



# Release Notes for Cisco NAC Appliance, Version 4.6(1)

---

Revised: April 7, 2011, OL-19353-01

## Contents

These release notes provide late-breaking and cumulative release information for Cisco® NAC Appliance, Release 4.6(1). This document describes new features, changes to existing features, limitations and restrictions (“caveats”), upgrade instructions, and related information. These release notes supplement the Cisco NAC Appliance documentation included with the distribution. Read these release notes carefully and refer to the upgrade instructions prior to installing the software.

- [Cisco NAC Appliance Releases, page 2](#)
- [System and Hardware Requirements, page 2](#)
- [Software Compatibility, page 6](#)
- [New and Changed Information, page 10](#)
- [Cisco NAC Appliance Supported AV/AS Product Lists, page 18](#)
- [Caveats, page 22](#)
- [New Installation of Release 4.6\(1\), page 58](#)
- [Upgrading to Release 4.6\(1\), page 59](#)
- [Known Issues for Cisco NAC Appliance, page 73](#)
- [Troubleshooting, page 81](#)
- [Documentation Updates, page 88](#)
- [Obtaining Documentation and Submitting a Service Request, page 88](#)



---

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

# Cisco NAC Appliance Releases

Cisco NAC Appliance Version	Availability
4.6(1) ED	July 1, 2009


**Note**

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

## System and Hardware Requirements

This section describes the following:

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

## Licensing

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

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

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

## Hardware Support

This section contains the following topics:

- [Release 4.6\(1\) and Hardware Platform Support](#)
- [Release 4.6\(1\) and Cisco NAC Profiler](#)
- [Supported Switches for Cisco NAC Appliance](#)

## Release 4.6(1) and Hardware Platform Support

Cisco NAC Appliance Release 4.5 and later only supports and can only be installed on Cisco NAC Appliance platforms CCA-3140, NAC-3310, NAC-3350, NAC-3390, and [Cisco NAC Network Module \(NME-NAC-K9\)](#).



**Note** If upgrading a CCA-3140 appliance from release 4.1(6), refer to [Known Issue with Upgrading CCA-3140 Appliance from Release 4.1\(6\)](#), page 77 prior to upgrade.

Additionally, Cisco NAC Appliance Release 4.6(1) provides substantial changes and enhancements for product hardware support, installation and upgrade:

- A single product installation CD (ISO) provides the option to perform CD installation on CCA-3140 and NAC-3300 series appliance platforms. The installation package detects whether a CAS, CAM or SuperCAM was previously installed along with the software version.
- **Web upgrade is no longer supported for upgrade starting from release 4.5.** To upgrade your CAM and CAS from 4.1(x) or 4.0(x) releases, you must copy the **cca\_upgrade-4.6.1-NO-WEB.tar.gz** file to each CAM and CAS appliance and run the upgrade script via the command line. Refer to [Upgrading to Release 4.6\(1\)](#), page 59 and [Known Issues with Web Upgrade in Release 4.1\(x\) and Earlier](#), page 74 for details.
- Neither the installation CD nor the upgrade file will execute if attempting to run them on a non-supported platform. Refer to [Changes for 4.6\(1\) Installation/Upgrade](#), page 60 for additional details.
- Legacy customers on non-appliance platforms who wish to upgrade to release 4.6(1) will need to purchase a supported platform to install the release 4.6(1) software. Refer to [Upgrading from Customer-Supplied Hardware to Cisco NAC Appliance Hardware Platforms](#), page 64 for additional details.

See also [Features Optimized/Removed](#), page 17 for additional information.

### Cisco NAC Network Module

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



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

For further details, including software installation instructions, refer to [Getting Started with Cisco NAC Network Modules in Cisco Access Routers](#).



**Note** You must run the same software version (e.g. 4.6(1)) on all CAM/CAS appliances and CAS network modules in your network.

## Release 4.6(1) and Cisco NAC Profiler

Release 4.6(1) includes version 2.1.8-37 of the Cisco NAC Profiler Collector component that resides on Clean Access Server installations. When upgrading Clean Access Server appliances (standalone or HA) to release 4.6(1), the upgrade script will check the version of the Collector and only upgrade it if version 2.1.8-37 is not already installed.

Refer to the [Release Notes for Cisco NAC Profiler](#) for software compatibility matrixes and additional upgrade and product information.

## Supported Switches for Cisco NAC Appliance

### Cisco NAC Appliance Wireless OOB Support

[Table 1](#) lists the Wireless LAN Controller platforms that Cisco NAC Appliance supports for the Wireless Out-of-Band feature. [Table 2](#) lists the recommended IOS versions for the switches used with Cisco NAC Appliance, Release 4.6(1).

**Table 1** Recommended WLC Platforms to Support Wireless OOB in Release 4.6(1)

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



#### Note

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

[Table 2](#) lists the IOS versions and switch platforms that are tested and known to work with the Wireless OOB feature in Release 4.6(1). If you encounter issues with WOOB support and are running a minimum IOS version listed as supported for your existing hardware platform in [Switch Support for Cisco NAC Appliance](#), you may need to upgrade the IOS on your switch to the version listed in [Table 2](#).

**Table 2** Switch IOS Versions Tested and Known to Work for WOOB in Release 4.6(1)

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

See [Switch Support for Cisco NAC Appliance](#) for complete details on:

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

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

[Table 3](#) lists VPN and wireless components supported for Single Sign-On (SSO) with Cisco NAC Appliance. Elements in the same row are compatible with each other.

**Table 3** *VPN and Wireless Components Supported By Cisco NAC Appliance For SSO*

Cisco NAC Appliance Version	VPN Concentrator/Wireless Controller	VPN Clients
4.5 and later	Cisco WiSM Wireless Service Module for the Cisco Catalyst 6500 Series Switches	N/A
	Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs) <sup>1</sup>	N/A
	Cisco ASA 5500 Series Adaptive Security Appliances, Version 8.0(3)7 or later <sup>2</sup>	AnyConnect
	Cisco ASA 5500 Series Adaptive Security Appliances, Version 7.2(0)81 or later	<ul style="list-style-type: none"> <li>• Cisco SSL VPN Client (Full Tunnel)</li> <li>• Cisco VPN Client (IPSec)</li> </ul>
	Cisco WebVPN Service Modules for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers	
	Cisco VPN 3000 Series Concentrators, Release 4.7	
	Cisco PIX Firewall	

1. For additional details, see also [Known Issues with Cisco 2200/4400 Wireless LAN Controllers \(Airespace WLCs\)](#), page 78.
2. Release 4.5 and later supports existing AnyConnect clients accessing the network via Cisco ASA 5500 Series devices running release 8.0(3)7 or later. For more information, see the [Release Notes for Cisco NAC Appliance, Version 4.1\(3\)](#), and [CSCsi75507](#).



### Note

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

For further details, see the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.6\(1\)](#) and the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.6\(1\)](#).

## Additional Support Information

Refer to [Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later](#) for additional details related to Windows/Mac OS X/Web Agent support.

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

## Software Compatibility

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

- [Release 4.6\(1\) Compatibility Matrix](#)
- [Release 4.6\(1\) CAM/CAS Upgrade Compatibility Matrix](#)
- [Release 4.6\(1\) Agent Upgrade Compatibility Matrix](#)

## Release 4.6(1) Compatibility Matrix

[Table 4](#) lists Cisco NAC Appliance Manager/Server/Agent compatibility per supported release. CAM/CAS/Agent versions displayed in the same row are compatible with one another. Cisco recommends that you synchronize your software images to match those shown as compatible in [Table 4](#).

**Table 4** Release 4.6(1) CAM/CAS/Agent Compatibility Matrix

Clean Access Manager <sup>1, 2</sup>	Clean Access Server <sup>1, 2</sup>	Cisco NAC Appliance Agents <sup>3</sup>		
		Windows	Mac OS X	Web Agent
Localized Server <sup>4</sup>		Localized Agent <sup>5</sup>		
4.6(1)	4.6(1)	4.6.2.113 (All languages)	N/A	N/A
		4.6.1.34 (Japanese and English only)		
English-Only Server		English-Only Agent		
4.6(1) <sup>6</sup>	4.6(1)	4.6.2.113	4.6.0.3	4.6.0
		4.6.1.34 <sup>7</sup>		
		4.5.1.0	4.5.0.0 <sup>7</sup>	
		4.5.0.0	4.1.3.0 <sup>8</sup>	
		4.1.8.0 <sup>8</sup>		
		4.1.6.0 <sup>8</sup>		
4.1.3.0 <sup>8</sup>				
English-Only Server		English-Only Agent		
4.1(3) and later	4.1(3) and later	4.6.2.113 <sup>9</sup>	4.6.0.3	4.6.0

1. Cisco NAC Appliance Release 4.5 and later only supports and can only be installed on Cisco NAC Appliance platforms CCA-3140, NAC-3310, NAC-3350, NAC-3390, and Cisco NAC Network Module (NME-NAC-K9). You cannot upgrade to or install release 4.6(1) on any other platform. See [Hardware Support, page 2](#) and [Changes for 4.6\(1\) Installation/Upgrade, page 60](#) for additional details.
2. Make sure that both CAM and CAS are of same version.
3. See [Enhancements in Release 4.6\(1\), page 10](#) for details on each version of the Windows/Mac OS X/Web Agents.

4. “Localized Server” means localized text added to administrator-configurable fields in the CAM web console that present text to the user (e.g. Agent Requirement descriptions). Some server-generated error messages may still include English text.
5. When distributed from the CAM, the Cisco NAC Agent installation dialogs are automatically localized upon installation to the local client operating system. AV/AS international product names are also supported, however AV/AS rules/requirements themselves are not localized in Release 4.6(1). Refer to [Cisco NAC Windows Agent Version 4.6.2.113, page 16](#) for the list of languages supported for Cisco NAC Agent localization. If you only upgrade to the latest version of the Cisco NAC Agent, and leave your CAM/CAS at release 4.5(1) or earlier, the Agent operates as an English-only entity—you cannot take advantage of the native operating system localization support available to Cisco NAC Agent users who are logging in to a 4.6(1) CAM/CAS network.
6. When upgrading the CAM from version 4.1(1) and earlier, Agent files are automatically upgraded to the latest Agent version packaged with the CAM software image (e.g. 4.6.2.113). When upgrading the CAM from release 4.1(2) and later, the script will prompt you whether or not to upgrade the Agent files to the latest version. This allows administrators to schedule the Agent upgrade separately from the CAM/CAS server upgrade. Cisco recommends upgrading to the latest 4.6.2.113 Agent version as soon as possible.
7. 4.6.x.x Windows/Mac OS X Clean Access Agents are supported on 4.1(3) and later CAM/CAS releases for basic compatibility (login/logout) and AV/AS product support. The maximum available AV/AS support is based on the maximum version of the Clean Access Agent Setup or Patch (upgrade) file uploaded to the CAM as well as the maximum version of the Agent on the client. See [Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later](#) for details. For full 4.5 and later features (including Mac OS X posture assessment), the 4.5.0.0 or later Agent must be run with the appropriate 4.5 or later CAM/CAS.
8. CAM/CAS release 4.6(1) supports 4.1.3.0 and later Agents for basic compatibility (login/logout) and AV/AS product support. The maximum available AV/AS support is based on the maximum version of the Clean Access Agent Setup or Patch (upgrade) file uploaded to the CAM as well as the maximum version of the Agent on the client. See [Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later](#) for details. For full 4.5 and later features (including Mac OS X posture assessment), the 4.5.0.0 or later Agent must be run with the appropriate 4.5 or later CAM/CAS.
9. If you only upgrade to the latest version of the Cisco NAC Agent, and leave your CAM/CAS at release 4.5(1) or earlier, the Agent operates as an English-only entity—you cannot take advantage of the native operating system localization support available to Cisco NAC Agent users who are logging in to a 4.6(1) CAM/CAS network.

## Release 4.6(1) CAM/CAS Upgrade Compatibility Matrix

[Table 5](#) shows CAM/CAS upgrade compatibility. You can upgrade/migrate your CAM/CAS from the previous release(s) specified to the latest release shown in the same row. When you upgrade your system software, Cisco recommends you upgrade to the most current release available whenever possible.

**Table 5** *Release 4.6(1) CAM/CAS Upgrade Compatibility Matrix*

Clean Access Manager <sup>1</sup>		Clean Access Server <sup>1,2</sup>	
Upgrade From:	To:	Upgrade From:	To:
4.5(x)	4.6(1)	4.5(x)	4.6(1)
4.1(x)		4.1(x)	
4.0(x)		4.0(x)	

1. Cisco NAC Appliance Release 4.5 and later only supports and can only be installed on Cisco NAC Appliance platforms CCA-3140, NAC-3310, NAC-3350, NAC-3390, and Cisco NAC Network Module (NME-NAC-K9). You cannot upgrade to or install release 4.6(1) on any other platform. See [Hardware Support, page 2](#) and [Changes for 4.6\(1\) Installation/Upgrade, page 60](#) for additional details.
2. The Clean Access Server is shipped with a default version of the Cisco NAC Profiler Collector. See [Release 4.6\(1\) and Cisco NAC Profiler, page 4](#) for details.

## Release 4.6(1) Agent Upgrade Compatibility Matrix

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



### Note

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

Refer to [Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later](#) for additional details related to Windows/Mac OS X/Web Agent support.

**Table 6** Release 4.6.2.113 Agent Upgrade Compatibility Matrix

Clean Access Manager	Clean Access Server	Cisco NAC Appliance Agent <sup>1</sup>		
		Upgrade From Cisco Clean Access Agent:	To Latest Compatible Cisco NAC Windows Agent:	To Latest Compatible Mac OS X Version:
4.6(1)	4.6(1)	4.6.1.34 4.5.x.x 4.1.x.x <sup>2, 3, 4</sup> 4.0.x <sup>2</sup>	4.6.2.113 <sup>5, 6, 7</sup>	4.6.0.3 <sup>5</sup>

1. See [Enhancements in Release 4.6\(1\), page 10](#) for details on each version of the Windows/Mac OS X/Web Agent.
2. Auto-upgrade to the latest 4.6.x.x Agent is supported from any 4.0.0.0 and later Windows Agent and any 4.1.3.0 and later Mac OS X Agent. To upgrade earlier Mac OS X Agent versions, download the Agent via web login and run the Agent installation.
3. When upgrading the CAM from version 4.1(1) and earlier, Agent files are automatically upgraded to the latest Agent version packaged with the CAM software image (e.g. 4.6.2.113). When upgrading the CAM from release 4.1(2) and later, the script will prompt you whether or not to upgrade the Agent files to the latest version. This allows administrators to schedule the Agent upgrade separately from the CAM/CAS server upgrade. Cisco recommends upgrading to the latest 4.6.2.113 Agent version as soon as possible.
4. CAM/CAS release 4.6(1) supports 4.1.3.0 and later Agents for basic compatibility (login/logout) and AV/AS product support. The maximum available AV/AS support is based on the maximum version of the Clean Access Agent Setup or Patch (upgrade) file uploaded to the CAM as well as the maximum version of the Agent on the client. See [Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later](#) for details. For full 4.5 or later features (including Mac OS X posture assessment) and 4.5 or later AV/AS product support, the 4.5.0.0 or later Agent must be run with the appropriate 4.5 or later CAM/CAS.
5. 4.6.x.x Clean Access Agents are supported on 4.1(3) and later CAM/CAS releases for basic compatibility (login/logout) and AV/AS product support (Windows only). The maximum available AV/AS support is based on the maximum version of the Clean Access Agent Setup or Patch (upgrade) file uploaded to the CAM as well as the maximum version of the Agent on the client. See [Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later](#) for details. For full 4.5 or later features (including Mac OS X posture assessment) and 4.5 or later AV/AS product support, the 4.5.0.0 or later Agent must be run with the appropriate 4.5 or later CAM/CAS.
6. Cisco NAC Appliance release 4.5 and later no longer supports Windows ME/98/NT client operating systems and you cannot install the Windows Clean Access Agent version 4.5.0.0+ to Windows ME/98/NT client machines.
7. For checks/rules/requirements, version 4.1.1.0 and later Windows Agents can detect “N” (European) versions of the Windows Vista operating system, but the CAM/CAS treat “N” versions of Vista as their US counterpart.



## Determining the Software Version

### Clean Access Manager (CAM) Version

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

### Clean Access Server (CAS) Version

- SSH or console to the machine (or network module) and type `cat /perfigo/build`
- CAS web console ([https://<CAS\\_eth0\\_IP\\_address>/admin](https://<CAS_eth0_IP_address>/admin)):  
**Administration > Software Upload | Current Version**
- CAM web console: **Device Management > CCA Servers > List of Servers > Manage [CAS\_IP] > Misc > Upgrade Logs | Current Version**

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

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

### Cisco Clean Access Updates

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

# New and Changed Information

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

- [Enhancements in Release 4.6\(1\), page 10](#)

## Enhancements in Release 4.6(1)

- [Posture Assessment Support for 64-Bit Windows Operating Systems, page 10](#)
- [Agent Localization Support for “Double-Byte” Languages, page 10](#)
- [Selective Application Privilege Support for Windows Operating Systems, page 11](#)
- [Accessibility Support Via the JAWS Screen Reader Interface, page 11](#)
- [Full UTF-8 Compliance, page 11](#)
- [Agent Log Recording and Retrieval, page 11](#)
- [Support for EVDO Client Machines, page 12](#)
- [Optimized Windows Operating System Support, page 12](#)
- [Agent Configuration XML File Upload Enhancement, page 12](#)
- [Cisco Log Packager Agent Log Compiler Application, page 14](#)
- [Agent Backward-Compatibility, page 16](#)
- [Agent Upgrade Optional When Upgrading Cisco NAC Appliance, page 16](#)
- [Cisco NAC Appliance Agent Reports Enhancement, page 16](#)
- [Cisco NAC Windows Agent Version 4.6.2.113, page 16](#)
- [Mac OS X Clean Access Agent Version 4.6.0.3, page 17](#)
- [Cisco NAC Web Agent Version 4.6.0, page 17](#)
- [Administrator Web Console Enhancements to Support Cisco NAC Agent, page 17](#)
- [Features Optimized/Removed, page 17](#)
- [Supported AV/AS Product List Enhancements \(Windows Version 78, Mac OS X Version 3\), page 17](#)

## Posture Assessment Support for 64-Bit Windows Operating Systems

Cisco NAC Agent version 4.6.2.113 can be installed and launched on 64-bit versions of Windows XP and Windows Vista, and can perform posture assessment and remediation on client machines. Earlier releases of Cisco NAC Appliance provided only authentication support for 64-bit client operating systems.

## Agent Localization Support for “Double-Byte” Languages

Cisco NAC Agent version 4.6.2.113 introduces MultiByte Character Support (MBCS) for posture assessment and remediation operations on double-byte language client machines. Version 4.6.2.113 of the Cisco NAC Agent provides localization support for Agent login, remediation and user-facing dialogs and messages for the languages listed in [Table 7](#).

**Table 7**      **Languages Supported for Cisco NAC Agent Localization, Version 4.6.2.113**

Catalan	French	Portuguese
Chinese (Simplified)	French Canadian	Russian
Chinese (Traditional)	German	Serbian (Cyrillic)
Czech	Hungarian	Serbian (Latin)
Danish	Italian	Spanish
Dutch	Japanese	Swedish
English	Korean	Turkish
Finnish	Norwegian	

## Selective Application Privilege Support for Windows Operating Systems

In Cisco NAC Appliance Release 4.6(1), to more effectively integrate with the Windows Vista operating system, different functional elements of Cisco NAC Agent have different privilege levels to support Windows Vista User Account Control (UAC).

