associates International, Inc.				
CA eTrust Antivirus	7.x	yes (3.5.0)	yes (3.5.0)	yes
eTrust EZ Antivirus	6.1.x	yes (3.5.3)	yes (3.5.8)	yes
eTrust EZ Antivirus	6.2.x	yes (3.5.0)	yes (3.5.0)	yes
eTrust EZ Antivirus	6.4.x	yes (3.5.0)	yes (3.5.0)	yes
eTrust EZ Antivirus	7.x	yes (3.5.0)	yes (3.5.0)	yes
eTrust EZ Armor	6.1.x	yes (3.5.0)	yes (3.5.8)	yes
eTrust EZ Armor	7.x	yes (3.5.0)	yes (3.5.0)	yes
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-Secure Corp.				
F-Secure Anti-Virus	5.x	yes (3.5.0)	yes (3.5.0)	yes
F-Secure Internet Security 2006 Beta	6.x	yes (3.5.8)	yes (3.5.8)	yes
Grisoft, Inc.				
Antivirussystem AVG 6.0	6.x	yes (3.5.0)	yes (3.5.0)	-
AVG 6.0 Anti-Virus - FREE Edition	6.x	yes (3.5.0)	yes (3.5.0)	-
AVG 6.0 Anti-Virus System	6.x	yes (3.5.0)	yes (3.5.0)	-

Table 7 Cisco Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 49, Release 3.5(11) and 3.5.13 Agent (Sheet 2 of 5)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Virus Definition	
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 Free Edition	7.x	yes (3.5.0)	yes (3.5.0)	yes
H+BEDV Datentechnik GmbH				
AntiVir/XP	6.x	yes (3.5.0)	yes (3.5.0)	-
Kaspersky Labs				
Kaspersky Anti-Virus 2006 Beta	6.0.x	yes (3.5.8)	yes (3.5.8)	-
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(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
McAfee, Inc.				
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 Internet Security 6.0	8.x	yes (3.5.4)	yes (3.5.4)	yes
McAfee Managed VirusScan	3.x	yes (3.5.8)	yes (3.5.8)	yes
McAfee 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 (3.5.1)	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 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
Panda Software				
Panda Antivirus 6.0 Platinum	6	yes (3.5.0)	yes (3.5.0)	yes
Panda Antivirus Lite	1.x	yes (3.5.0)	yes (3.5.0)	-
Panda Antivirus Lite	3.x	yes (3.5.9)	yes (3.5.9)	-
Panda Antivirus Platinum	7.04.x	yes (3.5.0)	yes (3.5.0)	yes
Panda Antivirus Platinum	7.05.x	yes (3.5.0)	yes (3.5.0)	yes

Table 7 Cisco Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 49, Release 3.5(11) and 3.5.13 Agent (Sheet 3 of 5)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Virus Definition	
Panda Antivirus Platinum	7.06.x	yes (3.5.0)	yes (3.5.0)	yes
Panda Platinum 2005 Internet Security	9.x	yes (3.5.3)	yes (3.5.3)	yes
Panda Platinum Internet Security	8.03.x	yes (3.5.0)	yes (3.5.0)	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 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
SalD Ltd.				
Dr.Web	4.32.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)	-
Sophos Plc.				
Sophos Anti-Virus	3.x	yes (3.5.3)	yes (3.5.3)	-
Sophos Anti-Virus	5.x	yes (3.5.3)	yes (3.5.3)	yes
Sophos Anti-Virus version 3.80	3.8	yes (3.5.0)	yes (3.5.0)	-
Symantec Corp.				
Norton AntiVirus 2003	9.x	yes (3.5.0)	yes (3.5.0)	yes
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
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 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

Table 7 Cisco Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 49, Release 3.5(11) and 3.5.13 Agent (Sheet 4 of 5)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Virus Definition	
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 SystemWorks 2003	6.x	yes (3.5.3)	yes (3.5.3)	yes
Norton SystemWorks 2004 Professional	7.x	yes (3.5.4)	yes (3.5.4)	yes
Norton SystemWorks 2005	8.x	yes (3.5.3)	yes (3.5.3)	yes
Norton SystemWorks 2005 Premier	8.x	yes (3.5.3)	yes (3.5.3)	yes
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 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)	-
Trend Micro Antivirus	11.x	yes (3.5.0)	yes (3.5.0)	yes
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 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)	-
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 7 Cisco Clean Access Antivirus Product Support Chart (Windows XP/2K) Version 49, Release 3.5(11) and 3.5.13 Agent (Sheet 5 of 5)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		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.

Supported AV Products (Windows ME / 98)

Table 8 lists Windows ME/98 Supported AV Products as of the latest release of the Cisco Clean Access software. (See Table 7 for Windows XP/2000.)

Table 8 ***Cisco Clean Access Antivirus Product Support Chart (Windows ME/98) Version 49, Release 3.5(11) and 3.5.13 Agent (Sheet 1 of 2)***

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		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 8 *Cisco Clean Access Antivirus Product Support Chart (Windows ME/98) Version 49, Release 3.5(11) and 3.5.13 Agent (Sheet 2 of 2)*

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		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.

Supported AV Product List Versions

Table 9 details enhancements made per version of the Supported Antivirus Product List. See Clean Access Supported Antivirus Product List, page 64 for the latest Supported AV list as of the latest release. See New and Changed Information, page 9 to return to the features list per release.

Table 9 Supported AV Product List Versions

Version	Enhancements
Release 3.5(11) —3.5.13 Agent	
Version 49, 48, 47, 46, 45, 44, 43, 42, 41, 40	Minor internally used data changes.
Release 3.5(10)—3.5.13 Agent	
Version 39	**AV Chart (Windows XP/2000/ME/98):** Removed virus def version support for CA eTrust Antivirus 7.x (def date used instead).
Version 38	Minor internally used data change,
Version 37	**AV Chart (Windows XP/2000):** Added Live Update support for Trend Micro OfficeScan Client 5.x, 6.x and 7.x
Release 3.5(10) —3.5.12 Agent	
Version 36, 35, 34	Minor internally used data changes.
Version 33	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):** Adds support to the 3.5.12 Agent for the following new products: • Ahnlab V3Pro 2004, 6.x (def date support) • AOL Safety and Security Center Virus Protection, 1.x • BitDefender 9 Internet Security AntiVirus, 9.x • CA eTrustITM Agent, 8.x • Dr.Web, 4.33.x • F-Prot for Windows, 3.16x • F-Secure Anti-Virus 5.44 (resolves caveat CSCsd53315). • Microsoft Windows OneCare Live, 0.8.x • Rising Antivirus Software AV, 17.x • Rising Antivirus Software AV, 18.x • Trend Micro Client/Server Security Agent, 7.x **AV Chart (Windows ME/98) —** No changes
Version 30	**AV Chart (Windows XP/2000)**—Adds support for Norton AntiVirus 2006, 12.x
Version 29	Minor internally used data change.