## Accessibility Support Via the JAWS Screen Reader Interface

To provide Cisco NAC Agent support for visually-impaired users, the Cisco NAC Agent is compatible with the Microsoft Job Access with Speech (JAWS) screen reader. Client machines are required to have the JAWS software installed in order to enable and use this feature.



### Note

Accessibility support in Cisco NAC Appliance Release 4.6(1) is limited to the Windows Cisco NAC Agent on the client machine, and is not applicable to the Cisco NAC Web Agent or Mac OS X Clean Access Agent. There are also no provisions supporting Accessibility on the CAM/CAS web console interface.

## Full UTF-8 Compliance

To help provide Cisco NAC Agent localization for “double-byte” languages like Japanese, Cisco NAC Appliance Release 4.6(1) offers features UTF-8 compliance. The Cisco NAC Agent, Clean Access Manager, and Clean Access Server components all feature UTF-8 capability to seamlessly communicate localized messages between the Agent on the client machine and the Cisco NAC Appliance network.



### Note

If you only upgrade to the latest version of the Cisco NAC Agent, and leave your CAM/CAS at release 4.5(1) or earlier, the Agent operates as an English-only entity—you cannot take advantage of the native operating system localization support available to Cisco NAC Agent users who are logging in to a 4.6(1) CAM/CAS network.

## Agent Log Recording and Retrieval

Starting from Cisco NAC Appliance 4.6(1), the Windows Cisco NAC Agent records and stores local login and operation events on the client machine in the C:\Documents and Settings\All Users\Application Data\Cisco\Cisco NAC Agent\logs directory. After the first Cisco NAC Agent login

session, two files reside in this directory: one backup file from the previous login session and one new file containing login and operation information from the current session. Each log file in the directory is limited to a maximum length, determined by the **LogFileSize** XML value in the Agent configuration file setting (see [Agent Configuration XML File Upload Enhancement, page 12](#)). The default file size is 5MB. If the log file for the current Cisco NAC Agent session grows beyond the specified file size, the first segment of Agent login and operation information automatically becomes the “backup” file in the directory and the Agent continues to record the latest entries in the current session file.

**Note**

Cisco NAC Agent log file contents are encrypted. Only internal Cisco resources (service engineers, TAC representatives, etc.) can decrypt and view the log file contents.

## Support for EVDO Client Machines

Cisco NAC Agent version 4.6.2.113 supports Windows client machines connected to the network via an Evolution Data Optimized (EVDO) connection. Traditionally, Cisco NAC Appliance could not authenticate this type of client connection, because there is no MAC address associated with client machines connecting via EVDO.

For more information, see [CSCsu30467, page 53](#).

## Optimized Windows Operating System Support

The Cisco NAC Agent version 4.6.2.113 supports the following Windows operating systems:

- Windows 2000 (SP4 and later)
- Windows XP (32-bit SP2 and later)
- Windows XP (64-bit SP2)
- Windows Vista (32- and 64-bit, SP1 and later)

The Agent does not support the following Windows Operating Systems:

- Windows 95
- Windows 98
- Windows Millennium
- Windows NT
- Windows 2000 Server
- Windows 2003 Server

## Agent Configuration XML File Upload Enhancement

**Note**

The **NACAgentCFG.xml** file is not included as a component in the Agent installer.

Cisco NAC Appliance Release 4.6(1) enables administrators to construct and distribute an optional Agent configuration XML file (named **NACAgentCFG.xml** and residing in the Agent install directory) that specifies parameter settings for the Windows Cisco NAC Agent. This XML configuration file method of setting up Agents on client machines replaces the previous Clean Access Agent configuration schema requiring Windows registry setting manipulation for custom parameters. If you previously

employed Windows registry settings to adjust Clean Access Agent behavior on client machines, you must specify the same settings in the XML Agent configuration file to preserve Agent behavior using the Cisco NAC Agent.

The XML Agent configuration file is not required for Cisco NAC Agent distribution, but can be used to customize login and operation settings on the client machine. If no custom XML file is configured and installed on the client machine, the Agent creates a default XML file and uses that file to specify login and operational settings until another file is installed that overwrites those default settings.

## Customization

When configuring a customized Agent configuration XML file, the administrator can choose to customize one or more (or all) settings and specify whether they should merge with or overwrite existing XML configuration settings on the client machine. In addition to providing specific values for the parameters defined below, the administrator can use the “mode” attribute in conjunction with the target XML parameter to direct the Agent to “merge” the setting with existing parameters, or simply “overwrite” existing settings.

- **“merge”**—specifies a value for a previously undefined XML setting and is ignored if a specific XML setting already exists on the client machine. This is the default behavior for the XML configuration file download feature.
- **“overwrite”**—the XML setting specified in the Agent configuration XML file automatically takes precedence over any existing value currently on the client machine.

For example, a `<Locale mode="merge">German</Locale>` entry in an Agent configuration XML file instructs the Agent not to change any previously-existing Locale setting on the client machine (merge instead of overwrite), but if no setting currently exists, then make the localization language German. If the example entry reads `<Locale mode="overwrite">German</Locale>`, then the new localized language setting for the Agent is German, regardless of whether or not any previous setting exists.

The settings available to configure for version 4.6.2.113 the Cisco NAC Agent are:

### XML Agent Configuration File Parameters Replacing Previous Windows Registry Attributes

- **VlanDetectInterval**



**Note** The maximum allowable **VlanDetectInterval** duration is increased to 900 seconds (15 minutes) in Cisco NAC Agent version 4.6.2.113. The original **VlanDetectInterval** maximum value in prior versions of the Clean Access Agent remains at 60 seconds (1 minute).

- **RetryDetection**
- **PingArp**
- **PingMaxTimeout**
- **SwissTimeout**
- **ExceptionMACList**
- **DiscoveryHost** (formerly **ServerURL**)
- **SignatureCheck** (formerly **Trust<N>**)

### New XML Agent Configuration File Parameters

- **RememberMe**

- **AutoPopUp**
- **PostureReportFilter**
- **BypassSummaryScreen**
- **DisableExit**
- **AllowCRLChecks**
- **GeneratedMAC**
- **LogFileSize** (see also [Cisco Log Packager Agent Log Compiler Application, page 14](#))
- **Locale** (see also [Agent Localization Support for “Double-Byte” Languages, page 10](#))
- **AccessibilityMode** (see also [Accessibility Support Via the JAWS Screen Reader Interface, page 11](#))

For more information on these settings and their respective default values and allowable ranges, see the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.6\(1\)](#).

### Automatic Agent Configuration XML File Updates

In Cisco NAC Appliance Release 4.6(1), the Cisco NAC Agent authentication process now includes an explicit request for Agent configuration XML file updates following SWISS discovery and negotiation. If a new XML configuration file exists at the time the Cisco NAC Agent performs authentication with Cisco NAC Appliance, the new XML file is automatically uploaded to the client machine and the settings defined in the file are automatically incorporated in Cisco NAC Agent operation according to the XML parameters configured and whether or not they are to overwrite or merge with existing settings on the client machine.

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

- **Device Management > Clean Access > Clean Access Agent > Installation**—new **Agent configuration XML file upload** option administrators can use to upload custom Agent configuration to client machines

### Cisco Log Packager Agent Log Compiler Application

Cisco NAC Appliance Release 4.6(1) introduces a new utility, the Cisco Log Packager, that users can launch on client machines to compile and view Agent log information to help diagnose and/or troubleshoot session login and operation issues. Once the Cisco NAC Agent is installed, users launch the Cisco Log Packager by navigating to the Windows Start menu command at Start > Program Files > Cisco > Client Utilities > Cisco Log Packager.

The Cisco Log Packager compiles several types of logs to enable Cisco NAC Appliance system administrators or other technical assistance personnel to easily locate and analyze critical information:

**Table 8** *Cisco Log Packager Files*

Agent Log File Name	Contents/Description
CiscoSupportReportLog.txt	This text file contains client machine system information, including CPU usage and memory allocation.
ipinfo.log	This log file contains network configuration and network connection status, including client machine IP interface status, IP statistics, and the client ARP table.

**Table 8**      **Cisco Log Packager Files**

Agent Log File Name	Contents/Description
<b>NACAgentLogPlugin.log</b>	This user-inaccessible log is one of the modules in the LogPacker component that calls the NACAgentDiags function to generate the NACAgentDiagnosticLog.txt log report.
<b>NACAgentDiagnosticsLog.txt</b>	This user-inaccessible text file contains diagnostic messages used to help debug AV issues.
<b>NACAgentDiagsLogMessages.txt</b>	This text file contains other regular log messages not used in the diagnostics output.
<b>NACAgentLogCurrent.log</b>	<p>This is an encrypted log file that contains the current Cisco NAC Agent messages from the active session and is used primarily to help debug Cisco NAC Agent issues. When the system reboots or services have been restarted, the existing <b>NACAgentLogOld.log</b> is erased, the active <b>NACAgentLogCurrent.log</b> becomes the new <b>NACAgentLogOld.log</b>, and a new <b>NACAgentLogCurrent.log</b> is created.</p> <p><b>Note</b> You can configure the size of Agent log files using the <b>LogFileSize</b> parameter in the <b>NACAgentCFG.xml</b> Agent configuration XML file (see <a href="#">Agent Configuration XML File Upload Enhancement, page 12</a>). If set to 0, no logging takes place. If set to non-zero, then the log file does not grow larger than the value (in Megabytes). The default is 5 MB. When <b>NACAgentLogCurrent.log</b> reaches the setting value, it is copied to <b>NACAgentLogOld.log</b> and a new <b>NACAgentLogCurrent.log</b> is created.</p>
<b>NACAgentLogOld.log</b>	<p>This is an encrypted log file that contains output from the previous active Cisco NAC Agent session and is also used to help debug Cisco NAC Agent issues. This file is created in one of two ways:</p> <ul style="list-style-type: none"> <li>• The “archived” log file from an active Cisco NAC Agent session that reached its maximum size (configured using the <b>LogFileSize</b> parameter in the <b>NACAgentCFG.xml</b> Agent configuration XML file).</li> <li>• When the system reboots or services are restarted, the existing <b>NACAgentLogOld.log</b> is erased, the active <b>NACAgentLogCurrent.log</b> becomes the new <b>NACAgentLogOld.log</b>, and a new <b>NACAgentLogCurrent.log</b> is created.</li> </ul>

**Note**

In Cisco NAC Appliance Release 4.6(1), the Cisco Log Packager application is only available for English and Japanese Windows platforms.

## Agent Backward-Compatibility

Cisco NAC Appliance release 4.6(1) offers backward compatibility with Windows Clean Access Agent versions 4.1.3.0 through 4.5.1.0 in addition to the most recent Agent versions available with the latest software release. Administrators can upload earlier versions of the Clean Access Agent and make them available to end users who log into Cisco NAC Appliance.

This feature also allows administrators the option to upgrade their Cisco NAC Appliance system to the latest release and “phase in” Agent upgrades for large client machine installations, rather than force Agent upgrade all at once.



### Note

Starting from release 4.6(1), the CAM no longer manages Clean Access Agent Patch/Upgrade files (CCAAgentUpgrade-4.x.y.z.tar.gz). If you are downgrading or replacing the current version of the Agent on the CAM, be sure you only upload Clean Access Agent installation files (CCAAgentSetup-4.x.y.z.tar.gz or CCAAgentMacOSX-4.x.y.z-k9.tar.gz) from the Cisco Software Download site.

## Agent Upgrade Optional When Upgrading Cisco NAC Appliance

When upgrading to Cisco NAC Appliance Release 4.6(1), the administrator can choose to retain their existing client version(s) instead of automatically upgrading the Agent to the version available with the latest software release.

## Cisco NAC Appliance Agent Reports Enhancement

When the Cisco NAC Agent performs posture assessment on client machines with 64-bit operating systems, the Agent reports in the CAM web console now accurately display the 64-bit (as opposed to 32-bit) nature of the operating system for the particular client machine.



### Note

This enhancement does not apply to backward-compatible Clean Access Agent posture assessment, as the Clean Access Agent does not support posture assessment on 64-bit client operating systems.

## Cisco NAC Windows Agent Version 4.6.2.113

The Cisco NAC Agent for Windows systems is a completely redesigned and enhanced client for Cisco NAC Appliance. It is intended to replace the Cisco Clean Access Agent starting from Release 4.6(1) and later. Refer to [Release 4.6\(1\) Compatibility Matrix, page 6](#) for additional compatibility details.

The Cisco NAC Agent version 4.6.2.113 includes the following new features for Cisco NAC Appliance Release 4.6(1):

- [Posture Assessment Support for 64-Bit Windows Operating Systems, page 10](#)
- [Agent Localization Support for “Double-Byte” Languages, page 10](#)
- [Selective Application Privilege Support for Windows Operating Systems, page 11](#)
- [Accessibility Support Via the JAWS Screen Reader Interface, page 11](#)
- [Full UTF-8 Compliance, page 11](#)
- [Agent Log Recording and Retrieval, page 11](#)
- [Support for EVDO Client Machines, page 12](#)



- [Optimized Windows Operating System Support, page 12](#)

## Mac OS X Clean Access Agent Version 4.6.0.3

To help provide Mac OS X Clean Access Agent localization for “double-byte” languages like Japanese, Cisco NAC Appliance Release 4.6(1) offers features UTF-8 compliance. The Mac OS X Clean Access Agent, Clean Access Manager, and Clean Access Server components all feature UTF-8 capability to seamlessly communicate localized messages between the Agent on the client machine and the Cisco NAC Appliance network.

## Cisco NAC Web Agent Version 4.6.0

There are no changes to the Cisco NAC Web Agent in Cisco NAC Appliance Release 4.6(1) except that the Cisco NAC Web Agent version is updated to version 4.6.0.

## Administrator Web Console Enhancements to Support Cisco NAC Agent

CAM web console elements, including the **Device Management > Clean Access > Clean Access Agent > Distribution** and **Device Management > Clean Access > General Setup > Agent Login** pages, are updated to replace the Windows “Clean Access Agent” text with “NAC Agent.” (Mac OS X Clean Access Agent text remains unchanged.)

## Features Optimized/Removed

Cisco NAC Appliance Release 4.6(1) no longer features both a Clean Access Agent Installation package and Agent Upgrade (Patch) package. All Clean Access Agent updates are performed as “re-installations” using the full Clean Access Agent installer package.

## Supported AV/AS Product List Enhancements (Windows Version 78, Mac OS X Version 3)

See [Cisco NAC Appliance Supported AV/AS Product Lists, page 18](#) for the latest AV/AS product charts.

## Cisco NAC Appliance Supported AV/AS Product Lists

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

You can access AV and AS product support information from the CAM web console under **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info**. For convenience, this section also provides the following summary and product charts. The charts list which product versions support virus or spyware definition checks and automatic update of client virus/spyware definition files via the user clicking the **Update** button on the Agent.

### Windows Vista/XP/2000

For Windows Vista/XP/2000 AV/AS support information, see the [Cisco NAC Appliance Release 4.6\(1\) Supported Windows Products](#) document optimized for UTF-8 character display.

### Mac OS X

- [Supported Mac OS X AV/AS Product List Version Summary, page 19](#)
- [Mac OS X AV Support Chart, page 20](#)
- [Mac OS X AS Support Chart, page 21](#)



#### Note

Release 4.5 and later removes support for Windows 98/ME/NT for the Clean Access Agent and Clean Access Agent Supported AV/AS Product List.



#### Note

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



#### Note

Where possible, Cisco recommends using AV Rules mapped to AV Definition Update Requirements when checking antivirus software on clients, and AS Rules mapped to AS Definition Update Requirements when checking anti-spyware software on clients. In the case of non-supported AV or AS products, or if an AV/AS product/version is not available through AV Rules/AS Rules, administrators always have the option of creating their own custom checks, rules, and requirements for the AV/AS vendor (and/or using Cisco provided pc\_checks and pr\_rules) through **Device Management > Clean Access > Clean Access Agent** (use New Check, New Rule, and New File/Link/Local Check Requirement). See the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.6\(1\)](#) for configuration details.

Note that Clean Access works in tandem with the installation schemes and mechanisms provided by supported AV/AS vendors. In the case of unforeseen changes to underlying mechanisms for AV/AS products by vendors, the Cisco NAC Appliance team will update the Supported AV/AS Product List

and/or Clean Access Agent in the timeliest manner possible in order to support the new AV/AS product changes. In the meantime, administrators can always use the “custom” rule workaround for the AV/AS product (such as pc\_checks/pr\_rules) and configure the requirement for “Any selected rule succeeds.”

Refer to [Enhancements in Release 4.6\(1\)](#), page 10 for additional details on Agent versions in this release.

## Supported Mac OS X AV/AS Product List Version Summary

[Table 9](#) summarizes enhancements made for each version update of the Supported Antivirus/Antispyware Product List for the Mac OS X Clean Access Agent. See [Mac OS X AV Support Chart](#), page 20 and [Mac OS X AS Support Chart](#), page 21 for details.

**Table 9** *Supported Mac OS X AV/AS Product List Versions*

Version	Enhancements
<b>Release 4.6(1)—4.6.0.3 Mac OS X Agent</b>	
Versions 3, 2	Minor internally used data change
Version 1	<p><b>Added AV products:</b></p> <ul style="list-style-type: none"> <li>• avast! Antivirus, 2.x</li> <li>• clamXav, 0.x</li> <li>• ClamXav, 1.x</li> <li>• eTrust Antivirus, 7.x</li> <li>• eTrust ITM Agent, 8.x</li> <li>• VirusBarrier X, 10.x</li> <li>• VirusBarrier X4, 10.4.x</li> <li>• VirusBarrier X5, 10.5.x</li> <li>• Virex 7.2, 7.2.x</li> <li>• Virex 7.5, 7.5.x</li> <li>• Virex 7.7, 7.7.x</li> <li>• VirusScan, 8.5.x</li> <li>• VirusScan, 8.6.x</li> <li>• Sophos Anti-Virus, 4.x</li> <li>• Norton AntiVirus, 10.x</li> <li>• Norton AntiVirus, 11.x</li> <li>• Norton AntiVirus, 8.x</li> <li>• Norton AntiVirus, 9.x</li> <li>• Trend Micro Security for Macintosh, 3.x</li> </ul> <p><b>Added AS products:</b></p> <ul style="list-style-type: none"> <li>• MacScan 2.x</li> </ul>

## Mac OS X AV Support Chart

Table 10 lists Mac OS X Supported AV Products for release 4.6(1) of the Cisco NAC Appliance software.

**Table 10** *Mac OS X Antivirus Product Support Chart  
Version 3, 4.6.0.3 Mac OS X Agent, CAM/CAS Release 4.6(1)*

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

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

- The Live Update column indicates whether the Agent supports live update for the product via the manual Agent **Remediate** button (configured by AV Definition Update requirement type). For products that support “Live Update,” the Agent launches the update mechanism of the AV product when the **Remediate** button is clicked. For products that do not support this feature, administrators can configure a different requirement type (such as “Local Check”) to present alternate update instructions to the user.