Table 9 Supported AV Product List Versions (continued)

Version	Enhancements
Version 28	No changes to AV support charts for 3.5.x Agents.
Version 27	Minor internally used data change.
Release 3.5(9) —3.5.11 Agent	
Version 26	**AV Chart (Windows XP/2000)**—Adds support for the following new products: • CA eTrust Internet Security Suite AntiVirus, 7.x • F-Prot for Windows, 3.16c • F-Prot for Windows, 3.16d • Kaspersky Anti-Virus Personal Pro, 5.0.x • WebAdmin Client Antivirus, 3.x **AV Chart (Windows ME/98) —** No changes
Version 25, 24, 23, 23, 21	No changes to AV support charts for 3.5.x Agents.
Release 3.5(8) —3.5.10 Agent, **Release 3.5(7) —3.5.9 Agent**	
Version 20	**Windows XP/2000**—Adds support for Panda Antivirus Lite, 3.x **Windows ME/98**—Adds support for Symantec AntiVirus Client, 8.x **Windows XP/2000**—Removes support for: • Sereniti Security Suite 1.x • The River Home Network Security Suite 1.x
Version 19	**Windows XP/2000**—Adds def version support for: • AVG Anti-Virus 7.0, 7.x • AVG Antivirensystem 7.0, 7.x • AVG Free Edition 7.x
Release 3.5(6) —3.5.8 Agent	

Table 9 Supported AV Product List Versions (continued)

Version	Enhancements
Version 18	**Windows XP/2000**—Adds support for: • F-Secure Internet Security 2006 Beta, 6.x • Kaspersky Anti-Virus 2006 Beta, 6.0.x • McAfee Managed VirusScan, 3.x • BitDefender 8 Free Edition, 8.x • BitDefender 9 Standard, 9.x • BitDefender 9 Professional Plus, 9.x • Trend Micro PC-cillin Internet Security 2006, 14.x **Windows ME/98**—Adds support for : • McAfee Managed VirusScan, 3.x • BitDefender 8 Free Edition, 8.x • BitDefender 9 Standard, 9.x • BitDefender 9 Professional Plus, 9.x • Symantec AntiVirus, 9.x
Release 3.5(5)	
Version 17	**Windows XP/2000**—Adds support for: • Authentium Sereniti Security Suite, 1.x • Eset NOD32 antivirus system, 2.x • ZoneAlarm Anti-virus, 6.x • ZoneAlarm Security Suite, 6.x • Norton AntiVirus 2006, 12.0.x **Windows XP/2000**—Removes support for: • NOD32 antivirus system • NOD32 Antivirus System • NOD32 antivirus System
Version 16	**Windows XP/2000**—Adds support for Trend Micro OfficeScan Client, 6.x
Version 15	**Windows XP/2000**—Removes support for Norton AntiVirus Corporate Edition 7.0 for WindowsNT, 7.x (The Clean Access Agent does not support Windows NT.) **Note** Customers should perform a Clean Update to remove the product from the CAM database and web console.
Version 14	**Windows XP/2000/ME/98**—Adds support for: • Norton AntiVirus 2002, 8.x • Norton Internet Security, 8.x
Version 13	**Windows XP/2000**—Adds support for Norton Internet Security, 8.2.x
Release 3.5(4)	

Table 9 Supported AV Product List Versions (continued)

Version	Enhancements
Version 12	**Windows XP/2000**—Adds support for: • ClamWin Free Antivirus, 0.x • McAfee VirusScan, 10.x • McAfee Internet Security 6.0, 8.x • Norton SystemWorks 2004 Professional, 7.x **Windows ME/98**—Adds support for McAfee VirusScan, 10.x
Version 11	**Windows XP/2000/ME/98**—Set Live Update to "no" for BitDefender Free Edition 7.x
Version 10	**Windows XP/2000**— Sophos Anti-Virus 5.x AV list updated to use virus definition date instead of version for AV definition check. **Note** The 3.5(3) CAM UI displayed this check as unavailable if using version 9 of the supported AV list. There is no impact for other releases.
Release 3.5(3)	
Version 9	Resolves McAfee Engine 9.x version fix (CSCei46351) and BitDefender definition date issue (CSCei46336). See Resolved Caveats - Release 3.5(3), page 89 for details. **Windows XP/2000**—Adds support for 12 new products: • eTrust EZ Antivirus, 6.1.x • Panda Platinum 2005 Internet Security, 9.x • Panda TruPrevent Personal 2005, 2.x • Sophos Anti-Virus, 3.x • Sophos Anti-Virus, 5.x • Symantec AntiVirus, 10.x • Symantec Client Security, 10.x • Norton SystemWorks 2003, 6.x • Norton SystemWorks 2005, 8.x • Norton SystemWorks 2005 Premier, 8.x • Trend Micro OfficeScan Corporate Edition, 7.x • Trend Micro PC-cillin Internet Security 2005, 12.x

Table 9 Supported AV Product List Versions (continued)

Version	Enhancements
	Windows 9x/ME—Adds support for 9 new products: • CA eTrust Antivirus, 7.x • eTrust EZ Armor, 6.1.x • eTrust EZ Antivirus, 7.x • McAfee VirusScan Professional, 8.x • McAfee VirusScan, 8.x • McAfee VirusScan, 9.x • McAfee VirusScan Professional, 9.x • Norton AntiVirus 2003 Professional Edition, 9.x • Trend Micro PC-cillin Internet Security 2005, 12.x • Trend Micro PC-cillin 2005
Release 3.5.2.1	
Version 8	**Windows XP/2000/ME/98**— Computer Associates products. AV list updated to use virus definition date instead of version for AV definition check.
Release 3.5(2)	
Version 7	**Windows XP/2000**—Adds support for new product ClamWin. **Windows ME/98**— Symantec ME/98 products. AV list updated to use virus definition date instead of version for AV definition checks.
Release 3.5(1)	
Version 6	**Windows XP/2000**—Adds support for 7 new product versions to existing vendors McAfee, Panda, Symantec, and Trend Micro.

Caveats

This section describes the following caveats:

- Open Caveats - Release 3.5.11.1, page 78
- Resolved Caveats - Release 3.5.11.1, page 78
- Resolved Caveats - Release 3.5(11), page 79
- Resolved Caveats - Release 3.5(10), page 80
- Resolved Caveats - Release 3.5(9), page 80
- Resolved Caveats - Release 3.5(8), page 82
- Resolved Caveats - Release 3.5(7), page 83
- Resolved Caveats - Release 3.5.6.1, page 83
- Resolved Caveats - Release 3.5(6), page 84
- Resolved Caveats - Release 3.5.5.1, page 84
- Resolved Caveats - Release 3.5(5), page 84
- Resolved Caveats - Release 3.5.4.1, page 86
- Resolved Caveats - Release 3.5(4), page 87
- Resolved Caveats - Release 3.5.3.2, page 88
- Resolved Caveats - Release 3.5.3.1, page 88
- Resolved Caveats - Release 3.5(3), page 89
- Resolved Caveats - Release 3.5.2.2, page 91
- Resolved Caveats - Release 3.5.2.1, page 91
- Resolved Caveats - Release 3.5(2), page 92
- Resolved Caveats - Release 3.5(1), page 93
- Resolved Caveats - Release 3.5(0), page 96

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 3.5.11.1

Table 10 List of Open Caveats

	Software Release 3.5.11.1	
DDTS Number	Corrected	Caveat
CSCsd90433	No	Apache does not start on HA-Standby CAM after heartbeat link is restored.
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.
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 3.5.11.1

Table 11 List of Resolved Caveats

	Software Release 3.5.11.1	
DDTS Number	Corrected	Caveat
CSCsd52349	Yes	Viewing details in Agent reports returns viewer to first page When viewing the CCA Agent report, if the admin clicks on a specific user to view details, the report refreshes back to the first page.

Table 11 List of Resolved Caveats (continued)

DDTS Number	Software Release 3.5.11.1	
	Corrected	**Caveat**
CSCse53459	Yes	Heartbeat module needs to be up before getting peer node status. **Note** Caveat CSCse53459 is not resolved if you upgrade from 3.5(x) to 3.5(11) and from 3.6(x) to 3.6(3) or 4.0(0). **Temporary Workaround**: SSH to the CAM and manually copy the following file: `cp /perfigo/control/bin/perfigo /etc/init.d/perfigo`
CSCsf18821	Yes	Linux-HA Heartbeat Remote Denial of Service 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
CSCsg44268	Yes	Need to accommodate for new daylight saving time regime from 2007 DST is changing to Mar (second sunday) and Nov (first sunday) starting from 2007 instead of Apr and Oct
CSCsg92130	Yes	Windows Vista should not be recognized as Windows NT in 3.5.x and 3.6.x Windows Vista machines should be categorized under “Windows_ALL” instead of “Windows_NT” when users log in.
CSCsh15238	Yes	Memory Leak in Radius Authentication/Accounting Module If you are using a Radius server to perform authentication/accounting functions in your network (set up in either **User Management > Auth Server > Auth Server** or **User Management > Auth Server > Accounting**), a slow memory leak exists that can eventually cause the server to run out of memory.