## Mac OS X AS Support Chart

[Table 11](#) lists Supported Mac OS X Antispyware Products for release 4.6(1) of the Cisco NAC Appliance software.

**Table 11** *Mac OS X Antispyware Product Support Chart*  
*Version 3, 4.6.0.3 Mac OS X Agent/CAM/CAS Release 4.6(1)*

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

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

# Caveats

This section describes the following caveats:

- [Open Caveats - Release 4.6\(1\), page 22](#)
- [Resolved Caveats - Release 4.6\(1\), page 50](#)
- [Resolved Caveats - Agent Version 4.6.2.113, page 53](#)



## Note

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

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

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

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

## Open Caveats - Release 4.6(1)



## Note

For caveats related to Cisco NAC Profiler, refer to the applicable version of the [Release Notes for Cisco NAC Profiler](#).

**Table 12**      **List of Open Caveats (Sheet 1 of 29)**

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsd03509	No	<p>The Time Servers setting is not updated in HA-Standby CAM web console</p> <p>After updating the “Time Servers” setting in HA-Primary CAM, the counterpart “Time Servers” setting for the HA-Standby CAM does not get updated in the web console even though the “Time Servers” setting is updated in the HA-Standby CAM database.</p>

Table 12 List of Open Caveats (Sheet 2 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsg07369	No	<p>Incorrect “IP lease total” displayed on editing manually created subnets</p> <p>Steps to reproduce:</p> <ol style="list-style-type: none"> <li>1. Add a Managed Subnet having at least 2500+ IP addresses (for example 10.101.0.1/255.255.240.0) using CAM web page <b>Device Management &gt; Clean Access Servers &gt; Manage [IP Address] &gt; Advanced &gt; Managed Subnet</b>.</li> <li>2. Create a DHCP subnet with 2500+ hosts using CAM web page <b>Device Management &gt; Clean Access Servers &gt; Manage [IP Address] &gt; Network &gt; DHCP &gt; Subnet List &gt; New</b>.</li> <li>3. Edit the newly created subnet using CAM web page <b>Device Management &gt; Clean Access Servers &gt; Manage [IP Address] &gt; Network &gt; DHCP &gt; Subnet List &gt; Edit</b>.</li> <li>4. Click <b>Update</b>. The CAM displays a warning informing the administrator that the current IP Range brings IP lease total up to a number that is incorrect. The CAM counts the IP address in the subnet twice, creating the incorrect count.</li> </ol> <p>The issue is judged to be cosmetic and does not affect DHCP functionality.</p>
CSCsg66511	No	<p>Configuring HA-failover synchronization settings on Secondary CAS takes an extremely long time</p> <p>Once you have configured the Secondary CAS HA attributes and click <b>Update</b>, it can take around 3 minutes for the browser to get the response from the server. (Configuring HA-failover synchronization on the Primary CAS is nearly instantaneous.)</p>
CSCsh77730	No	<p>Clean Access Agent locks up when greyed out <b>OK</b> button is pressed</p> <p>The Clean Access Agent locks up when the client machine refreshes its IP address. This only occurs when doing an IP release/renew, so the CAS must be in an OOB setup.</p> <p>If the <b>Automatically close login success screen after &lt;x&gt; secs</b> option is enabled and the duration set to 0 (instantaneous) in the <b>Clean Access &gt; General Setup &gt; Agent Login</b> page and the user clicks on the greyed out <b>OK</b> button while the IP address is refreshing, the Clean Access Agent locks up after refreshing the IP address. The IP address is refreshed and everything else on the client machine works, but the user cannot close the Clean Access Agent without exiting via the system tray icon, thus “killing” the Agent process.</p> <p><b>Workaround</b> Either uncheck the box or set that timer to a non-zero value. If it is set to anything else, and the user hits the greyed out OK button while the IP is refreshing, then the Agent window closes successfully.</p>

Table 12 List of Open Caveats (Sheet 3 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsi07595	No	<p>DST fix will not take effect if generic MST, EST, HST, etc. options are specified</p> <p>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.</p> <p><b>Workaround</b> 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.”</p> <p><b>Note</b> 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.</p>
CSCsj16366	No	<p>Time sync on CAS</p> <p>The CAS network module (NME-NAC-K9) appears as “not connected” in CAM web console after a router/rack power outage.</p> <p>This issue has been observed on a NME-NAC-K9 running Cisco NAC Appliance release 4.5(1) installed in a Cisco 2821 ISR in Out-of-Band Real-IP Gateway mode. In addition, the CAM returns the following event log message:</p> <p>“AutoConnectManager failed relinking CAM with CAS-i.p.add.rs.”</p> <p><b>Note</b> The time on the CAS module goes back to some time in 2006.</p> <p><b>Workaround</b> The administrator should manually reset the system time in the CAS web console.</p>



Table 12 List of Open Caveats (Sheet 4 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsk55292	No	<p>Agent not added to system tray during boot up</p> <p>When the Agent is installed on a Windows client, the Start menu is updated and Windows tries to contact AD (in some cases where the AD credentials are expired) to refresh the Start menu.</p> <p>Due to the fact that the client machine is still in the Unauthenticated role, AD cannot be contacted and an approximately 60 second timeout ensues, during which the Windows taskbar elements (Start menu, System Tray, and Task Bar) are locked. As a result, the Agent displays a “Failed to add Clean Access Agent icon to taskbar status area” error message.</p> <p><b>Workaround</b> There are two methods to work around this issue:</p> <ul style="list-style-type: none"> <li>• Allow AD traffic through the CAS for clients in the Unauthenticated role.</li> <li>• Try to start the Agent manually after the install and auto load process fails.</li> </ul>
CSCsl13782	No	<p>Microsoft Internet Explorer 7.0 browser pop-ups on Windows Vista launched from the Summary Report appear behind the Summary Report window</p> <p>This is also seen when you click on the Policy link in the Policy window. This issue appears on Vista Ultimate and Vista Home, but is not seen with Firefox or on Internet Explorer versions running in Windows 2000 or Windows XP.</p> <p><b>Note</b> This problem only happens when a Google tool bar is installed and enabled in Internet Explorer.</p>
CSCsl17379	No	<p>Multiple Clean Access Agent pop-ups with Multi NIC in L2 VGW OOB role-based VLAN</p> <p>The user sees multiple Clean Access Agent login dialogs with two or more active NICs on the same client machine pointing to the Unauthenticated network access point (eth1 IP address).</p> <p>After the first Clean Access Agent pops up and the user logs in, a second Agent login dialog pops up. If the user logs in to this additional Agent instantiation there are now two entries for the same system with both MAC addresses in the CAM’s Certified Device List and Online Users List.</p> <p><b>Workaround</b> The user can manually Disable Agent login pop-up after authentication.</p>

Table 12 List of Open Caveats (Sheet 5 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsl40626	No	<p>Cisco NAC Web Agent should handle certificate revocation dialogs similar to Clean Access Agent</p> <p>Upon logging in via the Cisco NAC Web Agent (with certificate revocation turned on or with Norton 360 installed), the user is presented with a “Revocation information for the security certificate for this site is not available. Do you want to proceed?” dialog box several times (approximately 40 to 50 times). If the user clicks <b>Yes</b> to proceed enough times, the Web Agent fails to login and reports “You will not be allowed to access the network due to internal error. Please contact your administrator.” back to the user.</p>
CSCsl40812	No	<p>The <b>Refresh Windows domain group policy after login</b> option is not functioning for Cisco NAC Web Agent</p> <p>(It is working fine with the Clean Access Agent.)</p> <p>This scenario was tested configuring a GPO policy for a Microsoft Internet Explorer browser title. The browser was not refreshed as expected after login in using the Web Agent.</p>
CSCsl75403	No	<p>Mac OS X Agent does not detect VPN interface-fails MAC filters/L3 strict mode</p> <p>This caveat addresses two issues:</p> <ol style="list-style-type: none"> <li>1. MAC filter does not work for Mac OS X client machines connected to the network in a VPN environment.</li> <li>2. L3 Strict mode does not allow Mac OS X users to log in and users see a “Access to network is blocked by the administrator” message.</li> </ol> <p>With MacOS X client machines, there are no separate interfaces created once the client machine successfully connects to the VPN concentrator. The implementation is different on Windows where a separate interface gets created having an IP address assigned by the VPN concentrator.</p> <p><b>Workaround</b> To work around these issues:</p> <ul style="list-style-type: none"> <li>• For issue 1, use IP based filters for Mac OS X client machines in VPN environment.</li> <li>• For issue 2, Disable L3 strict mode on the CAS.</li> </ul> <p><b>Note</b> This issue does not affect Windows client machines in VPN environment.</p>

**Table 12**      **List of Open Caveats (Sheet 6 of 29)**

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsl77701	No	<p>Network Error dialog appears during CAS HA failover</p> <p>When a user is logged in as ADSSO user on CAS HA system and the CAS experiences a failover event, the user sees is a pop-up message reading, “Network Error! Detail: The network cannot be accessed because your machine cannot connect to the default gateway. Please release/renew IP address manually.”</p> <p>This is not an error message and the user is still logged in to the system. The user simply needs to click on the <b>Close</b> button to continue normal operation.</p>
CSCsl88429	No	<p>User sees Invalid session after pressing [F5] following Temporary role time-out</p> <p>When a user presses [F5] or [Refresh] to refresh the web page after the Agent Temporary role access timer has expired, the user sees an “Invalid” session message. If the user then attempts to navigate to the originally requested web address, they are prompted with the web login page again and are able to log in.</p>
CSCsl88627	No	<p>Description of <b>removesubnet</b> has “updatesubnet” in op field</p> <p>The <b>removesubnet</b> API function description has “updatesubnet” listed in its operations field. The description should read “removesubnet.”</p>
CSCsm20254	No	<p>CAS duplicates HSRP packets with Cisco NAC Profiler Collector Modules enabled.</p> <p><b>Symptom</b> HSRP duplicate frames are sent by CAS in Real-IP Gateway with Collector modules enabled. This causes HSRP issues and the default gateway to go down.</p> <p><b>Conditions</b> Real-IP Gateway and Collector modules enabled on a CAS with ETH0 and or ETH1 configured for NetWatch.</p> <p><b>Workaround</b> Do not configure the CAS' ETH0 trusted interface or ETH1 untrusted interface in the NetWatch configuration settings for the CAS Collector. It is not a supported configuration.</p>

Table 12 List of Open Caveats (Sheet 7 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsm20655	No	<p>Can not do a minor upgrade for Clean Access Agent from MSI package.</p> <p>When CCAAgent.msi is used and the Clean Access Agent is upgraded to a minor version (e.g. 4.1.2.1 to 4.1.2.2) the following error message will be displayed:</p> <p>“Another version of this product is already installed. Installation of this version cannot continue. To configure or remove the existing version of this product, use Add/Remove Programs on the Control Panel.”</p> <p>This issue occurs because the Windows Installer uses only the first three fields of the product version. When a fourth field is included in the product version, the installer ignores the fourth field. For details refer to <a href="http://msdn2.microsoft.com/en-us/library/aa370859(VS.85).aspx">http://msdn2.microsoft.com/en-us/library/aa370859(VS.85).aspx</a></p> <p><b>Workaround</b> Uninstall the program from Add/Remove Programs before installing it. See also <a href="#">Known Issues with MSI Agent Installer, page 80</a>.</p>
CSCsm25788	No	<p>Avast 4.7 showing as not up to date with Cisco NAC Appliance Release 4.1(3)</p> <p>User is told that Avast needs to be updated, but shows as up to date. This occurs when user is running Avast 4.7 and the Agent version is 4.1.3.0 or 4.1.3.1</p> <p><b>Workaround</b> Create a custom check for Avast that allows the users on without verifying the definition version.</p>

Table 12 List of Open Caveats (Sheet 8 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsm61077	No	<p>ActiveX fails to perform IP refresh on Windows Vista with User Account Control (UAC) turned on.</p> <p>When logged in as a machine admin on Vista and using web login with IP refresh configured, IP address refresh/renew via ActiveX or Java will fail due to the fact that IE does not run as an elevated application and Vista requires elevated privileges to release and renew an IP address.</p> <p><b>Workaround</b> In order to use the IP refresh feature, you will need to:</p> <ol style="list-style-type: none"> <li>1. Log into the Windows Vista client as an administrator.</li> <li>2. Create a shortcut for IE on your desktop.</li> <li>3. Launch it by right-clicking the shortcut and running it as administrator. This will allow the application to complete the IP Refresh/Renew. Otherwise, the user will need to do it manually via Command Prompt running as administrator.</li> </ol> <p>This is a limitation of the Windows Vista OS.</p> <p>Alternatively, the Cisco NAC Web Agent can be used with no posture requirements enabled.</p> <p>See also <a href="#">Known Issue for Windows Vista and IP Refresh/Renew, page 79</a>.</p>
CSCso15754	No	<p>The ClamXAV live update feature may not work the first time if a “failed” ClamXAV installation requirement immediately precedes the live update in the Mac OS X Assessment Report remediation window</p> <p>If both a ClamXAV Link Distribution and a ClamXAV live update requirement are configured for Mac OS X client remediation, and the installation requirement appears right before the live definition update, then the ClamXAV live update may fail because as the installation process completes, the live update process begins and does not have a chance to read the updated ClamXAV version before launching. Therefore, if the timing is not right, users may have already started the live update while the actual ClamXAV application update tool is still copying onto the client machine.</p> <p><b>Workaround</b> The user needs to perform the remediation process again because it requires a little extra time for the live update tool to be ready following ClamXAV installation. If the user clicks the <b>Remediate</b> button again after seeing the requirement fail in the first round of remediation tasks, it works just fine.</p>

Table 12 List of Open Caveats (Sheet 9 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCso49473	No	<p>SEVERE: javax.naming.CommunicationException causes no provider list</p> <p>Configuration: ADSSO with LDAP Lookup</p> <p>If the LDAP connection to AD drops because the lookup takes a long time or the route is lost suddenly, the Agent does not receive the list of auth providers so the user is presented with a blank provider list.</p> <p>Symptom: The dropdown list of authentication providers is blank.</p> <p>Conditions: LDAP server fails to respond due to network connectivity failure or a long directory search. The failure must occur after communication to the LDAP server has begun.</p> <p>Workaround: None</p> <p><b>Note</b> <a href="#">CSCso61317</a> is a duplicate of this bug.</p>
CSCso50613	No	<p>Mac OS X Agent DHCP refresh fails if <b>dhcp_refresh</b> file does not exist</p> <p>DHCP refresh will fail with no notice (to the user or to the logs) if the <b>dhcp_refresh</b> file does not exist. The <b>dhcp_refresh</b> tool is required for all versions of Mac OS X Agents, so it always fails if the <b>dhcp_refresh</b> tool is missing regardless the Mac OS version.</p> <p><b>Workaround</b> There are three ways to work around this issue:</p> <ol style="list-style-type: none"> <li>1. Reinstalling the Mac OS X Agent automatically reinstalls the missing <b>dhcp_refresh</b> file.</li> <li>2. Users can sign on to Cisco NAC Appliance via web login. The Java applet installs the <b>dhcp_refresh</b> tool if the <b>Install DHCP Refresh tool into Linux/MacOS system directory</b> option is checked under <b>User Page &gt; Login Page &gt; Edit &gt; General</b>.</li> <li>3. When using the Apple Migration Assistant, the user can try to include <b>/sbin/dhcp_refresh</b> in the migration list.</li> </ol>

Table 12 List of Open Caveats (Sheet 10 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCso61317	No	<p>When LDAP lookup fails for an AD SSO user, the Provider list in the Agent dialog is empty</p> <p><b>Scenario 1</b> AD SSO configured with LDAP lookup</p> <p>When the LDAP lookup fails for the user (some misconfiguration or not able to reach the right server to find the user), the Agent displays a login window without a Provider list. This happens because the user has already passed the login stage, but has failed the lookup stage.</p> <p><b>Scenario 2 (less common)</b> The user is logged in to a machine that is not part of the domain, but the user does have an AD account.</p> <p>Steps that occur:</p> <ol style="list-style-type: none"> <li>1. A TGT, obtained with the AD account, is granted.</li> <li>2. The ST for the CAS is granted.</li> <li>3. Agent passes the local account information since the user has logged in locally to the machine.</li> <li>4. Authorization fails which causes the blank provider list.</li> </ol> <p><b>Note</b> This bug is a duplicate of <a href="#">CSCso49473</a>.</p>
CSCsr50995	No	<p>Agent doesn't detect Zone Alarm Security definitions correctly</p> <p>Symptom: User fails posture assessment when checking for AV definitions for Zone Alarm Security Suite 7.0.</p> <p>Conditions: This occurs using either the Any AV check or the Checkpoint Any check.</p> <p><b>Workaround</b> Create a custom check for Zone Alarm Security Suite definition.</p>

Table 12 List of Open Caveats (Sheet 11 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsr52953	No	<p>RMI error messages periodically appear for deleted and/or unauthorized CASs in CAM event logs</p> <p>Clean Access Servers connected to a CAM can periodically appear as “deleted” or “unauthorized” in the CAM event logs even though the CAS is functioning properly and has not experienced any connection issues with the Clean Access Manager. Error message examples are:</p> <ul style="list-style-type: none"> <li>“SSL Communication 2008-07-23 00:31:29 SSLManager:authorizing server failed CN=10.201.217.201, OU=Perfigo, O=Cisco Systems, L=San Jose, ST=California, C=US”</li> <li>“SSL Communication 2008-07-23 00:31:29 RMISocketFactory:Creating RMI socket failed to host 10.201.217.201:java.security.cert.CertificateException: Unauthorized server CN=10.201.217.201, OU=Perfigo, O=Cisco Systems, L=San Jose, ST=California, C=US”</li> </ul> <p><b>Workaround</b></p> <ul style="list-style-type: none"> <li>Reboot the CAS and wait for the CAM to re-establish connection.</li> <li>Reboot the CAM after deleting and removing the CAS from the Authorized CCA Server list using the CAM <b>Device Management &gt; CCA Servers &gt; Authorization</b> admin web console page.</li> </ul>
CSCsr61106	No	<p>Cannot upgrade CAS via CAM's web UI</p> <p>An HTTP status 500 error message occurs stating “java.lang.OutOfMemoryError” when upgrading the CAS via the CAM’s web user interface if the CAM’s memory is less than 1GB, or during CAS software upgrade via the CAM’s web user interface using 4.5.0 upgrade package.</p> <p>This problem is seen with non-Cisco hardware with only 512MB memory installed; i.e. Dell’s 750, 850, or 860.</p> <p>With 4.5.0, the problem is seen with all Cisco appliances including NAC-3140, NAC-3310, NAC-3350 &amp; NAC-3390.</p> <p><b>Workaround</b> Upgrade the CAS using the SSH method.</p>



Table 12 List of Open Caveats (Sheet 12 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsr90712	No	<p>Symantec Antivirus delays Clean Access Agent startup</p> <p>The Agent takes a long time to pop up on a client machine with real-time antivirus scanning enabled and operating.</p> <p><b>Workaround</b></p> <p>Exclude the Clean Access Agent AV411 directory from Symantec Antivirus scanning. See <a href="http://service1.symantec.com/support/ent-security.nsf/docid/2002092413394848">http://service1.symantec.com/support/ent-security.nsf/docid/2002092413394848</a>.</p> <p><b>Note</b> The step to configure Extensions can be omitted.</p> <p>For Vista, refer to <a href="http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008111414031848">http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008111414031848</a>.</p>
CSCsr95757	No	<p>CAM intermittently stops processing SNMP MAC notification traps from the switch</p> <p>This issue can occur on different edge switches. Once the problem is present, no further SNMP MAC notification traps are processed from the CAM for the switch in question.</p> <p><b>Note</b> There is no <b>perfigo-log0.log.0</b> information, but a <b>tcpdump</b> from a CAM CLI session indicates that the CAM is receiving SNMP MAC notification traps.</p> <p><b>Workaround</b> To re-establish correct SNMP trap handling on the CAM, open a CAM CLI session and enter the following commands:</p> <pre>service perfigo stop service perfigo start</pre> <p>The CAM immediately starts processing the SNMP MAC notification traps from the problem switch(es).</p> <p><b>Note</b> After a period of time, however, this problem may appear again.</p>
CSCsu47350	No	<p>Invalid version number displayed in CAM backup snapshot web page</p> <p>When the administrator navigates to another page in the CAM web console during the backup snapshot process, the resulting snapshot version number is invalid.</p>

Table 12 List of Open Caveats (Sheet 13 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsu63247	No	<p>DHCP IP refresh not working for some Fedora core 8 client machines</p> <p>DHCP IP refresh does not work on Fedora core 8 clients logging in to a Layer 3 Real-IP Gateway CAS using the current version of the Java applet. As a result, Fedora core8 clients must use web login to gain access to the Cisco NAC Appliance network.</p> <p><b>Note</b> There is no known workaround for this issue</p>
CSCsu63619	No	<p>Out-of-Band switch port information from OUL/CDL missing upon login after upgrade</p> <p>OOB switch port information in Online Users List/Certified Devices List is missing upon login after upgrading to release 4.5.</p> <p>This issue occurs when the client machine has not been disconnected from the network (has not generated a MAC notification trap from the switch), and logs into the OOB network after upgrade.</p> <p><b>Workaround</b> Disconnect the client machine from the switch and reconnect. This generates the MAC linkdown notification trap from the switch to the CAM updating the Discovered Clients list with the appropriate port information for this client machine.</p> <p><b>Note</b> This issue is cosmetic and does not affect Cisco NAC Appliance functionality.</p>
CSCsu69247	No	<p>ERROR: File type requirements does not exist</p> <p>During CD installation of Cisco NAC Appliance Release 4.5, users can see the following error message in the nac_manager.log file:</p> <p>“2008-09-21 19:25:55.592 -0700 ERROR com.perfigo.wlan.web.admin.DMSSoftwareManager - DMSM syncDMSSoftware: Directory('/perfigo/control/tomcat/webapps/packages/') for file type requirements does not exist”</p> <p>This is a benign error message related to webapps packages that have been relocated in the installation script and has no impact on image installation.</p>

Table 12 List of Open Caveats (Sheet 14 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsu78379	No	<p>Bandwidth settings for Receiver CAM roles should not change after Policy Sync</p> <p>Steps to reproduce:</p> <ol style="list-style-type: none"> <li>1. Create role on Master CAM, r1</li> <li>2. Edit Upstream and Downstream Bandwidth fields of r1 to equal 1Kbps</li> <li>3. Create role on Receiver CAM, r2</li> <li>4. Edit Upstream and Downstream Bandwidth fields of r2 to equal 2 Kbps</li> <li>5. Select role-based Master Policies to Export and perform manual sync</li> <li>6. Upstream and Downstream Bandwidth fields for role r1 on Receiver CAM are changed to -1 (not 2 Kbps and not 1 Kbps).</li> </ol> <p><b>Note</b> Receiver's Up/Down Kbps, Mode, Burst should either not change or should be the same as the Master.</p>
CSCsu84848	No	<p>CAM should set the switch port to Authentication VLAN before removing from OUL and DCL</p> <p>The CAM should set the switch port to the Authentication VLAN before removing the user from Online Users List and Discovered Client List when the Switch or WLC entry is deleted from the CAM.</p> <p><b>Workaround</b> Bounce the switch port to clear the OUL and DCL.</p>
CSCsu84977	No	<p>CAS: ERROR /proc/click/intern_filter_group/failsafe</p> <p>The following error message can appear to users during CD installation of Cisco NAC Appliance release 4.5 in Clean Access Servers:</p> <p>“com.perfigo.wlan.jmx.Shell - /proc/click/intern_filter_group/failsafe (No such file or directory)”</p> <p>This error message is related to a recently-removed file failsafe and has no impact on CD installation.</p>

Table 12 List of Open Caveats (Sheet 15 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsu88594	No	<p>Removal of www.perfigo.com Root CA from GUI</p> <p>The www.perfigo.com Root CA should be removed from the GUI.</p> <p>With the default configuration there is no CA certificate button to offer on the web (or user) login page. The Cisco NAC Appliance administrator must configure user page content and specify whether or not to offer the Root CA along with its content from the dropdown menu (either the www.perfigo.com CA certificate or an imported third-party CA certificate—the default choice is the www.perfigo.com CA).</p> <p><b>Workaround</b> To change this behavior go to <b>Administration &gt; User Pages &gt; Login Page &gt; Edit &gt; Content</b> and deselect the <b>Root CA</b> table entry.</p>
CSCsu88796	No	<p>CAM upgrade: Error message in 4.1(3)-to-4.5 upgrade details log</p> <p>When upgrading the Clean Access Manager from release 4.1(3) to 4.5, users may see a benign “scriptlet failed” error message listed in the upgrade details log file. This error message has no impact on upgrade to release 4.5.</p>
CSCsu89385	No	<p>“not a symbolic link” error message in 4.1(3)-to-4.5 CAS upgrade details log</p> <p>When administrators upgrade Clean Access Servers from release 4.1(3) to release 4.5, they may see a number of “not a symbolic link” error messages in the upgrade details log. These error messages have no effect on the CAS upgrade.</p> <p><b>Note</b> You can run <code>./showstate.sh</code> in the CAS CLI to verify successful upgrade.</p>
CSCsv18261	No	<p>HA Failover database sync times out in event log after reboot</p> <p>In Cisco NAC Appliance release 4.5, the CAM HA database copy function times out when the active CAM fails over and becomes the standby CAM. (Event log entries show that the database copy function times out.) This situation arises when the inactive CAM comes up and attempts to copy the database from the active CAM, but the database is still locked by the [now standby] CAM. This issue is not seen during normal operation and database sync because the entries are copied in real time.</p> <p><b>Note</b> In Cisco NAC Appliance releases prior to 4.5, there is no timeout function, and the database sync takes less time to complete because the CAM does not lock the database or verify the copy function.</p>

Table 12 List of Open Caveats (Sheet 16 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsv18995	No	<p>Three requirement types allow administrators to select single Windows XP/Vista operating systems when “All” is checked</p> <p>When creating a new Windows Update, Launch programs, and/or Windows Server Update Services (WSUS) requirement type, and checking the “Windows XP (All)” or “Windows Vista (All)” options, the individual OS options are also still selectable (although they should not be).</p> <p><b>Note</b> This issue is not seen on the other requirement types.</p> <p>There is no known workaround for this issue</p>
CSCsv20270	No	<p>Conflicting CAM's eth1 HA heartbeat address with 4.5.0 after upgrade</p> <p>The perfigo service cannot be started on the standby CAM because both the eth1 interface of HA CAMs have the same IP address: either 192.168.0.253 or 192.168.0.254.</p> <p>This happens in an HA setup when one of the CAMs is upgraded from release 4.0(x) to 4.5 and the other CAM is fresh CD installed.</p> <p><b>Workaround</b> Change to use the manual setting for eth1 on the fresh CD installed node or re-apply the HA config on the upgraded node.</p>
CSCsv22418	No	<p>CAS service IP not reachable after standby reboot due to race condition</p> <p>The Active CAS's service IP become unreachable after standby CAS reboot.</p> <p>In a rare race condition, the standby CAS temporarily becomes active for very short period of time after reboot.</p> <p><b>Workaround</b></p> <ol style="list-style-type: none"> <li>1. Increase the “Heartbeat Timeout” value from the recommended 15 seconds to 30 seconds.</li> <li>2. Or, run the heartbeat interface on Interface 3 (eth2 or eth3).</li> </ol>

Table 12 List of Open Caveats (Sheet 17 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsv78301	No	<p>VPN SSO login does not work with VPN in managed subnet after upgrade to Cisco NAC Appliance release 4.5</p> <p>Prior to release 4.5, the Clean Access Server associates the client with the VPN IP address and VPN Concentrator's MAC address after the first login. From there, the SWISS protocol only checks the IP address from the Agent and reports back to the Agent that the client is logged in (regardless of whether the client is connected via Layer 2 or Layer 3).</p> <p>In release 4.5, the SWISS protocol checks the MAC address for Layer 2 clients, but the MAC address reported by the Agent (which is the real client MAC address) is different from the one the CAS gets for the client (the VPN concentrator MAC address). As a result, the SWISS protocol tells the Agent that the client machine is not logged in (due to the different MAC addresses recorded) and the Agent launches the login dialog repeatedly, never able to complete login.</p> <p><b>Workaround</b> Remove the subnet making up the client machine address pool from the collection of managed subnets and create a Layer 3 static route on the CAS untrusted interface (eth1) with VPN concentrator's IP address as the gateway for the VPN subnet using the CAM web console <b>Device Management &gt; CCA Servers &gt; Manage [CAS_IP] &gt; Advanced &gt; Static Routes</b> page.</p>
CSCsv92867	No	<p>DB conversion tool (Latin1 to UTF8)-iconv cannot work with &amp;#8224; format</p> <p>Release 4.5 and earlier Clean Access Managers with foreign characters in the database cannot be upgraded to release 4.6(1).</p> <p><b>Workaround</b> To upgrade from release 4.1(6) or 4.5:</p> <ul style="list-style-type: none"> <li>• Perform a fresh install of release 4.6(1) (recommend).</li> <li>• Remove any foreign characters from the database prior to upgrade.</li> </ul>

Table 12 List of Open Caveats (Sheet 18 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsw39262	No	<p>Agent cannot be launched when switching between users in Vista</p> <p>The Cisco NAC Agent does not support Windows Fast User Switching. The effect is that the primary user is the only user that:</p> <ul style="list-style-type: none"> <li>• Can log into the Clean Access Server and based on the level of authentication will dictate the system's access to the network.</li> <li>• Will see the NAC Agent tray icon.</li> <li>• Will be able to re-authenticate if kicked off the network via the Clean Access Server.</li> </ul> <p><b>Note</b> This does not impact client machines that are part of a Windows Domain. It also does not impact users who log out before logging in as another user.</p> <p><b>Workaround</b> Logging out the first user or closing the Cisco NAC Agent before Fast Switching eliminates this problem.</p>
CSCsw45596	No	<p>Username text box should be restricted with max no of characters</p> <p>The Username text box is presently taking the characters such that the total size is ~5kb. It is better to have the upper bound for the Username text box to hold the number of characters that it can take.</p>
CSCsw67476	No	<p>Mac OS X Agent upgrade cannot be restarted once stopped</p> <p>User is not able to log in again (no agent screen or icon available) when they cancel the Mac OS X Agent upgrade process.</p> <p><b>Note</b> This issue has been observed when upgrading from release 4.5 to 4.6(1).</p> <p><b>Workaround</b> Manually start the agent which then started the upgrade portion.</p>
CSCsw88911	No	<p>Mac Agent freezes on login dialog, but remains operational</p> <p>The tray icon of a Mac OS X Agent logged into a Cisco NAC Appliance OOB deployment shows Click - Focus then Click again and is hung (looks like logging in).</p> <p><b>Workaround</b> Operationally, everything is running normally (the machine is OOB and logged in per CAM and client) just the user interface is locked up.</p>
CSCsw89027	No	<p>Mac OS X Agent logs can grow too large in debug and do not clean up</p> <p>When Agent logging is set to "Defect", Mac OS X Agent logs grow too large.</p> <p><b>Workaround</b> Do not compile Mac OS X Agent logs in debug mode for extended periods of time.</p>

Table 12 List of Open Caveats (Sheet 19 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsx03338	No	<p>HTTP packet to a host using reversed IP address after connection on Mac OS X client</p> <p>The Mac Agent sends a packet to UDP port 80 to the reversed IP address of the client's default gateway every 5 seconds.</p> <p><b>Note</b> This occurs only on the Mac Agent, and is a side effect of the Vlan Change Detection feature added in Cisco NAC Appliance Release 4.1(3).</p> <p><b>Workaround</b> Disable the access-to-auth vlan-detection by following the instructions at <a href="http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/461/cam/m_oob.html">http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/461/cam/m_oob.html</a>.</p>
CSCsx05054	No	<p>DHCP does not work with IGNORE fallback policy and CAS Failover</p> <p>If CAS Fallback policy is set to IGNORE and the CAM becomes unreachable from CAS, the CAS blocks all traffic and CAS DHCP stops working.</p> <p><b>Workaround</b> Setting the CAS Fallback policy to "Allow All" or "Block All" solves the issue. Also, if you can ensure that the active CAS does not fail over when CAM is unreachable, this situation should not happen.</p>
CSCsx05141	No	<p>Clients cannot get IP addresses from CAS DHCP relay agent in CAS fail-open with CAS fallback scenario</p> <p>Steps to reproduce this issue:</p> <ol style="list-style-type: none"> <li>1. Log into the CAM web console and set CAS Fallback policy as "Allow All."</li> <li>2. Configure DHCP relay on CAS and configure IP address of external DHCP server. All clients should be able to get the IP at this point.</li> <li>3. Make the CAM unreachable from CAS.</li> <li>4. Active CAS fails-open within 5 minutes. Clients can still get IP address assignments from the DHCP server (all traffic is allowed).</li> <li>5. Fail-over the CAS by executing "service perfigo stop" or rebooting the appliance. The HA-Secondary CAS now becomes Active and dhcrelay starts on the CAS if you enter netstat.</li> </ol> <p>Even though the administrator can see dhcrelay functioning, clients are now unable to get IP addresses through new Active CAS.</p>
CSCsx18496	No	Cisco Log Packager crashes on XP Tablet PC with Restricted User credentials



Table 12 List of Open Caveats (Sheet 20 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsx25557	No	<p>NOD32 3.x Def date is not recognized by Clean Access Agent</p> <p><b>Note</b> The support chart incorrectly showed that this version can be updated. Version 3.x is not able to be updated by the Agent. The update will have to be performed manually from the NOD32 console.</p> <p><b>Note</b> There is no known workaround for this issue.</p>
CSCsx27857	No	<p>With session timer disabled for the Agent Temporary role, version 4.6.0.3 of the Mac Agent times out</p> <p>If the Temporary role timer disabled on the CAM, the Mac Agent times out right away.</p> <p><b>Note</b> There is no known workaround for this issue.</p>
CSCsx29191	No	<p>Mac OS X Agent has no 'APPLE'+TAB presence</p> <p>When using the Mac OS X Agent, the GUI focus can get lost and is hard to regain. This issue was observed during upgrade.</p> <p><b>Workaround</b> Using hot corners to show all applications. With this tool, users can find the Agent and continue the process.</p>
CSCsx35438	No	<p>Clean Access Manager read timeout reached when deleting many DHCP IPs at once</p> <p>After upgrading to or installing release 4.1(8) and deleting hundreds of DHCP IPs at once, the Clean Access Server becomes unmanageable. This issue affects Clean Access Servers configured as a DHCP server on which the administrator tries to delete more than 800 DHCP IPs at once.</p> <p><b>Workaround</b> Please see <a href="#">Known Issue with Mass DHCP Address Deletion, page 73</a>.</p>
CSCsx35911	No	<p>Mac OS X Agent does not pop up for login and click-focus does not get user's attention</p> <p>When the user moves from a non-Cisco NAC Appliance network to a Cisco NAC Appliance network, the Agent login dialog does not automatically appear. Click-focus can resolve the issue, but the is not generally obvious to the user. The result of this issue is that users would likely be stuck in the authentication network and/or assigned to a restricted role for the duration of their session.</p> <p><b>Workaround</b> Click on the upper right icon that is saying click focus and then login.</p>

Table 12 List of Open Caveats (Sheet 21 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsx37073	No	<p>Cisco NAC Agent does not pop-up if authentication server name is \\</p> <p>Steps to reproduce:</p> <ol style="list-style-type: none"> <li>1. Create a Kerberos authentication server named \\ in addition to Local DB.</li> <li>2. Go to <b>Login Page &gt; Content</b> and check Provider Label, <b>Local DB</b>, \\ (def provider).</li> <li>3. Let the Cisco NAC Agent pop-up. User sees \\ and Local DB as Server options. (This is as expected.)</li> <li>4. Go to <b>Login Page &gt; Content</b> and uncheck <b>Local DB</b>.</li> <li>5. Let the Cisco NAC Agent pop-up again. This time, user sees only the \\ Server option. (This is also as expected.)</li> <li>6. Go to <b>User Management &gt; Auth Servers</b> and delete \\.</li> <li>7. Close the Cisco NAC Agent window, which does not pop-up again.</li> </ol> <p>Repeat the above steps with authentication server named “myKerberos” instead of \\. The CAM returns a “Clean Access Server is not properly configured. Please contact your administrator if the problem persists” error message.</p> <p><b>Workaround</b> Avoid non-alphabetic naming conventions when configuring authentication servers in Cisco NAC Appliance.</p>
CSCsx45051	No	<p>Agent may proceed with AV/AS auto remediation while it's not supported</p> <p>For an AV/AS Definition Update Requirement Type with Automatic Remediation Type and Antivirus/Anti-Spyware Vendor Name configured as ANY, when the client fails the requirement, the Agent should automatically launch the AV (or AS) update on the AV product for which the Agent supports live update. If live update is not supported, the Agent should prompt the user to perform manual remediation. With this issue, the Agent may proceed with auto remediation on a product for which the Agent does not support live update. As a result, auto remediation will fail, and the agent will prompt user to do manual remediation.</p> <p><b>Note</b> This issue is observed with MS Live One 2.x. Auto Remediation fails when configured for MS Live One 2.x.</p> <p><b>Workaround</b> Remediate AV manually while in the temporary role.</p>

**Table 12**      **List of Open Caveats (Sheet 22 of 29)**

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsx47987	No	<p>Incorrect behavior when client wired/wireless NIC on same subnet as CAS</p> <p>Scenario to reproduce:</p> <ul style="list-style-type: none"> <li>Client is connected through both wired and wireless port to the same OOB CAS.</li> <li>Wireless NIC IP address is on the same subnet as that of CAS.</li> <li>Wired port is assigned a lower metric compared to wireless, so wired is the preferred port.</li> <li>Upon login, client connects through wireless and is listed in the CAM's CDL and OUL as connected via wireless interface even though the wired network path is preferred.</li> </ul> <p>As a result, the client is not able to ping the CAM or access any outside network.</p>
CSCsx49160	No	<p>Cisco NAC Agent shows one less authentication provider if one of the provider names is \</p> <p>Steps to reproduce:</p> <ol style="list-style-type: none"> <li>Create a Kerberos authentication server called my_krbr.</li> <li>Create a login page and check the <b>Local DB</b> and <b>my_krbr</b> (def provider) Provider Labels.</li> <li>Let the Cisco NAC Agent pop-up. Both my_krbr (def provider) and the Local DB provider options are available.</li> <li>Go to the list of Authentication Servers and rename my_krbr to \.</li> <li>Go to the Login page. \ appears as the new Kerberos name.</li> <li>Close the Cisco NAC Agent and let it automatically pop-up again.</li> </ol> <p>This time, the authentication provider list only shows Local DB—\ is missing.</p> <p><b>Workaround</b> Avoid non-alphabetic naming conventions when configuring authentication servers in Cisco NAC Appliance.</p>
CSCsx78577	No	<p>ClamAV not showing def date</p> <p>ClamAV does not provide the definition date to the Agent.</p> <p><b>Workaround</b> There is no workaround at this time. This is a known issue.</p>