Resolved Caveats - Release 3.5(11)

Table 12 List of Resolved Caveats

DDTS Number	Software Release 3.5(11)	
	Corrected	**Caveat**
CSCsd59430	Yes	Upgrade summary & detail cannot be viewed on CAS due to missing jsp extension for “perfigo_update” in the hyperlink under Administration > Software Update | “List of Upgrade Logs” or “List of Upgrade Details”
CSCse39644	Yes	Heartbeat timer and the timing out of zero MAC entries from the online user list
CSCse56062	Yes	OOB online users are not deleted when timer removes certified devices

Resolved Caveats - Release 3.5(10)

Table 13 List of Resolved Caveats

	Software Release 3.5(10)	
DDTS Number	Corrected	Caveat
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.
CSCsd53315	Yes	Add support for F-Secure Anti-Virus 5.44 3.5.11 Agent does not currently recognize F-Secure Anti-Virus 5.44. The support for this product needs to be added.
CSCsd84272	Yes	Agent Update button not successfully triggering virus definition file update for TrendMicro OfficeScan Client 5.x, 6.x and 7.x. This problem existed in the 3.5.12 and prior releases for 3.5 agent, 3.6.2.0 and prior releases for 3.6 agent.

Resolved Caveats - Release 3.5(9)

Table 14 List of Resolved Caveats

	Software Release 3.5(9)	
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.

Table 14 List of Resolved Caveats (continued)

	Software Release 3.5(9)	
DDTS Number	**Corrected**	**Caveat**
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.
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 can cause DoS attack **Note** This caveat is resolved with security patch-CSCsc85405, which is included in the 3.5(9) upgrade. The security patch is not required if upgrading to 3.5(9), but is required for all other versions of 3.5(x). For further details, refer to: http://www.cisco.com/en/US/products/ps6128/products_security_notice09186a00805b87a7.html
CSCsc88240	Yes	Users 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 bypass the "Accept/Reject" these terms. Technically, the user never accepted the "Network Usage Terms & Conditions" and was allowed to access the network.
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
CSCsd12491	Yes	CAM sets trunk ports on switch to administratively down ("shut") state

Table 14 List of Resolved Caveats (continued)

	Software Release 3.5(9)	
DDTS Number	**Corrected**	**Caveat**
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.
CSCsd19177	Yes	SNMP trapsink settings are lost after performing upgrade
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.

Resolved Caveats - Release 3.5(8)

Table 15 Resolved Caveats

	Software Release 3.5(8)	
DDTS Number	**Corrected**	**Caveat**
CSCsc18842	Yes	FlexLM licenses are not always removed correctly using the GUI
CSCsc44051	Yes	Clean Access agent 3.5.9 when used with Sophos 5.x causes the Agent to crash.
CSCsc44335	Yes	Uninstall of Agent fails if performed from Start > All Programs > Cisco Systems > Cisco Clean Access > Uninstall Clean Access Agent. However, Agent can still be removed from Add or Remove Programs.
CSCsc47598	Yes	CAM incorrectly categorizes the “access” port as “trunk” port

Resolved Caveats - Release 3.5(7)

Table 16 Resolved Caveats

	Software Release 3.5(7)	
DDTS Number	Corrected	Caveat
CSCsb55488	Yes	CCA - Latest Anti-virus versions are not recognized as valid (unable to authenticate with newest version of AVG antivirus definitions installed) Symptom: McAfee 10.0.25 does not get properly detected by the Cisco Clean Access Agent for installation nor for update rules Conditions: McAfee antivirus 10.0.25; CCA Agent version 3.5.8 or prior; possible other Antivirus signature are also not detected properly. Workaround: Possible workaround of using pr-based signatures.
CSCsc08063	Yes	The SWISS protocol handler on the CAS causes discovery (therefore, authentication) to fail when the CAS receives certain spurious/malformed packets from a client.
CSCsc16424	Yes	In 3.5.5 and 3.5.6 CAM failover setups, synchronization may not occur properly in certain situations due to failed communication between the failover peers.
CSCsc20736	Yes	Daily database backup incorrectly numbers snapshot version
CSCsc29739	Yes	Distribution/Update CAM pages do not respect admin user privileges The Clean Access Agent Distribution page and the Clean Access Agent Rules update pages on the CAM UI do not respect the admin user privileges, i.e. even if the user is a read-only user, it allows the user to modify fields on the page.

Resolved Caveats - Release 3.5.6.1

Table 17 Resolved Caveats

	Software Release 3.5.6.1	
DDTS Number	Corrected	Caveat
CSCsc08063	Yes	The SWISS protocol handler on the CAS causes discovery (therefore, authentication) to fail when the CAS receives certain spurious/malformed packets from a client.
CSCsc16424	Yes	In 3.5.5 and 3.5.6 CAM failover setups, synchronization may not occur properly in certain situations due to failed communication between the failover peers.

Resolved Caveats - Release 3.5(6)

Table 18 Resolved Caveats

DDTS Number	Software Release 3.5(6)	
	Corrected	**Caveat**
CSCsb91210	Yes	McAfee 9.1 Updates on Windows 98/ME do not show up as clean Windows 98/ME devices running Cisco Clean Access 3.5.7 may not show correct clean status for McAfee 9.1 even if the server has it configured. The Agent complains of missing anti-virus software even when rule has been applied correctly.
CSCsb98431	Yes	Manual updates will no longer pull down Agent update files if the option to check for Agent updates is not checked.
CSCsb98484	Yes	It is possible, under certain network conditions, to 'partially' log a user off from CCA. In such situations, the user session is ended at the CAM but is not ended at the CAS. Hence, the CCA Agent shows such users as being logged in when they really are not. **Note** CSCej01028 is a duplicate of this issue.

Resolved Caveats - Release 3.5.5.1

Table 19 Resolved Caveats

DDTS Number	Software Release 3.5.5.1	
	Corrected	**Caveat**
CSCsc08063	Yes	The SWISS protocol handler on the CAS causes discovery (therefore, authentication) to fail when the CAS receives certain spurious/malformed packets from a client.
CSCsc16424	Yes	In 3.5.5 and 3.5.6 CAM failover setups, synchronization may not occur properly in certain situations due to failed communication between the failover peers.

Resolved Caveats - Release 3.5(5)

Table 20 Resolved Caveats

DDTS Number	Software Release 3.5(5)	
	Corrected	**Caveat**
CSCei86991	Yes	Enhancement option to configure both SNMP V1 & SNMP V3 on the CAM. The SNMP Trap Receiver can now accept all versions of notifications (v1/v2c/v3)
CSCej00935	Yes	Agent should stop issuing HTTP thread from sending any more requests after client machine has logged in

Table 20 Resolved Caveats (continued)

	Software Release 3.5(5)	
DDTS Number	**Corrected**	**Caveat**
CSCej01013	Yes	Under some situations, the postgres process does not start correctly because a database lock file is kept around. This is fixed in release 3.5(5).
CSCej01021	Yes	Change the CAS to provide an option to disable the L3 discovery for the agent
CSCsb56270	Yes	Clean Access Agent only respects and displays the auth providers in the login page set for ALL or WINDOWS_ALL operating systems. **Note** This issue is fixed in release 3.5(5). This issue does not affect web login users. When you configure auth providers in user pages for specific Windows OSes rather than ALL or WINDOWS_ALL (e.g. WINDOWS_XP) Clean Access Agent users will not be able to use the auth providers from that page. **Workaround (if not upgrading to 3.5.5):** A default login page must be present to allow all users (web login or Clean Access Agent) to log in. Put all auth providers you want to make available for Agent users in a WINDOWS_ALL login page. To edit the user login page: **1.** Go to Administration > User Pages | Login Page | List **2.** Click the Edit button for the desired login page for Agent users. **3.** Click the General sublink. **4.** Select WINDOWS_ALL from the Operating System dropdown menu. **5.** Click Update. **6.** Click the Content sublink. **7.** Click the checkboxes for Available Providers to allow these auth providers for Agent users. **8.** Make sure you have a Default Provider selected from the dropdown menu. **9.** Click Update.