Table 12 List of Open Caveats (Sheet 23 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsx80459	No	<p>JAVA_OPTS_TO of "" seen in CAM upgrade details</p> <p>When upgrading the Clean Access Manager to release 4.5(1), the additional message "Ended up with JAVA_OPTS_TO of "" may be seen in the upgrade details text displayed under Administration &gt; CCA Manager &gt; Software Upload. This message does not affect upgrade and is safe to ignore.</p> <p>Welcome to the CCA Manager migration utility.</p> <p>...Upgrading to newer rpms of 4.5.1...done.</p> <p>...Upgrading CCA files...Ended up with JAVA_OPTS_TO of ""</p> <p>Preparing...</p> <p>#####</p> <p>nac_manager</p> <p>#####</p>
CSCsx81395	No	<p>Sophos AV Definition rule fails even if Mac OS Agent has the latest definition</p> <p>The remediation window pops up for updating the Sophos definition files on the Mac OS Agent even though Sophos is updated.</p> <p>This occurs if Sophos is installed on the Mac OS client and an AV definition check for Sophos is configured on the CAM.</p> <p><b>Workaround</b> There is no workaround at this time.</p>
CSCsx95230	No	<p>Length of token is not printed in the ADSSO logs</p> <p>When ADSSO logging is changed to DEBUG for troubleshooting purposes, the ADSSO logs display the token but not the token size.</p> <p><b>Workaround</b> None.</p>

Table 12 List of Open Caveats (Sheet 24 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsy00609	No	<p>Role mapping uses cached entry on quick reconnects</p> <p>Users who disconnect and immediately reconnect using different credentials (VPN group, etc.) may still be mapped to their role based on previous credentials. These same users are mapped correctly if they wait a few minutes between disconnecting and reconnecting.</p> <p>This issue was reported in Cisco NAC Appliance release 4.1(6) using VPN Single Sign On (SSO) and a combination of the username and class attribute (user group) to map the user. Issue has also been observed using other criteria, such as client address, group, etc.</p> <p><b>Workaround</b> This issue is not actually a bug. Caching behavior is configurable using the <b>Authentication Cache Timeout</b> setting available on the <b>CAM User Management &gt; Auth Servers &gt; List/New</b> web console page. If it is desired to never cache user login, set this timer to 0.</p> <p><b>Note</b> This workaround may affect CAM performance due to increased authentication traffic for multiple users logging into Cisco NAC Appliance.</p>
CSCsy32119	No	<p>Cisco NAC Appliance CAM/CAS need ability to set port speed/duplex manually</p> <p>There have been instances where switch ports are not negotiating the same as other ports on the same appliance. This is inefficient since the ports in question do not necessarily use the highest possible speed. In addition, there could be collisions, FEC, and errors on a port if there is a mismatch.</p> <p><b>Note</b> There is no known workaround for this issue.</p>
CSCsy45807	No	<p>Mac OS X Agent does not pop up using Sprint Wireless</p> <p>This issue has been encountered using Sprint Wireless Novatel U727 on 2 different Mac OS X client machines.</p>
CSCsz19346	No	<p>Korean log packager GUI translations/buttons are garbled &amp; some missing</p> <p><b>Workaround</b> Some of the buttons are still readable. Click <b>Collect Data &gt; Locate File</b> and then click <b>Exit</b>.</p>

**Table 12**      **List of Open Caveats (Sheet 25 of 29)**

	Software Release 4.6(1)	
DDTS Number	Corrected	Caveat
CSCsz19912	No	<p>Log Packager CiscoSupportReport file shows ##### in place of system info</p> <p>The system logs created by the log packager are showing ##### instead of actual data, as in the following examples:</p> <pre>04/23/2009 10:49:22 W32Time (ID=0x825a0083): NtpClient# 'CCAVPN-AD'# DNS ## ### ## ## ##### ## ## ## #####. NtpClient# 15# ## ## ##### # ### ## ## ## # ## ##. ##: ## #### #####. (0x80072AF9).</pre> <pre>04/23/2009 10:49:21 W32Time (ID=0x825a0083): NtpClient# 'CCAVPN-AD'# DNS ## ### ## ## ##### ## ## ## #####. NtpClient# 15# ## ## ##### # ### ## ## ## # ## ##. ##: ## #### #####. (0x80072AF9).</pre> <p>This issue occurs on Japanese, Korean, and Chinese systems using Cisco Log Packager.</p> <p><b>Note</b> There is no known workaround for this issue. Log Packager is still functioning, but it is missing some non-critical system troubleshooting information.</p>
CSCsz38970	No	<p>Accessibility: login displays not announced</p> <p>After you log into Windows, you see the ADSSO display and then the local corporate display. JAWS does not announce the Cisco NAC Agent displays.</p> <p><b>Note</b> This issue has been observed in a deployment where JAWS is set to run at system startup.</p> <p><b>Workaround</b> You have to select the Cisco NAC Agent from the taskbar to have the Agent display announced.</p>
CSCsz48766	No	<p>MAC Agent VLAN change detection logic causes AnyConnect to disconnect</p> <p>Anyconnect client constantly loses connection to VPN network when using the Mac OS X Clean Access Agent with the VlanDetectInterval set to 5 seconds.</p> <p><b>Workaround</b> The <b>settings.plist</b> file does not contain the VlanDetectInterval value by default, so Mac users must add a “VlanDetectInterval value 0” child string and then restart the Agent to address the AnyConnect connection issues.</p>
CSCsz48847	No	<p>Accessibility: after successful log-in, JAWS is still on Cisco NAC Agent page</p> <p>JAWS stays on The Cisco NAC Agent window even though no Agent window is displayed.</p> <p><b>Workaround</b> Press the Windows key to go back to the Windows desktop.</p>

Table 12 List of Open Caveats (Sheet 26 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsz49147	No	<p>Accessibility: JAWS does not announce installer after upgrade</p> <p>During upgrade of the Cisco NAC Agent, the MS installer window is not announced.</p> <p><b>Note</b> This does not impact the upgrade process.</p> <p><b>Workaround</b> A blind user will need to check the running applications in the Windows taskbar.</p>
CSCsz80035	No	<p>“ANY” AV remediation for Trend Micro 17.1 fails</p> <p>The AV update for Trend Micro version 17.1.1250 shows a failure in the Cisco NAC Agent window, but the update is successful.</p> <p><b>Workaround</b> Click <b>OK</b> on the error display. The AV update is actually successful.</p>
CSCsz83270	No	<p>Agent file download fails at lower speed WAN links between CAS and CAM</p> <p>When the Agent is uploaded to the CAM, the .tar file gets partially downloaded and removed several times on CAS before it is successfully downloaded and its contents unpacked. As a result the client does not pop-up for a long time for upgrade or fresh install from the Cisco NAC Appliance web login page.</p> <p>This happens during agent upgrade or download from web page when CAS and CAM are separated by a WAN link (512kbps/256kbps).</p> <p><b>Workaround</b> If agent does not get downloaded for a long time, remove the contents of /perfigo/access/apache/www/perfigo_download to start the download of the file.</p> <p><b>Note</b> Problem usually corrects itself after a while, but if it does not, Cisco recommends following this workaround.</p>
CSCsz85892	No	<p>Web login display Guest ID instead of Username</p> <p>Steps to reproduce:</p> <ol style="list-style-type: none"> <li>1. Add a Kerberos auth server named “k1.”</li> <li>2. Enable the Local DB and “k1” providers on the Login Page, and make “k1” the default provider.</li> <li>3. Open a browser and check that Username is there and “k1” is the default provider.</li> <li>4. Delete “k1” from the roster of Auth Servers.</li> <li>5. Open another browser and note that the user name is now “Guest ID.”</li> </ol>

Table 12 List of Open Caveats (Sheet 27 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsz92761	No	<p>CAM GUI and publishing behavior during DB restore</p> <p>When a CAM snapshot is restored from a database, the CAM web console times out, and once refreshed, shows the associated CAS is offline as a result of triggering a database restoration.</p> <p>This issue occurs when the CAM and CAS are connected via WAN links (T1/256k/512k) with several CASs experiencing at least 400ms delay.</p> <p><b>Note</b> After the CAM completes its parallel connection at the end of the database restoration, it starts to publish to many of the CASs via serial connection.</p> <p><b>Workaround</b> DBrestore happens and CAS do get connected and publishing completed.</p>
CSCsz97199	No	<p>McAfee AV_TotalProtectionforSmallBusiness_4_7_x upgrade to 5.0 issues</p> <p>When auto-upgrading the McAfee AV_TotalProtectionforSmallBusiness_4_7_x to version 5.0 via the Cisco NAC Agent, all updates are downloaded and installed for 4.7, but then an automatic upgrade to 5.0 fails.</p> <p><b>Note</b> There is no known workaround for this issue.</p>
CSCta02433	No	<p>“Swiss Communication Logging” buttons do not work</p> <p>Even though the option has been enabled in the Administrator web console page, Swiss log messages are missing from the nac_server.log file.</p> <p><b>Workaround</b> The “CCA Server General Logging” and “CAS/CAM Communication Logging” options must be set to same desired log level.</p>
CSCta03527	No	<p>Discovery Host can not be changed by uploading XML on CAM</p> <p>When adding a new XML Agent configuration file to be pushed to Agents via the CAM upload page, the Discovery Host does not get changed when using the “overwrite” option.</p> <p><b>Workaround</b> Manually edit the XML file on the client machine or keep using the Discovery Host address specified on the CAM.</p>
CSCta12544	No	<p>Server communication error upon web and Agent login</p> <p>This issue can occur when a brand new CAS is connected to a CAM pair that has been upgraded from an older release of Cisco NAC Appliance to release 4.5 or later, resulting in unreliable communication between the CAM and CAS.</p> <p>For more information, see <a href="#">CAM-CAS Shared Secret Mismatch Following New CAS Installation</a>, page 81.</p>



Table 12 List of Open Caveats (Sheet 28 of 29)

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCta25247	No	<p>Nessus scan fails on Vista</p> <p>Nessus scan always fails on Vista client machines logging in with the Cisco NAC Agent. The Agent returns the following error message on the client:</p> <p>“Clean Access Server is not available on the network. Please contact your administrator if the problem persists.”</p> <p><b>Note</b> There is no workaround for this issue, as the Cisco NAC Agent does not support Nessus-based network scanning.</p>
CSCta34052	No	<p>Java Memory leak causing CAM to crash</p> <p>Customers using Kerberos or LDAP over GSSAPI see older versions of Java running out of memory due to a leak. This memory leak has been addressed in more recent versions of java. (Specifically, Java 6.)</p> <p><b>Workaround</b> While Cisco validates the use of Java 6 in Cisco NAC Appliance, customers may want to use LDAP with simple authentication over SSL.</p>
CSCta35376	No	<p>If Agent Popup option disabled, Agent does not download config file</p> <p>If the Agent “Popup Login Window” systray option is disabled, the Agent does not download the Agent configuration XML file from the CAM. As a result, the user cannot install configuration changes uploaded to the CAM on the client machine.</p> <p><b>Workaround</b> Users can manually enable the “Popup Login Window” option from the system tray.</p>
CSCta35732	No	<p>Deleting subnet filters causes CASs to disconnect</p> <p>When you delete the subnet filter one after another from the CAM, the web console slows down and loses connection to the associated CAS.</p> <p>The CAM connects to all the CASs every few minutes via serial interface and checks for heartbeats. If a CAS goes offline, the CAM tries to connect to the CAS to resume connection. However, the wait time depends on the number of CASs attached to the CAM.</p> <p><b>Note</b> After a few minutes, CASs come back online.</p>
CSCsx52263	No	<p>NAC Appliances always assume USA keyboard layout</p> <p>When connected via Keyboard and Monitor, if a keyboard with layout other than US layout is used, the Cisco NAC Appliances do not recognize the keyboard and it is possible to erroneously enter different characters.</p> <p><b>Workaround</b> Use a US layout keyboard or ensure that you know the key mapping if you are connecting a keyboard of different layout.</p>

**Table 12**      **List of Open Caveats (Sheet 29 of 29)**

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCtg39044	No	<p>Running Internet Explorer in offline mode effects Cisco NAC Agent auto-upgrade function</p> <p>When users access the network via Internet Explorer in offline mode, the Cisco NAC Agent auto-upgrade function does not work correctly for Agent versions 4.6.2.113 and earlier. The login session appropriately prompts the user to upgrade the Agent, but clicking <b>OK</b> brings up the login screen instead of launching the Agent installer.</p>

## Resolved Caveats - Release 4.6(1)


**Note**

For caveats related to Cisco NAC Profiler, refer to the applicable version of the [Release Notes for Cisco NAC Profiler](#).

**Table 13**      **List of Resolved Caveats (Sheet 1 of 3)**

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCso66333	Yes	<p>CAS/CAM time zone incorrect for Venezuela</p> <p>Since the DEC 2007 change to Venezuela time zone from GMT-4:00 to GMT-4:30, Clean Access Manager and Servers continue to display the old time zone for “America/Caracas” with a half hour offset.</p> <p><b>Note</b> There is no known workaround for this issue.</p>
CSCsy89640	Yes	<p>CAM HA does not recover from partition with some linkdetect configs</p> <p>CAM HA subsystem does not properly recover from network partition. After network partition is resolved, both CAM nodes in the HA pair remain active indefinitely.</p> <p>To address this issue, configure linkdetect behavior so that the “ping time” HA configuration value is larger than the “dead time” value. The link detect IP must not be reachable by at least one node during the partition.</p> <p><b>Workaround</b> Reboot both CAMs or perform <b>service perfigo stop/start</b> on both CAMs.</p>

Table 13 List of Resolved Caveats (Sheet 2 of 3)

Software Release 4.6(1)		
DDTS Number	Corrected	Caveat
CSCsz14431	Yes	<p><b>Device Management &gt; Clean Access &gt; Update</b> page needs to be updated for XML</p> <p>If you go to the CAM <b>Device Management &gt; Clean Access &gt; Update</b> web console page and enable <b>Check for Windows NAC Agent updates</b>, <b>Clean Update</b> causes the NACAgentCFG.xml to be defaulted, thus any custom <b>NACAgentCFG.xml</b> file is lost.</p> <p><b>Workaround</b> After clean update, upload the custom XML Agent configuration file again.</p>
CSCsz24839	Yes	<p><b>addlocaluser</b> API function should not allow &lt;,&gt;," characters as username</p> <p>Steps to reproduce:</p> <ol style="list-style-type: none"> <li>1. Try to create a local user with username as &lt; on the CAM. The CAM returns an "Invalid user name: Characters ('&lt;', '&gt;', ',' ) are not allowed" error message.</li> <li>2. Specify a username as &lt; using the <b>addlocaluser</b> API functions. The &lt; username appears in the CAM.</li> </ol> <p>Both the CAM web console and <b>addlocaluser</b> API should exhibit the same behavior.</p>
CSCsz27928	Yes	<p>Read-only administrator able to remove all MAC addresses with <b>removemaclist</b> API function</p> <p>Steps to reproduce:</p> <ol style="list-style-type: none"> <li>1. Create three MAC addresses: 11:11:11:11:11:11 22:22:22:22:22:22 33:33:33:33:33:33</li> <li>2. Create a Read-only administrator called "roa."</li> <li>3. Call the <b>removemaclist</b> API function using roa permissions.</li> </ol> <p>Cisco NAC Appliance removes all three MAC addresses. Read-only administrators should not be able to remove MAC addresses.</p>
CSCsv32010	Yes	<p>Primary CAM should stop trying to sync db upon standby failure</p> <p>The HA-Primary CAM continues to try to sync databases with the HA-Secondary CAM, even after it has detected a failure. This causes authentication outages.</p> <p>This issue has been observed on all versions of Cisco NAC Appliance up to and including release 4.5(1).</p> <p><b>Note</b> There is no known workaround for this issue.</p>

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

DDTS Number	Software Release 4.6(1)	
	Corrected	Caveat
CSCsv94334	Yes	<p>Host based filters not working on NME CAS</p> <p>Host based policies do not work with the NME-NAC module in any deployment.</p> <p><b>Workaround</b> Replace /lib/modules/2.6.11-perfigo/kernel/drivers/net/e1000_bryce/e1000_bryce.ko with the modified version, and reboot.</p>
CSCsx08078	Yes	<p>User traffic passes when user is not in OUL or CDL</p> <p>Part1: User authenticates through a CAS that they are supposed to be on. Then the user authenticate to another CAS with out changing their IP Address. As a result, the OUL will show 2 users with the same IP Address but on different CASs.</p> <p>Part2: After Part 1 is created, clear the entry for the user IP Address that is on the incorrect CAS. The result is that the user is not in OUL or CDL and can still pass traffic through the CAS.</p> <p>This issue is found during Layer 3 Web login.</p> <p><b>Workaround</b> Apply an ACL to prevent users from getting to the other CASes interface from behind the CAS that the users are coming from.</p>
CSCsx95516	Yes	<p>Certified Device List timer does not account for DST</p> <p>The Cisco NAC Appliance CDL timer executes an hour sooner after DST takes effect.</p> <p><b>Workaround</b> Manually reset the CDL timer.</p>
CSCsz17279	Yes	<p>HTML XSS in NAC Appliance</p> <p>HTML injection is possible on Cisco NAC appliance versions 4.1(x) and 4.5(x).</p> <p>Additional information regarding mitigation of cross-site scripting can be found in the following document:</p> <p><a href="http://www.cisco.com/en/US/products/products_applied_mitigation_bulletin09186a008073f7b3.html">http://www.cisco.com/en/US/products/products_applied_mitigation_bulletin09186a008073f7b3.html</a></p> <p><b>Note</b> There is no known workaround for this issue.</p>

## Resolved Caveats - Agent Version 4.6.2.113

Refer to [Enhancements in Release 4.6\(1\)](#), page 10 for additional information.

**Table 14** *List of Resolved Caveats (Sheet 1 of 5)*

DDTS Number	Agent Version 4.6.2.113	
	Corrected	Caveat
CSCse86581	Yes	<p>Agent does not correctly recognize def versions on the following Trend AV products:</p> <ul style="list-style-type: none"> <li>• PC-cillin Internet Security 2005</li> <li>• PC-cillin Internet Security 2006</li> <li>• OfficeScan Client</li> </ul> <p>Tested Clients:</p> <ul style="list-style-type: none"> <li>• PC-cillin Internet Security 2006 (English) on US-English Windows 2000 SP4</li> <li>• OfficeScan Client (English) on US-English Windows 2000 SP4</li> <li>• VirusBaster 2006 Internet Security (Japanese) on Japanese Windows XP SP2</li> <li>• VirusBaster Corporate Edition (Japanese) on Japanese Windows XP SP2</li> </ul>
CSCso05850	Yes	<p>Remove UAC prompt when Clean Access Agent executes Vista users are prompted for permissions to run the Clean Access Agent. This is prompt is standard for Vista machines that have the User Access Control feature enabled.</p> <p><b>Workaround</b> There is no known workaround for this issue.</p>
CSCsu30467	Yes	<p>NIC must be present when using VPN over EVDO</p> <p>The Clean Access Agent does not work if the machine has the wireless and/or wired adapter disabled and the user is using an EVDO-only connection. (Evolution Data Only/Evolution Data Optimized is a 3G wireless broadband standard.) This is because the Agent considers the MAC address for PPP and VPN connections “irrelevant” so the Agent cannot find a unique MAC with which to associate.</p> <p><b>Workaround</b> Enable the wireless or wired adapter.</p>
CSCsu69802	Yes	<p>Agent Messages in Czech and Russian language showing incorrectly</p> <p>Customer is not seeing the correct Czech characters on the Agent Popup windows during the posture assessment and remediation phase. The agent does not has the characters with the “inverse hat” symbol and displays #283, #268, #344, instead.</p> <p><b>Workaround</b> There is no known workaround for this issue.</p>

**Table 14**      **List of Resolved Caveats (Sheet 2 of 5)**

DDTS Number	Agent Version 4.6.2.113	
	Corrected	Caveat
CSCsu92417	Yes	<p>Agent crashes with error “Run-time error ‘6’: Overflow”</p> <p>Clean Access Agent crashes with the message “Run-time error ‘6’: Overflow”. This happens when the CAM has a very large number of checks configured.</p> <p><b>Workaround</b> Reduce the number of checks that the agent has to perform.</p>
CSCsv29066	Yes	<p>Clicking <b>Cancel</b> should stop posture check</p> <p>The Cisco NAC Agent does not seem to be responsive when the <b>Cancel</b> button is clicked during posture assessment. Clicking <b>Cancel</b> during a relatively lengthy posture assessment does not appear to cancel the login attempt.</p> <p><b>Note</b> When the checking processing is complete, the cancel request is processed.</p>
CSCsx26297	Yes	<p>AV/AS remediation takes a long time if ANY used for multiple requirements</p> <p>AV/AS remediation takes a long time if the ANY option is used for multiple client machine requirements.</p> <p><b>Workaround</b> Specify vendor names for requirements when possible.</p>
CSCsx32470	Yes	<p>System tray tooltip is not displayed correctly on Japanese OS</p> <p>When the user hovers the mouse over the Cisco NAC Agent icon in the system tray, the tooltip does not display “Cisco NAC Agent,” nor does it display the proper state.</p> <p><b>Note</b> Before the Agent successfully authenticates with Cisco NAC Appliance, the tooltip should display “login window pop-up,” and after authentication, should display “login.”</p>
CSCsx34697	Yes	<p>Cancel dialog allocates memory and does not release until application exits</p> <p>The Cisco NAC Agent user interface allocates memory and does not release it until the application terminates.</p> <p><b>Note</b> Canceling an operation like remediation generates a Cancel dialog prompt.</p>
CSCsx41086	Yes	<p>Cisco NAC Agent removes OUL when client restarted, but not Clean Access Agent</p> <p>The Cisco NAC Agent erroneously logs the user out of the Cisco NAC Appliance system when the client machine reboots even if the CAM is configured to keep the user in the online users list when the client machine reboots/restarts.</p>

**Table 14**      **List of Resolved Caveats (Sheet 3 of 5)**

DDTS Number	Agent Version 4.6.2.113	
	Corrected	Caveat
CSCsx45087	Yes	<p>TrendMicro 16.x auto-remediation happens but reports as fail</p> <p>TrendMicro AntiVirus 16.x auto-remediation takes place as designed, but reports as having failed.</p> <p><b>Workaround</b> Clicking <b>OK</b> in the failed remediation dialog triggers another auto-remediation which passes.</p>
CSCsx45529	Yes	<p>Flip from Auto to Manual remediation causes confusion</p> <p>When auto-remediation fails, the Cisco NAC Agent flips to manual remediation and prompts user to repair until the temporary role timer expires.</p> <p><b>Workaround</b> When configuring a requirement with the auto-remediation feature, the requirement <b>Description</b> should explain that we are attempting to remediate and if that fails, the user will be asked to remediate manually by hitting the <b>Repair</b> button and initiating remediation, manually.</p> <p><b>Note</b> If the user does not wish to continue from this point, they can click <b>Cancel</b> or opt for restricted network access (if is available) and contact the administrator.</p>
CSCsx45633	Yes	<p>Cisco NAC Agent is “chatty” during auto-remediation</p> <p>During McAfee AV 13.x a auto-remediation via the Cisco NAC Agent, the screen flashes with various AV UIs as it remediates the client machine.</p>
CSCsx47781	Yes	<p>Cisco NAC Agent mandatory service check not running</p> <p>A mandatory check for a service that is not running on the client machine results in a false positive.</p> <p><b>Workaround</b> Use a check to make sure the required program is running on the system.</p>
CSCsy25850	Yes	<p>Selecting about from systray breaks the BFE GUI layout</p> <p>If a user selects <b>About</b> or <b>Properties</b> from the Systray before they are logged in, everything in the dialog moves to top right corner.</p> <p><b>Workaround</b> In order to get the login screen to display properly, exit the Cisco NAC Agent and restart.</p>
CSCsy32777	Yes	<p>Cisco NAC Agent mandatory remediation with one requirement has a “Skip” option</p> <p>There is a <b>Skip</b> button available when there should not be. In certain situations allow user to by pass mandatory requirement (WSUS).</p> <p><b>Workaround</b> Disregard the <b>Skip</b> button.</p>

**Table 14**      **List of Resolved Caveats (Sheet 4 of 5)**

DDTS Number	Agent Version 4.6.2.113	
	Corrected	Caveat
CSCsy81845	Yes	<p>NIC must be present when using VPN over EVDO</p> <p>If there is no NIC (wireless or wired) enabled on the client then EDVO will not authenticate properly to a Cisco NAC Appliance network</p> <p><b>Workaround</b> Enable at least one Network Interface other than the EDVO card on the system.</p>
CSCsz12218	Yes	<p>Cisco NAC Agent login display is not completely localized for German</p> <p>Button text is localized but other text is not.</p>
CSCsz12226	Yes	<p>For German, text and fields jump to left when you click in the Cisco NAC Agent window</p> <p>This issue occurs on the Cisco NAC Agent user log in display, if you click with the mouse outside of the log in boxes the log in fields will shift to the left.</p> <p><b>Note</b> There is no workaround for this purely cosmetic issue.</p>
CSCsz12549	Yes	<p>Some German language systray options and tool tip are in English</p>
CSCsz29185	Yes	<p>Default discovery host in XML file is hard-coded to 192.168.137.3</p> <p>Currently, the default discovery host in the XML file is hard coded to 192.168.137.3. This applies to both fresh installations as well as upgrades to Cisco NAC Appliance Release 4.6(1).</p> <p>The default value for this parameter in XML file should be blank or set to CAM IP address.</p> <p><b>Workaround</b> Upload an empty XML file or a new XML file with the appropriate hostname/IP address of the Discovery Host.</p>
CSCsz32533	Yes	<p>Discovery host (DH) in XML file does not get updated when using the CAM web console</p> <p>This issue occurs when the Discovery Host IP/hostname is changed using the CAM <b>Device Management &gt; Clean Access &gt; Clean Access Agent &gt; Installation</b> web console page.</p> <p><b>Workaround</b> Upload an XML file using CAM web console Installation page with appropriate discovery host populated.</p>
CSCsz37349	Yes	<p>Accessibility, Cancel dialog box is not announced or read by JAWS</p> <p>When using JAWS and the Cancel link is selected on the SCC display, the Cancel dialog box is not announced or read by JAWS. If you try reading the page you get the SCC page not the Cancel dialog box text.</p> <p><b>Note</b> The <b>OK</b> and <b>Cancel</b> buttons on the Cancel dialog box function normally.</p>



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

Agent Version 4.6.2.113		
DDTS Number	Corrected	Caveat
CSCsz41044	Yes	<p>Uploading Agent file without a version should not be allowed</p> <p>Agent version on CAM web console <b>Monitoring &gt; Summary</b> screen is blank. This happens because the Agent can be uploaded using the <b>Device Management &gt; Clean Access &gt; Clean Access Agent &gt; Distribution</b> page without version field populated.</p> <p><b>Workaround</b> Be sure to populate the Agent <b>Version</b> field with the Agent version info when uploading to the CAM (for example, 4.6.2.113).</p>
CSCsz43835	Yes	<p>Roll back Log Packager version</p> <p>Due to build and localization issues, Cisco has decided to stick with an English language-based Log Packager for all languages.</p> <p><b>Note</b> As this is only a diagnostic/troubleshooting tool, customers/help desks will/can assist their user community to select the appropriate buttons.</p>
CSCsz58750	Yes	<p>Change downloaded XML file to default to MERGE</p> <p>If a parameter is defined in the client machines's XML Agent configuration file, then the downloaded parameter values will not overwrite any existing settings unless specifically configured to do so.</p>
CSCsz66290	Yes	<p>NACAgentCFG.xml file is downloaded to agent with only Discovery Host filled in even though a custom XML had been previously uploaded to CAM</p> <p>If a custom NACAgentCFG.xml file had been uploaded to the CAM and a new Agent .tar.gz file was uploaded to CAM with no Agent version string (or an incorrect Agent version string), then even after the Agent .tar.gz file is uploaded correctly with the correct Agent version, the custom NACAgentCFG.xml file cannot be downloaded to the CAS and the Agent.</p> <p><b>Workaround</b> If you receive an error about the version when you upload an Agent .tar. gz file to the CAM, you need to upload a custom NACAgentCFG.xml file again, and then attempt to upload the Agent .tar.gz file again, this time using the correct 4-digit agent string. If you have already correctly uploaded the Agent .tar.gz file, then you still need to upload a custom NACAgentCFG.xml file again.</p> <p><b>Note</b> If you are not using a custom NACAgentCFG.xml file, then your setup will not be affected.</p>

# New Installation of Release 4.6(1)

The following steps summarize how to perform new CD software installation of release 4.6(1) on supported Cisco NAC Appliance hardware platforms (see [Release 4.6\(1\)](#) and [Hardware Platform Support](#), page 3 for additional support details).


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

To upgrade on an existing NAC Appliance, refer to the instructions in [Upgrading to Release 4.6\(1\)](#), page 59.

## For New Installation:

With release 4.6(1), installation occurs in two phases:

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

- 
- Step 1** If you are going to perform a new installation but are running a previous version of Cisco Clean Access, Cisco recommends backing up your current Clean Access Manager installation and saving the snapshot on your local computer, as described in [General Preparation for Upgrade](#), page 63.
- Step 2** Follow the instructions on your welcome letter to obtain product license files for your installation. See [Licensing](#), page 2 for details. (If you are evaluating Cisco Clean Access, visit <http://www.cisco.com/go/license/public> to obtain an evaluation license.)
- Step 3** Install the latest version of 4.6(1) on each Clean Access Server and Clean Access Manager, as follows:
- a. Log in to the [Cisco NAC Appliance Software Download Site](#). You will likely be required to provide your CCO credentials.
  - b. Navigate to the Cisco NAC Appliance 4.6.1 subdirectory, download the latest 4.6(1) .ISO image, (e.g. **nac-4.6\_1-K9.iso**) and burn the image as a bootable disk to a CD-R.
- 

**Note** Cisco recommends burning the .ISO image to a CD-R using speeds 10x or lower. Higher speeds can result in corrupted/unbootable installation CDs.
- 
- c. Insert the CD into the CD-ROM drive of each installation server, and follow the instructions in the auto-run installer.
- Step 4** After software installation, access the Clean Access Manager web admin console by opening a web browser and typing the IP address of the CAM as the URL. The Clean Access Manager License Form will appear the first time you do this to prompt you to install your FlexLM license files.
- Step 5** Install a valid FlexLM product license file for the Clean Access Manager (either evaluation, starter kit, or individual license).
- Step 6** At the admin login prompt, login with the web console username and password you configured when you installed the Clean Access Manager.
- Step 7** In the web console, navigate to **Administration > CCA Manager > Licensing** to install any additional license files for your CASS, CAM HA pairs or CAS HA pairs. You must install the CAS license to add the CASS to the CAM and an OOB CAS license to enable OOB features on the CAM.

**Step 8** For detailed steps on initial configuration, refer to the [Cisco NAC Appliance Hardware Installation Quick Start Guide, Release 4.6\(1\)](#).

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

- [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.6\(1\)](#)
- [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.6\(1\)](#)

**Note**

Clean Access Manager 4.6(1) is bundled with version 4.6.2.113 of the Cisco NAC Appliance Agents.

**Note**

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

## Upgrading to Release 4.6(1)

This section provides instructions for how to upgrade your existing supported Cisco NAC Appliance platform to release 4.6(1). If you need to perform a CD software installation, refer instead to [New Installation of Release 4.6\(1\), page 58](#).

Refer to the following information prior to upgrade:

- [Changes for 4.6\(1\) Installation/Upgrade](#)
- [General Preparation for Upgrade](#)
- [Upgrade Instructions for Standalone Machines](#)
- [Upgrade Instructions for HA Pairs](#)

**Caution**

During the upgrade process, new users will not be able to log in or authenticate with Cisco NAC Appliance until the Clean Access Server reestablishes connectivity with the Clean Access Manager.

**Note**

Cisco NAC Appliance 4.6(1) release includes Cisco NAC Profiler Collector version 2.1.8-37 by default. When upgrading the CAS to a newer Cisco NAC Appliance release, the current version of the Collector is replaced with the default version of the Collector shipped with the Cisco NAC Appliance release. For example, if you are running Release 4.5(x) and Collector 2.1.8-38, and you upgrade to NAC 4.6(1), the Collector version will be downgraded to 2.1.8-37. Refer to the [Release Notes for Cisco NAC Profiler](#) for software compatibility matrixes and additional upgrade and product information.

## Changes for 4.6(1) Installation/Upgrade

Cisco NAC Appliance (Cisco Clean Access) release 4.6(1) ED and later is a major software release with Early Deployment status. Cisco strongly recommends to test new releases on a pilot system prior to upgrading your production system.

If planning to upgrade to Cisco NAC Appliance 4.6(1) ED and later, note the following:

- [Hardware Considerations](#)
- [Features That May Change With Upgrade](#)
- [Upgrade Changes](#)
- [Password Changes](#)

### Hardware Considerations

- **Release 4.5 and later only supports and can only be installed on Cisco NAC Appliance CCA-3140, NAC-3310, NAC-3350, NAC-3390, and NME-NAC-K9 (NAC network module) platforms.** You cannot upgrade to or install release 4.5 and later on any other platform. See [Hardware Support, page 2](#) for additional details.
- With release 4.6(1), there is only one product installation CD (.ISO) for all appliance platforms. The installation package determines whether the Clean Access Server, Clean Access Manager, or Super Clean Access Manager was previously installed, as well as the previous software version.
- If performing CD software installation on a NAC-3310 based appliance which is not reading the software on the CD ROM drive, refer to [Known Issue with NAC-3310 Based Appliances](#).
- If you are planning to upgrade the CCA-3140 appliance, a workaround is needed if upgrading from release 4.1.6 to release 4.6(1). Refer to [Known Issue with Upgrading CCA-3140 Appliance from Release 4.1\(6\), page 77](#) for details.

### Features That May Change With Upgrade

- If you employed any of the previous Windows registry settings (for the parameters noted in [Agent Configuration XML File Upload Enhancement, page 12](#)) to adjust Windows Clean Access Agent behavior on client machines, you must specify the same settings in the XML Agent configuration file to preserve Agent behavior using the Cisco NAC Agent.
- For new installations of Cisco NAC Appliance Release 4.5(1) and later, the CAS Fallback behavior enhancement introduces new default values for the **Detect Interval** and **Detect Timeout** settings (20 and 300 seconds, respectively) and requires that the **Detect Timeout** value be at least 15 times the specified **Detect Interval**. If you are upgrading to release 4.5(1) and later, however, your existing values for these settings are preserved and you must specify new values for these settings to take advantage of the enhanced CAS Fallback capabilities available in release 4.5(1).
- When upgrading a VPN SSO Cisco NAC Appliance network to release 4.6(1), user login does not work properly **when the user VPN is part of a managed subnet on the CAS**. For more information, see [Known Issue for VPN SSO Following Upgrade to Release 4.5 and Later, page 74](#).

## Upgrade Changes



### Warning

If your previous deployment uses a chain of SSL certificates that is incomplete, incorrect, or out of order, CAM/CAS communication may fail after upgrade to release 4.5 and later. You must correct your certificate chain to successfully upgrade. For details on how to fix certificate errors on the CAM/CAS after upgrade to release 4.5 and later, refer to the [How to Fix Certificate Errors on the CAM/CAS After Upgrade Troubleshooting Tech Note](#).



### Note

Web upgrade is no longer supported for upgrade to release 4.5 and later. To upgrade your CAM and CAS from 4.1(x) or 4.0(x) releases, you must copy the **cca\_upgrade-4.6.1-NO-WEB.tar.gz** file to each CAM and CAS appliance and run the upgrade script via the command line. Refer to [Known Issues with Web Upgrade in Release 4.1\(x\) and Earlier, page 74](#) for details.

- Starting from release 4.6(1), the CAM no longer manages Clean Access Agent Patch/Upgrade files (CCAAgentUpgrade-4.x.y.z.tar.gz). If you are downgrading or replacing the current version of the Agent on the CAM, be sure you only upload Clean Access Agent installation files (CCAAgentSetup-4.x.y.z.tar.gz or CCAAgentMacOSX-4.x.y.z-k9.tar.gz) from the Cisco Software Download site.
- If you only upgrade to the latest version of the Cisco NAC Agent, and leave your CAM/CAS at release 4.5(1) or earlier, the Agent operates as an English-only entity—you cannot take advantage of the native operating system localization support available to Cisco NAC Agent users who are logging in to a 4.6(1) CAM/CAS network.
- If you are upgrading from a release 4.5(1) or earlier CAM on which you are using non-English characters in Cisco NAC Appliance (for names or user roles or custom checks/requirements for example), the non-English data may not render properly after upgrade to release 4.6(1). To work around this issue, you can do one of three things:
  - Translate the non-English elements to English prior to upgrade
  - Remove the non-English items from the CAM prior to upgrade and replace them once upgrade is complete
  - Perform a fresh install of release 4.6(1) and re-create all of the non-English elements after installation



### Note

Including non-English data on the CAM/CAS in Cisco NAC Appliance releases prior to 4.6(1) is not officially supported, although certain implementations have been successful in lab environments.