Table 20 Resolved Caveats (continued)

	Software Release 3.5(5)	
DDTS Number	**Corrected**	**Caveat**
CSCsb65542	Yes	Nessus plugins fail to install Symptom: Trying to install the NESSUS plugins, the browser eventually times out and the plugins are never installed. Workaround: 1. Perform “service perfigo restart” on CAM CLI / or reboot CAM 2. Disconnect all CASes from the CAM GUI 3. Upload plugins from the CAM GUI 4. Reconnect (manage) all CASes from the CAM GUI All steps are required and must be in the above order.
CSCsb72670	Yes	Change L3 HTTP-based discovery to SWISS-based discovery for CAM/CAS
CSCsb72687	Yes	Instead of using the Windows_ALL tag, the Agent should provide complete and accurate O/S information to the CAS. **Note** This is a duplicate of CSCsb56270.
CSCsb74632	Yes	The Switch Management events for notifications received by the CAM from switches are no longer written to event log. Most of the logging is now moved from event log (database) to only /perfigo/logs/perfigo-log0.log.0 by default.
CSCsb74642	Yes	Now, OOB respects entries in the Filters -> Devices list. If devices are entered there, then no clean access policies are applied to it.
CSCsb74650	Yes	RADIUS Accounting Failover now interprets the timeout value in seconds as it should instead of the earlier interpretation (ms).
CSCsb79391	Yes	Cannot update DAT files after upgrading Agent to 3.5.6 **Note** Issue affects 3.5.5/3.5.6 Agent and is fixed with 3.5.7 Agent. Symptom: After upgrading the Agent to 3.5.6, McAfee Enterprise 8.0 updates cannot be installed Workaround: 1. Downgrade to 3.5.4; 2. Take the PC off the clean access network, disable the Agent and then update Mcafee

Resolved Caveats - Release 3.5.4.1

Table 21 Resolved Caveats

	Software Release 3.5.4.1	
DDTS Number	**Corrected**	**Caveat**
CSCsb79166	Yes	Agent 3.5.6 patch breaks client communication to CAS. **Note** This issue resolved by 3.5.4.1, 3.5.3.2,3.5.2.2 CAS patches.

Resolved Caveats - Release 3.5(4)

Table 22 Resolved Caveats

	Software Release 3.5(4)	
DDTS Number	**Corrected**	**Caveat**
CSCei62255	Yes	HTTP 503 Error Users might see "503 Service Unavailable" occasionally when they try to access the login page or admin GUI on both CAS and CAM.
CSCei72195	Yes	In OOB, when "require users to certify at every login" is selected, the action of a user logging out due to a link-down trap being received does not cause the certified device entry to be deleted. This causes subsequent connection attempts to pass through unchallenged. Also, the behavior is not consistent with the in-band version of the product.
CSCsb31070	Yes	Clean Access Agent, GrisSoft AVG version 7 update scanning. If a customer is using AVG version 7, Clean Access Agent will not detect if it has the correct version/update of the virus definition file.
CSCsb45063	Yes	DHCP renew does not work, but DHCP release and renew works Description: When multiple managed subnets are used and the CAS is used as a DHCP server, a DHCP renew from the client does not work and just hangs. However, if you do a DHCP release and then a renew, everything works as it should. A capture of the DHCP packets shows that the DHCP ACK from the CAS is sourced from the trusted interface in the case where it fails and it the case when it works it is sourced from the untrusted interface as it should. Symptom: The CAS DHCP server may not respond from the correct managed subnet when dhcp renew is performed. Workaround: Perform a dhcp /release then /renew, OR Add a new route to the CAS via the 'route add' command: % route add -net 192.168.183.0 netmask 255.255.255.0 fake1 One route needs to be added per managed subnet per affected CAS. Adding a route to the CAS for the subnet will address this issue. e.g: For a managed subnet 192.168.183.0 route add -net 192.168.183.0 netmask 255.255.255.0 eth1 To make sure the route exists after rebooting the CAS create the file /etc/sysconfig/static-routes and add the following line: any net 192.168.183.0 netmask 255.255.255.0 eth1
CSCsb48572	Yes	Authentication enhancement for API JSP.
CSCsb53655	Yes	When there is any floating device configured, no MAC address will be added into the certified device list.

Resolved Caveats - Release 3.5.3.2

Table 23 Resolved Caveats

DDTS Number	Software Release 3.5.3.2	
	Corrected	**Caveat**
CSCsb79166	Yes	Agent 3.5.6 patch breaks client communication to CAS. **Note** This issue resolved by 3.5.4.1, 3.5.3.2,3.5.2.2 CAS patches.

Resolved Caveats - Release 3.5.3.1

Table 24 Resolved Caveats

DDTS Number	Software Release 3.5.3.1	
	Corrected	**Caveat**
CSCei62255	Yes	HTTP 503 Error Users might see "503 Service Unavailable" occasionally when they try to access the login page or admin GUI on both CAS and CAM.

Resolved Caveats - Release 3.5(3)

Table 25 Resolved Caveats

	Software Release 3.5(3)	
DDTS Number	Corrected	Caveat
CSCei11049	Yes	Add server type to List of Server Window Today, the following information is shown in the List of Servers: IP Address | Location | Status | Manage | Disconnect | Reboot | Delete. Server Type should be added to list to reflect OOB and IB servers.

CSCei14927	Yes	Upgrade from 3.5.0.1 to 3.5(2) fails; Integer expression expected
		Problem: Upgrading from Cisco Clean Access version 3.5.0.1 to version 3.5(2) will fail with the following message:
		`sh ./UPGRADE.sh`
		`./UPGRADE.sh: [: 0.: integer expression expected`
		`This package will upgrade from 3.4.x or 3.5.x to 3.5.2.`
		`This server is running 3.5.0.`
		How to determine if you are hitting this bug:
		SSH to the CAM or CAS and view file /perfigo/build. If build version is reported as 3.5.0.1, then you will hit this bug when upgrading. Below is an example of a build file from an affected version.
		`[root@camanager1 perfigo]# cat /perfigo/build`
		`VERSION=3.5.0.1`
		`NAME=Clean Access Manager`
		`DATE=2005/06/02`
		`[root@camanager1 perfigo]#`
		Workaround: Edit the /perfigo/build file, so VERSION line reads as: VERSION=3.5.0.
		After doing this the upgrade should complete successfully.

CSCei29275	Yes	Failover issue when both devices are active If two machines fail over and the failover heartbeat link between them fails, both machines stay active until the administrator manually reboots them. The configuration is either direct connect and/or switches for the heartbeat link.
CSCei32812	Yes	OOB Server limit is not correct if Perfigo-style license is used If a Perfigo-style license key is used with a Server limit (SSSL) set to a positive number (e.g. 3), then it is not possible to add an OOB server. This is because the SecureSmartOBServerLimit (SSSL) is not being set correctly in SmartManagerConf.java. It is not being set but is being used to make a decision.
CSCei35778	Yes	Need documentation for installing CCA 3.5.2.1 To upgrade from Cisco Clean Access Manager 3.5.2 to 3.5.2.1 follow the instructions below: 1) Download the cam-3.5.2-to-3.5.2.1-upgrade.tar.gz file to /store on the server 2) Unzip the file with 'tar zxvf cam-3.5.2-to-3.5.2.1-upgrade.tar.gz' 3) Run 'sh ./cam-3.5.2-to-3.5.2.1-upgrade.sh' 4) After this has completed, issue 'service perfigo restart'

Table 25 Resolved Caveats (continued)

DDTS Number	Software Release 3.5(3)	
	Corrected	**Caveat**
CSCei38494	Yes	A filter with MAC 00:00:00:00:00:00 is created automatically Problem: In certain situations, a filter will automatically be created on the Clean Access Manager that will exempt all devices. The filter will have a MAC address of 00:00:00:00:00. This will allow all traffic to match this filter, and no users will be prompted for authentication. The filter is created when “Exempt certified devices from web login requirement” is enabled under “Clean Access -> General Setup” and a client attempts to login, and there is a layer 3 device between the client and the CAS. Workaround: Disable the “Exempt certified devices from web login requirement” option.
CSCei46336	Yes	Bit Defender 7.x not detecting the correct virus definition date from the client
CSCei46351	Yes	Certain versions of McAfee not working correctly with Agent Because the agent didn't discover the AV engine version correctly, certain versions of McAfee didn't work correctly.
CSCpe00158	Yes	Preview button on User Pages Administration -> User Pages -> Login Page -> Edit The unsaved modifications will be lost if “Preview” button is pressed. The preview window doesn't use the unsaved values, it uses the saved values instead. For now, the button will be changed in 3.5.3 to indicate “View” (rather than Preview) in order to mitigate confusion The “Preview” button is a bit misleading as the original intention for this button is to view the current state of the user pages. If this button is clicked without committing any changes, then changes that were made will be backed out.
CSCsb30690	Yes	NTLM authentication/Transparent Windows login isn't functioning in 3.5(1), 3.5(2).
CSCsb32620	Yes	When a PC network interface card has any 169.x.x.x address, Clean Access Agent 3.5.2 login button is greyed out. This affects version 3.5(2).
CSCsb32913	Yes	LDAP multivalue attributes mapping isn’t working Symptom: User who belongs to multiple groups gets authenticated but will not be placed in the appropriate role except in the case where the attribute is checked for the last group in the list. For example, if user belongs to admin, student, vpn groups he gets placed in the appropriate role only when attribute mapping is done for vpn group in the memberOf attribute. All others fail. Conditions: This will work if a user belongs to only one group. Fails when the same user belongs to multiple groups and you check the attribute from any group other than last group.

Resolved Caveats - Release 3.5.2.2

Table 26 Resolved Caveats

	Software Release 3.5.2.2	
DDTS Number	**Corrected**	**Caveat**
CSCsb79166	Yes	Clean Access Agent 3.5.6 patch breaks client communication to CAS. **Note** This issue is resolved by the 3.5.4.1, 3.5.3.2, and 3.5.2.2 patches to the CAS.

Resolved Caveats - Release 3.5.2.1

Table 27 Resolved Caveats

	Software Release 3.5.2.1	
DDTS Number	**Corrected**	**Caveat**
CSCei17273	Yes	AV ANY definition rule not updating **Note** This affects 3.5(2). Although vendor-specific AV rules are updated when performing an Update or Auto-Update to the Supported AV product list, AV definition versions/dates are not updated for AV definition rules configured with ANY Antivirus Vendor or ANY product version for a specific vendor. To update ANY AV def rules, you must perform a Clean Update at regular intervals. This does not affect other checks (pc_) and rules (pr_).
CSCei35778	Yes	Need documentation for installing CCA 3.5(2).1 To upgrade from Cisco Clean Access Manager 3.5(2) to 3.5.2.1 follow the instructions below: 1) Download the .tar.gz file to /store on the server 2) Unzip the file with 'tar zxvf <filename> 3) Run 'sh ./<filename.sh> 4) After this has completed, issue 'service perfigo restart' See Upgrade via Web Console (from 3.5.3 and Above Only).

Resolved Caveats - Release 3.5(2)

Table 28 Resolved Caveats

	Software Release 3.5(2)	
DDTS Number	**Corrected**	**Caveat**
CSCei03402	Yes	CAM Apache/Tomcat processes die when monitored by a 3rd party app **Note** This only affects the 3.5(0) and 3.5(1) releases. If a third party monitoring application connects to the Clean Access Manager on port 80 to determine if the webserver is running, it is possible that repeated connections can cause the Manager to freeze up or stop responding. The only errors are problems with Tomcat and Apache in the system logs. Symptom: Clean Access Manager keeps shutting down periodically, and the Clean Access Servers cannot be correctly managed. Conditions: Running an application that connects to port 80 on the Manager to check to see if the webserver is up will cause this to occur. Specifically, something as little as running the "HEAD/1.1" command periodically can cause the system to crash. Workaround: Turn off any monitoring tool until 3.5(2)
CSCei04375	Yes	Re-tag Trusted Side VLAN ID does not work correctly in Real-IP mode This affects 3.5(0) Clean Access Server in Real-IP mode. When vlan retag is used for the trusted side in Real-IP mode, the return packet is also retagged onto the untrusted network. In doing so, the end device on the untrusted cannot communicate to the external (trusted) network.
CSCei07657	Yes	Clean Access Agent New AV Rule Antivirus vendor dropdown has "--Please update AV list--" With new installs or upgrade to 3.5(1), and with the current version of Clean Access agent installed, the New AV Rule dropdown for Antivirus vendor only lists "--Please update AV list --".
CSCei08915	Yes	Replacing all occurrences of $user$ in filters (LDAP auth) The first occurrence was changed, others had been left unaltered.
CSCei08925	Yes	Input validation on LDAP Attribute Mapping rule. The name parameter in mapping rule conditions should not be empty.
CSCei10242	Yes	Crashes when closed by clicking X when timer expires When creating a rule on the server so the client won't pass through it, and logging in from the client, if the requirement is not finished and the client times out from temporary role, and instead of clicking the OK button uses the window x button on the top right corner to close the window, the client crashes.

Table 28 Resolved Caveats (continued)

	Software Release 3.5(2)	
DDTS Number	**Corrected**	**Caveat**
CSCei10529	Yes	Any Rule fails if vendor is not Norton and using def version **Note** This affects 3.5(1) and is fixed in 3.5(2). If you created AV definition rules in 3.5(1), see Known Issues for Release 3.5(2), page 44 for additional details. The ANY definition rule will only succeed if: • It's a Norton product because there is special handling for Norton • If we check date instead of version for virus definition file for the product on the client Otherwise it will fail. The ANY installation check is not affected.

Resolved Caveats - Release 3.5(1)

Table 29 Resolved Caveats

	Software Release 3.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCeh31769	Yes	**Note** The 3.5(1) upgrade script incorporates a DHCP script which regenerates all ARP entries upon upgrade. This issue was fixed starting with version 3.4(3). However, customers on prior versions may have been affected if upgrading from a release affected by this issue. Devices on managed subnets do not respond to ARP queries from the untrusted interface in trunked VLAN mode. The Clean Access Server will send the ARP request originating from the managed subnet default gateway. Some devices will not respond to the ARP request. This affects version 3.3 and 3.4 of the Clean Access Server Software. The list of ARP entries will have been removed. The work-around is to auto generate the DHCP subnet lists again after the 3.5(0) upgrade.

Table 29 Resolved Caveats (continued)

	Software Release 3.5(1)	
DDTS Number	Corrected	Caveat

CSCeh33102	Closed	**Note** This problem is not reproducible.
		Cisco Clean Access field overflow - Require Use of Clean Access Agent (SmartEnforcer). Seen in Cisco Clean Access release 3.3.5, 3.4.1. This problem is currently found in Internet Explorer 6.
		In Device Management > CleanMachines | General Setup | Require use of Clean Access Agent (SmartEnforcer) field has no bounds limit but gives a perfigo_validate.jsp error when certain HTML scripting is placed inside of the field.
		Conditions: Having too many characters in your field entry with HTML tags:
		`<html><head><title>Quarantined</title></head><body>`
		`<center><p>Sorry!`
		`You computer has been found to be vulnerable or has been`
		`compromised.`
		`</p><p>Please correct this condition before attempting access`
		`to this network.</p></center></body></html>`
		Workaround: Shortening the field entry with less information with HTML code/tags:
		`<html><head><title>Quarantined</title></head><body>`
		`<center><p>Sorry!`
		`You computer has been found to be vulnerable or has been`
		`compromised.`
		`</p><p>Please correct this network.</p></center></body></html>`

Table 29 Resolved Caveats (continued)

	Software Release 3.5(1)	
DDTS Number	**Corrected**	**Caveat**
CSCeh35509	Yes	service perfigo config default value inconsistencies Symptom: In certain cases, the option presented by 'service perfigo config' dialog does not reflect the currently configured settings. This only happens when the 'service perfigo config' command is run on a previously configured CA Server. The dialog of the 'service perfigo config' script is inconsistent with its pre-set values. When assigning a gateway to an interface, the dialog does not display the existing value as the default value. Instead, the value offered as the default is the lowest available address on the same subnet as the interface. For example, assume an interface is configured with 10.1.1.5/24 and has a gateway of 10.1.1.99. When the 'service perfigo config' script is run, the suggested IP address of the interface will be 10.1.1.5 and the subnet will be 255.255.255.0, but the gateway will be 10.1.1.1 even though the current configuration has it set as 10.1.1.99. This inconsistency also exists for the hostname. Instead of using the currently configured hostname, the dialog defaults the value to be 'caserver'. This could potentially cause problems with certificates generated with the server's hostname. Workaround: Be very careful when running the 'service perfigo config' command to change the settings on the CA Server. Verify that the suggested value for all questions are correct and reflect the desired configuration. If the hostname is different than before running the 'service perfigo restart' command, the certificate may need to be re-generated. **Note** This is only true if the certificate was generated with the hostname, not if it was generated with the IP address.