- Users without administrator privileges upgrading their Windows client machine from an earlier version of the Clean Access Agent (version 4.5.1.0 or 4.1.10.0 and earlier) to the Cisco NAC Agent must have the **CCAAgentStub.exe** Agent Stub installed on the client machine to facilitate upgrade. (Users with administrator privileges do not need this file.) After successful Cisco NAC Agent installation, the user is not required to have administrator privileges on the client machine, nor is the **CCAAgentStub.exe** Agent Stub file needed.
- Macintosh client machines require the CAS to have a name-based SSL certificate in order to communicate with Cisco NAC Appliance. Note that if you generate or import a new name-based certificate, you must reboot the CAS using the **service perfigo reboot** or **reboot** command from the CAS CLI.

- When upgrading the CAM to version 4.6(1), Agent files are automatically upgraded to the latest Cisco NAC Agent version packaged with the CAM software image (e.g. 4.6.2.113).
- Starting from Cisco NAC Appliance release 4.1(6), the Clean Access Manager and Clean Access Server require encrypted communication. Therefore, you must upgrade CASs *before* the CAM that manages them to ensure the CASs have the same (upgraded) release when the CAM comes back online and attempts to reconnect to the managed CASs. If you upgrade the Clean Access Manager by itself, the Clean Access Server (which loses connectivity to the CAM during Clean Access Manager restart or reboot) continues to pass authenticated user traffic only if the CAS Fallback Policy specifies that Cisco NAC Appliance should “ignore” traffic from client machines.
- When upgrading CAM/CAS software images prior to release 4.1(6), administrators may notice “4.1.6” upgrade messages during the release 4.6(1) upgrade process. These messages are part of a normal two-step upgrade process and do not have any impact on the release 4.6(1) upgrade.
- Upgrade file names are slightly different if you use the CAM/CAS web console to upload the upgrade file to the CAM/CAS instead of using WinSCP, SSH File Transfer, or PSCP to copy the upgrade file to your machines. The names of files uploaded via web console contain appended numeric codes that you must know in order to extract upgrade files and initiate the upgrade process. For more information, see [Known Issues with Web Upgrade in Release 4.1\(x\) and Earlier, page 74](#).
- Release 4.6(1) includes version 2.1.8-37 of the Cisco NAC Profiler Collector component that resides on the CAS installations. When upgrading CAS appliances (standalone or HA) to release 4.6(1), the upgrade script will check the version of the Collector and only upgrade it if version 2.1.8-37 is not already installed. Refer to the [Release Notes for Cisco NAC Profiler](#) for software compatibility matrixes and additional upgrade and product information.

**Caution**


---

New users will not be able to log in or authenticate with Cisco NAC Appliance until the Clean Access Server reestablishes connectivity with the Clean Access Manager.

---

## Password Changes

- To offer increased security against potential unauthorized access to Cisco NAC Appliance, the CAM and CAS root admin password you specify during initial system configuration (when performing fresh install or release 4.6(1) or reconfiguring the appliance via **service perfigo config**) must now meet strong password standards. However, any existing CAM/CAS root passwords are preserved during upgrade.
- For new installations of Cisco NAC Appliance, there is no longer a default **cisco123** CAM web console password. Administrators must specify a unique password for the CAM web console. However, any existing CAM web console passwords (including the old default **cisco123**) are preserved during upgrade.

For additional details, see also:

- [Hardware Support, page 2](#)
- [Known Issues for Cisco NAC Appliance, page 73](#)

## General Preparation for Upgrade



### Caution

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

- **Homogenous Clean Access Server Software Support**

You must upgrade your Clean Access Manager and all your Clean Access Servers (including NAC Network Modules) concurrently. The Cisco NAC Appliance architecture is not designed for heterogeneous support (i.e., some Clean Access Servers running 4.6(1) software and some running 4.5(x) or 4.1(x) software).

- **Upgrade Downtime Window**

Depending on the number of Clean Access Servers you have, the upgrade process should be scheduled as downtime. For minor release upgrades, our estimates suggest that it takes approximately 10 to 20 minutes for the Clean Access Manager upgrade and 10 minutes for each Clean Access Server upgrade. Use this approximation to estimate your downtime window.

- **Upgrade Clean Access Servers Before Clean Access Manager**

Starting with Cisco NAC Appliance release 4.1(6), the Clean Access Manager and Clean Access Server require encrypted communication. Therefore, you must upgrade CASs *before* the CAM that manages them to ensure the CASs have the same (upgraded) release when the CAM comes back online and attempts to reconnect to the managed CASs.

If you upgrade the Clean Access Manager by itself, the Clean Access Server (which loses connectivity to the CAM during Clean Access Manager restart or reboot) continues to pass authenticated user traffic only if the CAS Fallback Policy specifies that Cisco NAC Appliance should “ignore” traffic from client machines.



### Caution

New users will not be able to log in or authenticate with Cisco NAC Appliance until the Clean Access Server reestablishes connectivity with the Clean Access Manager.

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

When connecting high availability (failover) pairs via serial cable, BIOS redirection to the serial port must be disabled for NAC-3300 series appliances, and for any other server hardware platform that supports the BIOS redirection to serial port functionality. See also [Known Issues with NAC-3300 Series Appliances and Serial HA \(Failover\) Connection](#), page 78.

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

Cisco recommends creating a manual backup snapshot before and after upgrade of your CAM database. The snapshot contains CAM database configuration and CAS configuration for all CASs added to the CAM's domain. Pre- and post-upgrade snapshots allow you to revert to your previous database should you encounter problems during upgrade and preserves your upgraded database as a baseline after upgrade. Make sure to download the snapshots to another machine for safekeeping. After upgrade, delete all earlier snapshots from the CAM web console as they are no longer compatible. See [Copy the Upgrade File to the CAS/CAM](#), page 66.



### Warning

**You cannot restore a CAM database from a snapshot created using a different release. For example, you cannot restore a 4.1(x) or 4.5(x) database snapshot to a 4.6(1) CAM.**

- **Software Downgrade**

Once you have upgraded your software to release 4.6(1), if you wish to revert to your previous version of software, you will need to reinstall the previous version from the CD and recover your configuration based on the backup you performed prior to upgrading to 4.6(1). See [Upgrade Instructions for Standalone Machines, page 64](#) for additional details.

- **Passwords**

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

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

If you are running the Cisco NAC Appliance software (release 4.1(x) or earlier) on a non-appliance platform, you will need to purchase Cisco NAC Appliance hardware before you can upgrade your system to Release 4.6(1). You may additionally need to obtain proper FlexLM product licenses. Once you obtain a Cisco NAC platform, Cisco recommends that you:

- 
- Step 1** Back up your current system and create a backup snapshot for the software version you are running (e.g. 4.1(x) or 4.5(x)).
  - Step 2** Download and install the same software version on your new Cisco NAC appliance platform (e.g. 4.1(x) or 4.5(x)).
  - Step 3** Restore the snapshot to your new Cisco NAC appliance.
  - Step 4** If necessary, upgrade your appliance to 4.0(x) or 4.1(x). Then follow the appropriate upgrade procedure to upgrade your Cisco NAC Appliance to release 4.6(1).
  - Step 5** Create a backup snapshot of your upgraded system.
- 


**Note**

If you need to upgrade from a much older version of Cisco Clean Access, you may need to perform an interim upgrade to a version that is supported for upgrade to 4.6(1). In this case, refer to the applicable [Release Notes](#) for upgrade instructions for the interim release. Cisco recommends to always test new releases on a different system first before upgrading your production system.

---

## Upgrade Instructions for Standalone Machines


**Note**

**Web upgrade is no longer supported for upgrade to release 4.5 and later.** To upgrade your CAM and CAS from 4.5(x), 4.1(x), or 4.0(x) releases, you must copy the `cca_upgrade-4.6.1-NO-WEB.tar.gz` file to each CAM and CAS appliance and run the upgrade script via the command line. Refer to [Known Issues with Web Upgrade in Release 4.1\(x\) and Earlier, page 74](#) for details.

---

This section describes how to upgrade standalone (i.e. non-HA) CAM/CAS machines from release 4.0(x)/4.1(x)/4.5(x) to release 4.6(1).

Review [Changes for 4.6\(1\) Installation/Upgrade, page 60](#) and [General Preparation for Upgrade, page 63](#) before proceeding with these upgrade instructions.



After you have downloaded and copied the upgrade file to the CAM/CAS, you must use the CAM/CAS CLI to extract the upgrade image files and perform the upgrade procedure as described in [Run Upgrade Script on the CAM/CAS, page 66](#).

## Summary of Steps for Standalone Upgrade

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

1. [Create CAM DB Backup Snapshot, page 65](#)
2. [Download the Upgrade File, page 65](#)
3. [Copy the Upgrade File to the CAS/CAM, page 66](#)
4. [Run Upgrade Script on the CAM/CAS, page 66](#)

## Create CAM DB Backup Snapshot

This section describes how to back up your current system.

- 
- Step 1** From the CAM web console, go to the **Administration > Backup** page.
- Step 2** The **Snapshot Tag Name** field automatically populates with a name incorporating the current time and date (e.g. 07\_01\_09-15-47\_snapshot). You can also either accept the default name or type another.
- Step 3** Click **Create Snapshot**. The CAM generates a snapshot file and adds it to the snapshot list at the bottom of the page. The file physically resides on the CAM machine for archiving purposes. The Version field and the filename display the software version of the snapshot for convenience (e.g. **07\_01\_09-15-47\_snapshot\_VER\_4\_6\_1.gz**).
- Step 4** For backup, download the snapshot to another computer by clicking the **Tag Name** or the **Download** button for the snapshot to be downloaded.
- Step 5** In the file download dialog, select the **Save File to Disk** option to save the file to your local computer.
- Step 6** After upgrade, delete all earlier snapshots from the CAM web console as they will no longer be compatible.
- 



### Note

Cisco NAC Appliance creates automatic snapshots before and after software upgrades and failover events, and preserves the last 5. For further details, see “Database Recovery Tool” in the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.6\(1\)](#).

---

## Download the Upgrade File



### Note

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

**Web upgrade is no longer supported for upgrade to release 4.5 and later.** To upgrade your CAM and CAS from 4.5(x), 4.1(x), or 4.0(x) releases, you must copy the **cca\_upgrade-4.6.1-NO-WEB.tar.gz** file to each CAM and CAS appliance and run the upgrade script via the command line. Refer to [Known Issues with Web Upgrade in Release 4.1\(x\) and Earlier, page 74](#) for details.

---

- 
- Step 1** Log in to the [Cisco NAC Appliance Software Download Site](#). You will likely be required to provide your CCO credentials.
- Step 2** Navigate to the Cisco NAC Appliance 4.6.1 subdirectory, download the latest 4.6(1) upgrade file (e.g. **cca\_upgrade-*<version>*.tar.gz**), and save it to the local computer from which you are accessing the CAM web console.
- 

## Copy the Upgrade File to the CAS/CAM

This section describes how to copy the upgrade file to the Clean Access Manager and Clean Access Server(s) respectively using [WinSCP](#), [SSH File Transfer](#), or [PSCP](#) as described below.



### Caution

If upgrading from Release 4.1(6) or earlier, the upgrade file **MUST** be copied to the **/store** directory on the respective CAM or CAS machine before running upgrade from the command line as described in [Run Upgrade Script on the CAM/CAS](#), page 66.

---

### If using WinSCP or SSH File Transfer

- 
- Step 1** Access the CAM via WinSCP or SSH File Transfer.
- Step 2** Copy the **cca\_upgrade-4.6.1-NO-WEB.tar.gz** file from your local machine to the **/store** directory on the Clean Access Manager.
- Step 3** Access each CAS via WinSCP or SSH File Transfer.
- Step 4** Copy the **cca\_upgrade-4.6.1-NO-WEB.tar.gz** file from your local machine to the **/store** directory on *each* Clean Access Server.
- 

### If using PSCP

- 
- Step 1** Open a command prompt on your Windows computer.
- Step 2** Cd to the path where your PSCP resides (e.g. C:\Documents and Settings\desktop).
- Step 3** Enter the following command to copy the file to the **/store** directory on the CAM:
- ```
pscp cca_upgrade-4.6.1-NO-WEB.tar.gz root@<ipaddress_manager>:/store
```
- Step 4** Enter the following command to copy the file to the **/store** directory on the CAS (copy to each CAS):
- ```
pscp cca_upgrade-4.6.1-NO-WEB.tar.gz root@<ipaddress_server>:/store
```
- 

## Run Upgrade Script on the CAM/CAS

This section describes how to untar the upgrade file and run the script to upgrade standalone CAM/CAS machines from release 4.0(x)/4.1(x)/4.5(x) to release 4.6(1). You will need to login with your CAM and CAS **root** user passwords and access the command line of the CAM or CAS machine using one of the following methods:

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

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

**Note**

The 4.6(1) upgrade script only executes if the current system is a supported Cisco NAC Appliance platform. Otherwise, the script exits with message “Unable to upgrade, not a recommended hardware platform for 4.6.x”.

**Upgrade the CAM****Note**

If upgrading a CCA-3140 appliance from 4.1.6 to 4.6(1), refer to [Known Issue with Upgrading CCA-3140 Appliance from Release 4.1\(6\), page 77](#) prior to upgrade.

- Step 1** Connect to the Clean Access Manager to upgrade using a console connection, or [Putty](#) or [SSH](#).
- Step 2** Log in as user `root` with root password.
- Step 3** Change directory to `/store`:
- ```
cd /store
```
- Step 4** Locate the upgrade file. If you used WinSCP, SSH File Transfer, or PSCP, the upgrade filename is `cca_upgrade-4.6.1-NO-WEB.tar.gz`.
- ```
ls -l
```
- Step 5** Extract the contents of the downloaded upgrade file:
- ```
tar xzvf cca_upgrade-4.6.1-NO-WEB.tar.gz
```
- The extraction process automatically places the upgrade files and necessary upgrade script in the `/cca_upgrade-4.6.1` directory.
- Step 6** Change to the `/cca_upgrade-4.6.1` directory and execute the upgrade process:
- ```
cd cca_upgrade-4.6.1
./UPGRADE.sh
```
- Step 7** When prompted to update the Windows Agent, specify `y` or `n` to upgrade the Agent or retain the current Agent version.
- ```
Please choose whether to upgrade Windows Agent to 4.6.2.113 (It's highly recommended to upgrade) (y/n)? [y]
Please choose whether to upgrade Mac Agent to 4.6.0.3 (It's highly recommended to upgrade) (y/n)? [y]
```
- Step 8** Wait for the upgrade to complete. This will take several minutes
- ```
...stopping CCA Manager...

Welcome to the CCA Manager migration utility.

...Upgrading to newer rpms of 4.6.1...done.
...Upgrading CCA files...done
```

```
Windows Agent version upgraded to 4.6.2.113.
Mac Agent was upgraded to version 4.6.0.3.
Clearing Tomcat cache...checking ssl configuration...done.
[root@cam127 cca_upgrade-4.6.1]#
```

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

```
reboot
```



**Tip**

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

## Upgrade the CAS



**Note**

If upgrading a CCA-3140 appliance from 4.1.6 to 4.6(1), refer to [Known Issue with Upgrading CCA-3140 Appliance from Release 4.1\(6\), page 77](#) prior to upgrade.

**Step 1** Connect to the Clean Access Server to upgrade using a console connection, or [Putty](#) or [SSH](#).

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

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

```
cd /store
```

**Step 4** Locate the upgrade file. If you used WinSCP, SSH File Transfer, or PSCP, the upgrade filename is `cca_upgrade-4.6.1-NO-WEB.tar.gz`.

```
ls -l
```

**Step 5** Extract the contents of the downloaded upgrade file:

```
tar xzvf cca_upgrade-4.6.1-NO-WEB.tar.gz
```

The extraction process automatically places the upgrade files and necessary upgrade script in the `/cca_upgrade-4.6.1` directory.

**Step 6** Change to the `/cca_upgrade-4.6.1` directory and execute the upgrade process:

```
cd cca_upgrade-4.6.1
./UPGRADE.sh
```

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

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

Welcome to the CCA Server migration utility.

...Upgrading to newer rpms of 4.6.1...done.
...Upgrading CCA files...done
Clearing Tomcat cache...checking ssl configuration...done.
[root@cas128 cca_upgrade-4.6.1]#
```

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

reboot

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



**Tip**

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

## Upgrade Instructions for HA Pairs

This section describes how to upgrade high-availability (HA) pairs of CAM or CAS servers from release 4.0(x)/4.1(x)/4.5(x) to release 4.6(1).

If you have standalone CAM/CAS servers, refer instead to [Upgrade Instructions for Standalone Machines](#), page 64.

Review [Changes for 4.6\(1\) Installation/Upgrade](#), page 60 and [General Preparation for Upgrade](#), page 63 before proceeding with these upgrade instructions.



**Note**

**Web upgrade is no longer supported for upgrade to release 4.5 and later.** To upgrade your CAM and CAS from 4.5(x), 4.1(x), or 4.0(x) releases, you must copy the `cca_upgrade-4.6.1-NO-WEB.tar.gz` file to each CAM and CAS appliance and run the upgrade script via the command line. Refer to [Known Issues with Web Upgrade in Release 4.1\(x\) and Earlier](#), page 74 for details.



**Warning**

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

**If you are using serial connection for HA, BIOS redirection to the serial port must be disabled for NAC-3300 series appliances, and for any other server hardware platform that supports the BIOS redirection to serial port functionality. See also [Known Issues with NAC-3300 Series Appliances and Serial HA \(Failover\) Connection](#), page 78.**



**Note**

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

## Upgrading HA-CAM and HA-CAS Pairs

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



**Warning**

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

**Note**

If upgrading a CCA-3140 appliance from 4.1.6 to 4.6(1), refer to [Known Issue with Upgrading CCA-3140 Appliance from Release 4.1\(6\), page 77](#) prior to upgrade.

**Step 1** Download and save the upgrade file to your local PC, as described in [Download the Upgrade File, page 65](#).

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

**Note**

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

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

**Step 4** Copy the upgrade image to each CAM/CAS machines' **/store** directory as described in [Copy the Upgrade File to the CAS/CAM, page 66](#).

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

```
cd /store
```

**Step 6** Locate the upgrade file. If you used WinSCP, SSH File Transfer, or PSCP, the upgrade filename is **cca\_upgrade-4.6.1-NO-WEB.tar.gz**.