CSCeh51673	Yes	CAM Login Failure Message Security Issue
		After entering an incorrect login or password into a Clean Access Manager, the CAM's error message specifies which is incorrect. If the username does not exist, the cam responds with:
		`Invalid admin account:bob or invalid admin group`
		If the username exists, but the password is wrong, CAM responds:
		`Invalid password for admin:admin`

CSCeh81643	Yes	When editing the Description field for a Link-type Requirement, the changes are not saved. The text reverts to the initial text entered when the requirement was created. However, if text is deleted from the Description field when editing a requirement (link), the changes are saved.
CSCeh96638	Yes	3.5.0 Agent Gets Error When Detecting New Agent The 3.5.0 Clean Access Agent informs the user when it detects that the CAS has a newer version of the Agent. When it does, it attempts to download the new agent and gets an error.

Resolved Caveats - Release 3.5(0)

Table 30 Resolved Caveats

	Software Release 3.5(0)	
DDTS Number	Corrected	Caveat
CSCeh48638	Yes	User rejects network policy, placed in temp role policy not applied If a user on a client running the Clean Access Agent rejects the network policy, the user is placed into the temporary role. However, the temporary role policies may not be applied upon the second login.
CSCeh49766	Yes	Automatic Update option for Nessus plugins has been removed for release 3.5(0) Prior to release 3.5(0), the Automatic Update option was available on the user interface, but did not work for plugins. Trying to automatically update network scanner plugins failed. Occurs on all versions of Clean Access Manager. Workaround: Manually updating the plugins, or migrating to using the Clean Access Agent for network checking and authentication.
CSCeh60554	Yes	Nessus plugin update fails to show plugin in Clean Access Manager After uploading a new Nessus plugin for the Network Scan component in the Clean Access Manager, the plugin is not visible via the web GUI in the Plugin configuration page although the plugin does get successfully uploaded to /usr/lib/nessus/plugins on the manager's file system. Conditions: Must have tried to upload the same plugin twice. Workaround: Remove all existing plugins from /usr/lib/nessus/plugins on the Clean Access Manager and then upload a collection of new plugins. Further Problem Description: plugin_id is a primary key in the database. If plugins are uploaded with duplicate plugin IDs, for example, two plugins of id 12109 the database will cause errors when it tries to load plugins with the same ID (and therefore same primary key) into the database. This will also cause the database to stop loading the remaining plugins. This will be fixed by only loading one of the plugins into the database and preventing a duplicate ID from loading in the upcoming releases.

Known Issues for Cisco NAC Appliance

This section describes known issues when integrating Cisco NAC Appliance with third-party elements.

Known Issues with Switches

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

Installing or Upgrading to a New Software Release

This section provides the following software installation and upgrade information:

- General Procedure, page 97
- New Installation of 3.5(x), page 98
- Upgrade Procedure for 3.5(x), page 99
- Upgrading High Availability Pairs, page 107
- Cisco NAC Appliance Service Contract/Licensing Support, page 2

General Procedure

⚠ **Caution** The Clean Access Manager database changes considerably with release 3.5. The upgrade script will automatically migrate the contents of your old database when it upgrades your system to release 3.5(x). Do NOT import any snapshot you made prior to 3.5 migration after you have upgraded to release 3.5, or you will impede the functioning of your Clean Access Manager.

Cisco recommends that you:

1. Back up your current Clean Access Manager installation and save the snapshot on your local computer, as described in Create CAM DB Backup Snapshot, page 100.
2. Upgrade your Clean Access Server(s) to the latest version of 3.5 (from 3.2.6 and above) using either:
   - New Installation of 3.5(x), page 98, or
   - Upgrade Procedure for 3.5(x), page 99
3. Upgrade your Clean Access Manager to the latest version of 3.5 (from 3.2.6 and above) using either:
   - New Installation of 3.5(x), page 98, or
   - Upgrade Procedure for 3.5(x), page 99
4. Take a database snapshot from the upgraded 3.5 Clean Access Manager and download it to your desktop/laptop for safekeeping. Remove any previous snapshots from the CAM and do NOT restore any previous snapshots that are prior to 3.5.
5. Update the Clean Access Manager to obtain the latest Cisco Checks & Rules, CCA Agent Upgrade Patch, Supported Antivirus Product List, and Default Host Policies (From the web admin console, go to **Device Management** > **Clean Access** > **Clean Access Agent** > **Updates**.)

New Installation of 3.5(x)

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

For New Installation:

1. Follow the instructions on your welcome letter to obtain a license file for your installation. See Cisco NAC Appliance Service Contract/Licensing Support, page 2 for details. (If you are evaluating Cisco Clean Access, visit http://www.cisco.com/go/license/public to obtain an evaluation license.)
2. Do one of the following:
   a. Insert the product CD in the CD-ROM drive for each installation machine, and follow the auto-run procedures.
   b. Or, download the two 3.5.x.ISOs from http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml and burn them onto two CD-Rs. Insert them into the respective CD-ROM drive of each of your installation servers. Follow the instructions in the auto-run installer.
3. 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.
4. Install a valid FlexLM license file for the Clean Access Manager (either evaluation, starter kit, or individual license).
5. 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.
6. 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.

Note Clean Access Manager 3.5(11) is bundled with Clean Access Agent 3.5.13.

For detailed software installation steps, see the following guides:

- *Cisco Clean Access Manager Installation and Administration Guide, Release 3.5*
- *Cisco Clean Access Server Installation and Administration Guide, Release 3.5*

Upgrade Procedure for 3.5(x)

Before upgrading to 3.5 from 3.2.6 or above, carefully read the following instructions:

- Before You Upgrade
- Create CAM DB Backup Snapshot
- Download the Upgrade File
- Upgrade via Web Console (from 3.5.3 and Above Only), or
- Upgrade via Console/SSH (standard instructions for standalone machines)

If upgrading failover pairs, you must use the procedure described in:

- Upgrading High Availability Pairs, page 107

Before You Upgrade

⚠ **Caution** Please review this section carefully before you commence the upgrade process.

- **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 currently not designed for heterogeneous support (i.e., some Clean Access Servers running 3.5 software and some running 3.4 software).

- **Upgrade Downtime Window**

  Depending on the number of Clean Access Servers you have, the upgrade process should be scheduled as downtime. 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.

- **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 3.4 or 3.3 database should you encounter problems during upgrade. Backing up immediately following upgrade preserves your upgraded tables and provides a baseline of your 3.5 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 100.

Warning **You cannot restore a 3.4 or earlier database to a 3.5 Clean Access Manager.**

- **Software Downgrade**

  Once you have upgraded your software to 3.5, if you wish to revert to 3.4 or 3.3, note that you will need to reinstall 3.4 or 3.3 from the CD and recover your configuration based on the backup you performed prior to upgrading to 3.5.

- **Passwords**

  For upgrade via SSH, you will need your CAM and CAS `root` user password (default password is `cisco123`). For web console upgrade (release 3.5(3) and above), you will need your CAM web console `admin` user password (and, if applicable, CAS direct access console `admin` user password).

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 3.5 database.

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

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

Step 2 The **Snapshot Tag Name** field automatically populates with a name incorporating the current time and date (e.g. 01_16_07-15:12_snapshot). You can also either accept the default name or type another. To facilitate backup file identification, it is recommended to insert the release version in the snapshot, for example, 01_16_07-15:12_**3.5.11**_snapshot. You can also either accept the default name or type another.

Step 3 Click **Create Snapshot**. The Clean Access Manager generates a snapshot file, which is added to the snapshot list.

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

Step 4 To download the snapshot to another computer, click the **Tag Name** or the **Download** button for the snapshot to be downloaded.

Step 5 In the file download dialog, select the save file to disk option to save the file to your local computer.

Download the Upgrade File

For Cisco Clean Access 3.5 release upgrades, a single file, **cca_upgrade_3.5.x.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/kobayashi/sw-center/sw-ciscosecure.shtml) and click the link for Cisco Clean Access Software.

Step 2 On the Cisco Secure Software page for Cisco Clean Access, click the link for the appropriate release. Upgrade files use the following format (replace the .x in the file name with the minor version number to which you are upgrading, for example, `cca_upgrade_3.5.11.1.tar.gz`):

- **cca_upgrade_3.5.x.tar.gz** (CAM/CAS release upgrade file)
- **cca-3.5.x-to-3.5.x.y-upgrade.tar.gz** (CAM/CAS patch upgrade file)
- **cam-3.5.x-to-3.5.x.y-upgrade.tar.gz** (CAM-only patch upgrade file)
- **cas-3.5.x-to-3.5.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 (from 3.5.3 and Above Only)

If running release 3.5(3) or above of the Cisco Clean Access software on standalone machines, 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**

Note

- For web upgrade, you **must** upgrade each CAS first, then the CAM.
- You can always upgrade the CAS from the CAS direct web console for any release above 3.5(3).
- Release 3.5(3) or above must be installed and running on your CAM/CAS(es) before you can upgrade via web console.
- If running 3.5(2) or below, you must use the upgrade procedure described in Upgrade via Console/SSH, page 105.
- If upgrading failover pairs, refer to Upgrading High Availability Pairs, page 107.

Note the following:

- If running release 3.5(5) or above, you can upgrade the CAS from the CAS management pages (or CAS direct web console), and upgrade the CAM from the CAM web console.
- If running release 3.5(3) or 3.5(4), you can upgrade the CAS from the CAS direct web console, and upgrade the CAM from the CAM web console.

- If running a release prior to 3.5(3), you must follow the instructions in Upgrade via Console/SSH, page 105.

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 (see Database Recovery Tool, page 36 for details). 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 (3.5.5 and above), **or**
2. Upgrade CAS from CAS Web Console (3.5.3/3.5.4), **and**
3. Upgrade CAM from CAM Web Console

Upgrade CAS from CAS Management Pages (3.5.5 and above)

Once release 3.5(5) is installed on the CAS, web upgrades to the CAS (e.g. to 3.5(6) and above) can be performed via the CAS management pages as described below. If you are running release 3.5(3) or 3.5(4) you must follow the instructions in Upgrade CAS from CAS Web Console (3.5.3/3.5.4).

Step 1 Download the Upgrade File.

Step 2 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 3 Click **Browse** to locate the upgrade file you just downloaded from Cisco Downloads, for example:

cca_upgrade_3.5.*x*.tar.gz (CAM/CAS release upgrade file), or

cca-3.5.x-to-3.5.x.y-upgrade.tar.gz (CAM/CAS patch upgrade file), or

cas-3.5.x-to-3.5.x.y-upgrade.tar.gz (CAS-only patch upgrade file)

Step 4 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 will display the newly-uploaded upgrade file with its date and time of upload, file name, and notes (if applicable).

Step 5 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 When upgrading via web console only, the machine automatically reboots after upgrade.

Step 6 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 7 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)

Step 8 Repeat steps 2, 5, 6 and 7 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 Web Console (3.5.3/3.5.4)

If running release 3.5(3) or 3.5(4), you must use the CAS direct web console to upgrade the CAS via web. If running release 3.5(5) or above, you can follow the instructions to Upgrade CAS from CAS Management Pages (3.5.5 and above), or optionally use the instructions below.

Step 1 Download the Upgrade File.

Step 2 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 3 In the CAS web console, go to **Administration** > **Software Update**.

Step 4 Click **Browse** to locate the upgrade file you just downloaded, for example:

cca_upgrade_3.5.*x*.tar.gz (CAM/CAS release upgrade file), or

cca-3.5.x-to-3.5.x.y-upgrade.tar.gz (CAM/CAS patch upgrade file), or

cas-3.5.x-to-3.5.x.y-upgrade.tar.gz (CAS-only patch upgrade file), or

Step 5 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 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 will automatically reboot.

Note

- If upgrading from 3.5(3), click **Open** to load the upgrade .tar.gz file as the **Upload Patch File**, then click **Update**.
- When upgrading via web console only, the machine automatically reboots after upgrade.

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

Step 8 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)

Step 9 Repeat steps 2 to 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 CAM from CAM Web Console

After you have upgraded each CAS, upgrade your CAM as described below.

Step 1 Download the Upgrade File.

Step 2 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 3 Click **Browse to** locate the upgrade file you just downloaded from Cisco Downloads, for example:

cca_upgrade_3.5.x.tar.gz (CAM/CAS release upgrade file)

cca-3.5.x-to-3.5.x.y-upgrade.tar.gz (CAM/CAS patch upgrade file)

cam-3.5.x-to-3.5.x.y-upgrade.tar.gz (CAM-only patch upgrade file)

Step 4 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 5 Click the **Apply** icon for the upgrade file, and click **OK** in the confirmation dialog that appears. This will start the CAM upgrade. After the upgrade is complete, the CAM will automatically reboot.

Note
- If upgrading from 3.5(3), click **Open** to load the upgrade .tar.gz file as the **Clean Access Manager Patch File**, then click **Apply Patch**.
- When upgrading via web console only, the machine automatically reboots after upgrade.

Step 6 Wait 2-5 minutes for the upgrade and reboot to complete.The CAM web console will become unavailable during the reboot.

Step 7 Access the CAM web console again. You should now see the new version, “Cisco Clean Access Manager Version 3.5.x”, at the top of the web console. (See also Determining the Software Version, page 8.)

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

Upgrade via Console/SSH

Use the instructions in this section to upgrade your standalone CAM/CAS using the standard console/SSH upgrade procedure.

Note If running release 3.5(2) or below, you must use SSH to perform upgrade.

Note Starting from release 3.5(3) and above, the upgrade script allows you to upgrade directly to the latest major version of 3.5(x) from release 3.2(6), 3.3(x). 3.4(x), and previous 3.5(x) versions. You cannot upgrade directly to 3.5(x) from 3.1.

Note Your CAM/CAS must already be running 3.5(x) to apply the 3.5.11.1 patch upgrade. If running 3.4(x) or below, you must upgrade to 3.5(x) first before you can apply the 3.5.11.1 patch.

For release 3.5 upgrades, a single file, **cca_upgrade_3.5.x.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 3.2(6) and above.

Download the Upgrade File and Copy to CAM/CAS

Step 1 Download the Upgrade File.

Step 2 Copy the file (with the .x in the filename corresponding to the proper version) to the Clean Access Manager and Clean Access Server(s) respectively using WinSCP, SSH File Transfer or PSCP, as described below.

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

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

b. Copy **cca_upgrade_3.5.x.tar.gz** to the /store directory on **each** Clean Access Server.

If using PSCP (replace .x with minor 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_3.5.x.tar.gz root@ipaddress_manager:/store
```

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

```
pscp cca_upgrade_3.5.x.tar.gz root@ipaddress_server:/store
```

Perform SSH Upgrade on the CAM

Step 3 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 .x with minor upgrade version number):

```
tar xzvf cca_upgrade_3.5.x.tar.gz
```

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

```
cd cca_upgrade_3.5.x
sh ./UPGRADE.sh
```

Note With upgrade to release 3.5(10) and above, when upgrading the CAM, the 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 3.5.13 for release 3.5(11)). 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 3.5.x? (y/n)? [y]
```

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

```
reboot
```

Perform SSH Upgrade on the CAS

Step 4 Connect to the Clean Access Server to upgrade using Putty or SSH:

a. SSH to the Clean Access Server.

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

c. Change directory to /store:

```
cd /store
```

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

```
tar xzvf cca_upgrade_3.5.x.tar.gz
```

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

```
cd cca_upgrade_3.5.x
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.

Upgrading High Availability Pairs

If upgrading an existing high-availability (failover) pair of Clean Access Managers or Clean Access Servers to 3.5(x), you must use the instructions in this section.

This section describes the following:

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

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.

Determining Active and Standby Clean Access Server

For a Clean Access Server High-Availability pair:

- Access the primary CAS by opening a web console for the trusted-side (eth0) IP address of the primary CAS:

  `https://<primary CAS (eth0)IP>/admin`
  For example, `https://172.16.1.2/admin`

- Access the secondary CAS by opening a web console for the trusted-side (eth0) IP address of the secondary CAS:

  `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.

Instructions for Upgrading High Availability CAM and CAS

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

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 105 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 .x with minor upgrade version number):

```
tar xzvf cca_upgrade_3.5.x.tar.gz
```

b. CD into the created "cca_upgrade_3.5.x" 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 for 3.5(3) and above only. 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 107.

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_3.5.x" directory on the active box (replace .x with minor upgrade the version number, for example, `cca_upgrade_3.5.11.1`).

Step 7 Run the following command on the active box:

```
./fostate.sh
```

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

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

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

b. From the untarred upgrade directory created on the active box (for example "cca_upgrade_3.5.11"):, run the upgrade script on the active box:

```
./UPGRADE.sh
```

Note With upgrade to release 3.5(10) and above, when upgrading the CAM, the 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 3.5.13 for release 3.5(11)). 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.

c. 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 3.5.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 (replace .x with minor upgrade version number, for example “cca_upgrade_3.5.11”):

```
cd cca_upgrade_3.5.x
```

c. Run the upgrade script on the standby box:

```
./UPGRADE.sh
```

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.

d. 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 3.5.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.

Troubleshooting

This section discusses the following:

- No Web Login Redirect / CAS Cannot Establish Secure Connection to CAM
- CAM/CAS Support Logs
- Agent AV Rule Troubleshooting
- IE 7.0 Beta and Clean Access Agent
- Enable Debug Logging on the Clean Access Agent
- Recovering Root Password for CAM/CAS (Release 3.5.x or Below)
- Troubleshooting Switch Support Issues
- Troubleshooting Network Card Driver Support Issues
- Other Troubleshooting Information

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

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

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

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

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

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

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

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

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

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

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

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

To identify common issues:

1. Check the CAM's certificate and verify it has not been generated with the IP address of the CAS: (under **Administration** > **CCA Manager** > **SSL Certificate** > **Export Certificate Request**)
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.

CAM/CAS Support Logs

Starting with release 3.5(3), there are two new **Support Logs** web console pages for the CAM and CAS to facilitate TAC support when a customer has issues. The **Support Logs** page allows 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 following support logs from the CAM web console when sending their customer support request:

- **Administration** > **CCA Manager** > **Support Logs**
- **Device Management** > **CCA Servers** > **IPaddress** > **Misc** > **Support Logs**

For releases prior to 3.5(3), contact TAC for assistance on manually creating the support logs.

Agent AV Rule Troubleshooting

To view administrator reports for the Clean Access Agent go to **Device Management** > **Clean Access** > **Clean Access Agent** > **Reports**.

When troubleshooting AV 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 vendor product.
4. What is failing—AV installation check or AV update checks? What is the error message?
5. What is the current value of the AV def date/version on the failing client machine?
6. What is the corresponding value of the AV def date/version being checked for on the CAM? (see **Device Management** > **Clean Access** > **Clean Access Agent** > **Rules** > **Agent-AV Support Info**)

IE 7.0 Beta and Clean Access Agent

Internet Explorer 7.0 Beta is not supported when using the Clean Access Agent. The Agent will not be able to login and perform other operations if the user has IE 7.0 installed.

Problem User sees “Invalid parameter: 87” error from the Windows API.

Solution Uninstall IE 7.0 Beta 2.

See also Web Browser Compatibility, page 8.

Enable Debug Logging on the Clean Access Agent

Note For the 3.5.11 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 3.5.10 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:
    a. Open Start > Run
    b. In the Open: field, type: `%APPDATA%/CiscoCAA`
    c. You will find event.log file there.

Note

- For 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\.

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**.

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.

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:

http://www.cisco.com/en/US/products/ps6128/products_device_support_table09186a008043a8d9.html#wp44095

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 31 Updates to Release Notes for Cisco Clean Access (NAC Appliance) Version 3.5(x)

Date	Description
6/28/07	Added caveat CSCsd90433 to Open Caveats - Release 3.5.11.1, page 78
3/16/07	Moved caveat CSCsi07595 to Open Caveats - Release 3.5.11.1, page 78
3/9/07	Added caveat CSCsi07595 to address the DST 2007 fix
19-Jan-07	Release 3.5.11.1 • Updated Software Compatibility Matrixes, page 4 • Added Enhancements for Release 3.5.11.1, page 10 • Updated Supported AV Product List Versions, page 72 • Updated Open Caveats - Release 3.5.11.1, page 78 • Added Resolved Caveats - Release 3.5.11.1, page 78 • Added Recovering Root Password for CAM/CAS (Release 3.5.x or Below), page 113 • Updated template and boilerplate information.
18-Aug-06	• Updated all switch support information to point to *Switch Support for Cisco NAC Appliance* • Updated general Cisco support boilerplate
14-Jul-06	Moved CSCse53459, page 79 to Open Caveats table for 3.5(11)
7-Jul-06	Updated Resolved Caveats - Release 3.5(11), page 79 (for CSCse53459)
27-Jun-06	Supported Switches for Cisco Clean Access, page 4 - updates for 4000/4500 and 6000/6500
26-Jun-06	Release 3.5(11) • Updated Supported Switches for Cisco Clean Access, page 4 • Added Switch Support for CAS Virtual Gateway/VLAN Mapping (IB and OOB), page 5 • Updated Software Compatibility, page 4 • Added Enhancements for Release 3.5(11), page 10 • Updated Clean Access Supported Antivirus Product List, page 64 • Added Resolved Caveats - Release 3.5(11), page 79 • Updated Troubleshooting, page 110
7-Mar-06	Release 3.5(10)
30-Jan-06	Release 3.5(9)
29-Nov-05	Release 3.5(8)
27-Oct-05	Release 3.5(7)
12-Oct-05	Release 3.5.6.1
12-Oct-05	Release 3.5.5.1

Table 31 Updates to Release Notes for Cisco Clean Access (NAC Appliance) Version 3.5(x)

Date	Description
28-Sep-05	Release 3.5(6)
6-Sep-05	Release 3.5.4.1
6-Sep-05	Release 3.5.3.2
6-Sep-05	Release 3.5.2.2
31-Aug-05	Release 3.5(5)
10-Aug-05	Release 3.5(4)
27-Jul-05	Release 3.5.3.1
20-Jul-05	Release 3.5(3)
15-Jun-05	Release 3.5.2.1
2-Jun-05	Release 3.5(2)
20-May-05	Release 3.5(1)
14-Apr-05	Release 3.5(0)

Related Documentation

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

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

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

- *Cisco Clean Access Installation Quick Start Guide, Release 3.5*
- *Cisco Clean Access Manager Installation and Administration Guide, Release 3.5*
- *Cisco Clean Access Server Installation and Administration Guide, Release 3.5*
- *Release Notes for Cisco Clean Access Version 3.5(x)*
- *Supported Hardware and System Requirements for Cisco NAC Appliance (Cisco Clean Access)*
- *Switch Support for Cisco NAC Appliance*

See the latest updates to the 3.5(x) Cisco Clean Access documentation at:

http://www.cisco.com/univercd/cc/td/doc/product/vpn/ciscosec/cca/cca35/index.htm

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

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

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products
- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

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

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/en/US/support/index.html

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- “What’s New in Cisco Documentation” is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of “What’s New in Cisco Documentation” at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in Related Documentation, page 115.

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