```
ls -l
```

**Step 7** Extract the contents of the downloaded upgrade file:

```
tar xzvf cca_upgrade-4.6.1-NO-WEB.tar.gz
```

The extraction process automatically places the upgrade files and necessary upgrade script in the **/cca\_upgrade-4.6.1** directory.

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

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

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

**Note**

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

- Access the web console as described in “Accessing Web Consoles in High Availability Pairs” sections of the “Configuring High Availability” chapters in both the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.6\(1\)](#) and the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.6\(1\)](#).
- SSH to the Service IP of the CAM/CAS pair, and type **ifconfig eth0**. The Service IP will always access the active CAM or CAS, with the other pair member acting as standby.

- Step 9** Stop services on the standby appliance by entering the following command via the console/SSH terminal:
- ```
service perfigo stop
```
- Step 10** Wait until the standby appliance has suspended services.
- Step 11** Change directory and run the **fostate.sh** command on the active appliance:
- ```
cd /perfigo/common/bin/
./fostate.sh
```
- Make sure this returns “My node is active, peer node is dead” before continuing.
- Step 12** Upgrade the active appliance as follows:
- Make sure the upgrade package is untarred in the **/store** directory on the active appliance.
  - From the untarred upgrade directory created on the active appliance (for example **cca\_upgrade-4.6.1**), run the upgrade script on the active appliance:
- ```
./UPGRADE.sh
```
- For the CAM, when prompted to update the Windows Agent, specify **y** or **n** to upgrade the Agent or retain the current Agent version.
- ```
Please choose whether to upgrade Windows Agent to 4.6.2.113 (It's highly recommended
to upgrade) (y/n)? [y]
Please choose whether to upgrade Mac Agent to 4.6.0.3 (It's highly recommended to
upgrade) (y/n)? [y]
```
- Step 13** After the upgrade is completed, stop services on the active appliance by entering the following command via the console/SSH terminal:
- ```
service perfigo stop
```
- Wait until the active appliance has suspended services.
- Step 14** Restart services on the standby appliance by entering the following command via the console/SSH terminal:
- ```
service perfigo start
```
- Step 15** Upgrade the standby appliance as follows:
- Make sure the upgrade package is untarred in the **/store** directory on the standby appliance.
  - Change to the untarred upgrade directory created on the standby appliance:
- ```
cd cca_upgrade-4.6.1
```
- Run the upgrade script on the standby appliance:
- ```
./UPGRADE.sh
```
- For the CAM, when prompted to update the Windows Agent, specify **y** or **n** to upgrade the Agent or retain the current Agent version.
- ```
Please choose whether to upgrade Windows Agent to 4.6.2.113 (It's highly recommended
to upgrade) (y/n)? [y]
Please choose whether to upgrade Mac Agent to 4.6.0.3 (It's highly recommended to
upgrade) (y/n)? [y]
```
- Step 16** After the upgrade is completed, stop services on the standby appliance by entering the following command via the console/SSH terminal:
- ```
service perfigo stop
```

**Step 17** Reboot the active appliance by entering the following command via the console/SSH terminal:

**reboot**

Wait until it is running normally and you are able to connect to the web console.

**Step 18** Reboot the standby appliance by entering the following command via the console/SSH terminal:

**reboot**



**Note**

There will be approximately 2-5 minutes of downtime while the appliances reboot.



# Known Issues for Cisco NAC Appliance

This section describes known issues when integrating Cisco NAC Appliance:

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

## Known Issue with Mass DHCP Address Deletion

An issue exists in release 4.5(1) and later where a Clean Access Server configured to be a DHCP server can become unmanageable if the administrator attempts to delete more than 800 DHCP addresses from the appliance using the Clean Access Manager web console. If you have more than 800 DHCP addresses, Cisco recommends deleting addresses in smaller blocks of no more than 800 addresses at a time.

In addition to ensuring you do not delete more than 800 DHCP addresses at a time, there are two methods to work around this potential issue.

### Workaround 1

The DHCP IP delete can be done manually by connecting to the CLI and executing the following commands:

```
service perfigo stop
rm -f /var/state/dhcp/dhcpd.leases
touch /var/state/dhcp/dhcpd.leases
service perfigo start
```

If on an HA system, Cisco strongly recommends taking the CASs offline and performing the commands on both machines simultaneously, taking particular care to issue the **service perfigo start** on the two appliances at roughly the same time.

### Workaround 2

If you experience this problem more than once, Cisco recommends changing the Clean Access Manager timeout value by editing the `/perfigo/control/bin/starttomcat` file and adding “-DRMI\_READ\_TIME\_OUT=<new value>” to the end of the CATALINA\_OPTS options string. (The

current default value is 60 seconds, and Cisco does not recommend increasing the timeout value to any more than 300 seconds.) Please note that increasing the read time out value can likely lower the resiliency of WAN deployments, thus reversing the CAM/CAS connectivity improvements introduced when Cisco addressed caveat CSCsw20607 in the [Release Notes for Cisco NAC Appliance, Version 4.5\(1\)](#).

**Note**

In release 4.6(1), the CAM only allows 60 seconds for a response on remote calls to the CAS. This impacts deleting hundreds of DHCP IPs at once, particularly on slower CAS hardware platforms. Cisco recommends that you do not delete any more than 3 class C address segments at once.

For more information, see [CSCsx35438](#), page 41.

## Known Issue for VPN SSO Following Upgrade to Release 4.5 and Later

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

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

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

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

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

Starting from Release 4.5, web upgrade is no longer supported and cannot be used to upgrade Cisco NAC Appliances on 4.1(x) and 4.0(x) releases to Release 4.5 and later. To upgrade your Cisco NAC Appliances from 4.1(x) or 4.0(x) releases, you must copy the upgrade file to each appliance and run the upgrade script via the command line, as described in [Upgrading to Release 4.6\(1\)](#), page 59.

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

- When attempting to upgrade the CAS by uploading the upgrade file to the CAM's **Device Management > CCA Servers > Manage [CAS\_IP] > Misc > Update** page and clicking the **Apply** button, an HTTP 500 error occurs ("java.lang.OutOfMemoryError") ([CSCsr61106](#), page 32).
- When attempting to upload the upgrade file to the CAS via the CAS **Administration > Software Update** page, an error results ("Error: Failed to upload file Content Length Error (260551527 > 209715200)") and the file is not uploaded ([CSCsu26775](#)).

- Web upgrade of the CAM via the CAM's **Administration > CCA Manager > System Upgrade** may still function but is not supported for upgrade to Release 4.5.

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

Starting from Release 4.5:

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



#### Caution

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

Upgrade files that are uploaded to the CAM and CAS via web console are located in different directories, depending on the software release, as listed in [Table 15](#).

**Table 15** *Web-Upload Directory Locations for CAM/CAS Upgrade Files*

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



#### Note

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

## Known Issues with www.perfigo.com Root CA

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

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

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

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

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

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

## Known Issue with Active HA CAM Web Console Following Failover

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

To manually reproduce this scenario:

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

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

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

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



### Note

This defect only applies to systems that have been upgraded to 4.1.6. Systems upgraded directly from 4.1.3.1 or earlier are not affected by this defect.

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

## CSCsv52402 Workaround

**Step 1** To find out if your 4.1(6) system might be affected, type:

```
% rpm -qa | grep "tg3"
```

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

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

```
% rm /boot/2.6.11-perfigo-sp9
% cd /store/cca_upgrade-4.6.x
% ./UPGRADE.sh
```

## Further Problem Description

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

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

**To resolve this issue:**

**Step 1** Run the following commands:

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

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

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

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

**Step 4** The system should run normally.

---

## Known Issue with NAC-3310 Based Appliances

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

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

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

## Known Issues with Switches

For complete details, see [Switch Support for Cisco NAC Appliance](#).

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

Due to changes in DHCP server operation with Cisco NAC Appliance release 4.0(2) and later, networks with Cisco 2200/4400 Wireless LAN Controllers (also known as Airespace WLCs) which relay requests to the Clean Access Server (operating as a DHCP server) may have issues. Client machines may be unable to obtain DHCP addresses. Refer to the “Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs) and DHCP” section of [Switch Support for Cisco NAC Appliance](#) for detailed instructions.



### Note

For further details on configuring DHCP options, refer to the applicable version of the [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide](#).

---

**Note**

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

## Known Issue for Windows Vista and IP Refresh/Renew

When logged in as a machine admin on Windows Vista and using web login with IP refresh configured, IP address refresh/renew via ActiveX or Java will fail due to the fact that Internet EXplorer does not run as an elevated application and Vista requires elevated privileges to release and renew an IP address.

### Workaround

In order to use the IP refresh feature, you will need to:

1. Log into the Windows Vista client as an administrator.
2. Create a shortcut for IE on your desktop.
3. Launch it by right-clicking the shortcut and running it as administrator. This will allow the application to complete the IP Refresh/Renew. Otherwise, the user will need to do it manually via Command Prompt running as administrator. This is a limitation of the Windows Vista OS.

See also [CSCsm61077](#), page 29.

## Known Issues for Windows Vista and Agent Stub

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

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

### “Interactive Services Dialog Detection” and Uninstall

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

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



## Known Issues with MSI Agent Installer

### MSI File Name

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

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

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

### Minor Version Updates

You cannot upgrade minor version (4th digit) updates of the Clean Access Agent from the MSI package directly. You must uninstall the program from Add/Remove programs first before installing the new version. Refer to [CSCsm20655](#), page 28 for details.

See also [Troubleshooting](#), page 81 for additional Agent- related information.

## Known Issue with Windows 2000 Clean Access Agent/Local DB Authentication

When a user logs in via the Clean Access Agent on a Windows 2000 machine with a username/password linked to the “Local DB” provider and must validate a requirement (in a test environment, for example), the Agent returns a “The application experienced an internal error loading the SSL libraries (12157)” error message. Following the error message, the Agent remains in the login state even though it is not actually logged in and the user must either stop the process or restart the client machine for the Agent login dialog to re-appear. (Requirements are not validated and the CAM does not create an Agent report for the Windows 2000 session, so it can be difficult to determine which requirement fails.)

## Known Issue with Windows XP/2000 and Windows Script 5.6

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

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

Filename: scriipten.exe

URL:

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



**Tip**

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



# Troubleshooting

This section provides troubleshooting information for the following topics:

- [CAM-CAS Shared Secret Mismatch Following New CAS Installation](#)
- [Vista/IE 7 Certificate Revocation List](#)
- [Windows Vista Agent Stub Installer Error](#)
- [Agent Stub Upgrade and Uninstall Error](#)
- [Clean Access Agent AV/AS Rule Troubleshooting](#)
- [Generating Windows Installer Log Files for Agent Stub](#)
- [Debug Logging for Cisco NAC Appliance Agents](#)
- [Creating CAM/CAS Support Logs](#)
- [Recovering Root Password for CAM/CAS](#)
- [Troubleshooting CAM/CAS Certificate Issues](#)
- [Troubleshooting Switch Support Issues](#)
- [Other Troubleshooting Information](#)



**Note**

For additional troubleshooting information, see also [New Installation of Release 4.6\(1\), page 58](#).

## CAM-CAS Shared Secret Mismatch Following New CAS Installation

Following a new installation of a CAS in an existing CAM pair upgraded from a previous Cisco NAC Appliance release, the CAM-CAS communication may become unreliable, resulting in garbled HTTP communication between the CAM and CAS, like incoherent requests in CAS apache logs, for example. This could be a result of mismatched Shared Secrets on the CAM and CAS.

To discover whether or not you have a Shared Secret mismatch in your system:

**Step 1** Log into the CAM CLI and enter the following command:

```
[root@cam1 ~]# cat .secret
PERFIGO_SECRET=clpmUXkvroVyw
```

**Step 2** Log into the CAS CLI and enter the same command:

```
[root@cas1 ~]# cat .secret
PERFIGO_SECRET=clMrPFjECbmF6
```

If the two `PERFIGO_SECRET` values do not match, be sure to reset your Cisco NAC Appliance Shared Secret.

For more information, see [CSCta12544, page 48](#).

## Vista/IE 7 Certificate Revocation List



### Note

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

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

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

To resolve the error, perform the following actions:

- Step 1** (**Preferred**) When using a CA-signed CAS SSL certificate, check the “CRL Distribution Points” field of the certificate (including intermediate or root CA), and add the URL hosts to the allowed Host Policy of the Unauthenticated/Temporary/Quarantine Roles. This will allow the Agent to fetch the CRLs when logging in.
- Step 2** Or, if continuing to use temporary certificates for the CAS (i.e. issued by www.perfigo.com), the user will need to perform ONE of the following actions:
  - a. Import the certificate to the client system's trusted root store.
  - b. Disable the “Check for server certificate revocation (requires restart)” checkbox under IE's Tools > Internet Options > Advanced | Security settings.

## Windows Vista Agent Stub Installer Error

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

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

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

To solve the problem:

- Step 1** Disable the Windows Vista UAC and restart the computer.
- Step 2** In a Command Prompt window, run `C:\windows\system32\CCAAgentStub.exe install`.
- Step 3** Launch the Agent stub installer again and choose **Remove**.
- Step 4** Enable the Windows Vista UAC and restart the computer.

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

## Agent Stub Upgrade and Uninstall Error

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

- Step 1** Run `c:\windows\system32\CCAAgentStub.exe` install from a Command Prompt window.
- Step 2** Launch the Clean Access Agent stub installer again and choose **Remove**.
- Step 3** Manually delete “%systemroot%\system32\ccaagentstub.exe.”



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

## Clean Access Agent AV/AS Rule Troubleshooting

When troubleshooting AV/AS Rules:

- View administrator reports for the Clean Access Agent from **Device Management > Clean Access > Clean Access Agent > Reports**
- Or, to view information from the client, right-click the Agent taskbar icon and select **Properties**.

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

1. Version of CAS, CAM, and Clean Access Agent (see [Determining the Software Version, page 9](#)).
2. Version of client OS (e.g. Windows XP SP2).
3. Version of Cisco Updates ruleset
4. Product name and version of AV/AS software from the Add/Remove Program dialog box.
5. What is failing—AV/AS installation check or AV/AS update checks? What is the error message?
6. What is the current value of the AV/AS def date/version on the failing client machine?
7. What is the corresponding value of the AV/AS def date/version being checked for on the CAM? (See **Device Management > Clean Access > Clean Access Agent > Rules > AV/AS Support Info.**)
8. If necessary, provide Agent debug logs as described in [Debug Logging for Cisco NAC Appliance Agents, page 84](#).
9. If necessary, provide CAM support logs as described in [Creating CAM/CAS Support Logs, page 87](#).

## Generating Windows Installer Log Files for Agent Stub

Users can compile the Windows Installer logs generated by the Install Shield application when the Windows Agent is installed on a client machine using the MSI or EXE installer packages.

## MSI Installer

To compile the logs generated by a Windows Agent MSI installer session as the installation takes place, enter the following at a command prompt:

**ccaagent.msi /log C:\ccainst.log**

This function creates an installer session log file called “ccainst.txt” in the client machine’s C:\ drive when the MSI Installer installs the Agent files on the client.

## EXE Installer

You can use the Windows Installer /v CLI option to pass arguments to the **msiexec** installer within **CCAAgent\_Setup.exe** by entering the following at a command prompt:

**CCAAgent\_Setup.exe /v“/L\*v \”C:\ccainst.log””**

This command saves an installation session log file called “ccainst.log” in the client machine’s C:\ drive when the embedded **msiexec** command installs the Agent files on the client.

For more information, refer to the [Windows Installer CLI reference page](#).

## Debug Logging for Cisco NAC Appliance Agents

This section describes how to view and/or enable debug logging for Cisco NAC Appliance Agents. Refer to the following sections for steps for each Agent type:

- [Cisco NAC Web Agent Logs](#)
- [Generate Windows Agent Debug Log](#)
- [Generate Mac OS X Agent Debug Log](#)

Copy these event logs to include them in a customer support case.

### Cisco NAC Web Agent Logs

The Cisco NAC Web Agent version 4.1.3.9 and later can generate logs when downloaded and executed. By default, the Cisco NAC Web Agent writes the log file upon startup with debugging turned on. The Cisco NAC Web Agent generates the following log files for troubleshooting purposes: **webagent.log** and **webagentsetup.log**. These files should be included in any TAC support case for the Web Agent.

Typically, these files are located in the user’s temp directory, in the form:

**C:\Document and Settings\<user>\Local Settings\Temp\webagent.log**

**C:\Document and Settings\<user>\Local Settings\Temp\webagentsetup.log**

If these files are not visible, check the TEMP environment variable setting. From a command-prompt, type “echo %TEMP%” or “cd %TEMP%”.

When the client uses Microsoft Internet Explorer, the Cisco NAC Web Agent is downloaded to the **C:\Documents and Settings\<user>\Local Settings\Temporary internet files** directory.

## Generate Windows Agent Debug Log


You can enable debug logging on the Clean Access Agent by adding a LogLevel registry value on the client with value “debug.” For Windows Agents (see [Enhancements in Release 4.6\(1\), page 10](#)), the event log is created in the directory %APPDATA%\CiscoCAA, where %APPDATA% is the Windows environment variable.



### Note

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

To view and/or change the Agent LogLevel setting:

- Step 1** Exit the Clean Access Agent on the client by right-clicking the taskbar icon and selecting **Exit**.
  - Step 2** Edit the registry of the client by going to Start > Run and typing **regedit** in the **Open:** field of the Run dialog. The Registry Editor opens.
  - Step 3** In the Registry Editor, navigate to HKEY\_CURRENT\_USER\Software\Cisco\Clean Access Agent\.
- 

**Note** For 3.6.0.0/3.6.0.1 and 3.5.10 and earlier, this is HKEY\_LOCAL\_MACHINE\Software\Cisco\Clean Access Agent\
- Step 4** If “LogLevel” is not already present in the directory, go to Edit > New > String Value and add a String to the Clean Access Agent Key called **LogLevel**.
  - Step 5** Right-click **LogLevel** and select Modify. The **Edit String** dialog appears.
  - Step 6** Type **debug** in the **Value data** field and click **OK** (this sets the value of the LogLevel string to “debug”).
  - Step 7** Restart the Clean Access Agent by double-clicking the desktop shortcut.
  - Step 8** Re-login to the Clean Access Agent.
  - Step 9** When a requirement fails, click the **Cancel** button in the Clean Access Agent.
  - Step 10** Take the resulting “event.log” file from the home directory of the current user (e.g. C:\Documents and Settings\<username>\Application Data\CiscoCAA\event.log) and send it to TAC customer support, for example:
    - a.** Open **Start > Run**.
    - b.** In the **Open:** field, enter %APPDATA%/CiscoCAA. The “event.log” file should already be there to view.
  - Step 11** **When done, make sure to remove** the newly added “LogLevel” string from the client registry by opening the Registry Editor, navigating to HKEY\_CURRENT\_USER\Software\Cisco\Clean Access Agent\, right-clicking **LogLevel**, and selecting **Delete**.



### Note

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

## Generate Mac OS X Agent Debug Log

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

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



### Note

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

To view and/or change the Agent LogLevel:

- Step 1** Open the navigator pane and navigate to *<local drive ID>* > **Applications**.
- Step 2** Highlight and right-click the **CCAAgent.app** icon to bring up the selection menu.
- Step 3** Choose **Show Package Contents** > **Resources**.
- Step 4** Choose **setting.plist**.
- Step 5** If you want to change the current LogLevel setting using Mac **Property Editor** (for Mac OS 10.4 and later) or any standard text editor (for Mac OS X releases earlier than 10.4), find the current LogLevel Key and replace the existing value with one of the following:
  - **Info**—Include only informational messages in the event log
  - **Warn**—Include informational and warning messages in the event log
  - **Error**—Include informational, warning, and error messages in the event log
  - **Debug**—Include all Agent messages (including informational, warning, and error) in the event log



### Note

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



### Note

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

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

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

in the file.

You must be the root user to edit the file.

---

## Creating CAM DB Snapshot

See the instructions in [Copy the Upgrade File to the CAS/CAM, page 66](#) for details.

## Creating CAM/CAS Support Logs

The **Support Logs** web console pages for the CAM and CAS allow administrators to combine a variety of system logs (such as information on open files, open handles, and packages) into one tarball that can be sent to TAC to be included in the support case. Refer to “Support Logs” sections of the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide](#) or [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide](#).

## Recovering Root Password for CAM/CAS

Refer to the “Recovering Root Password” section of the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide](#) or [Password Recovery Procedure for the Cisco NAC Appliance \(Cisco Clean Access\)](#).

## Troubleshooting CAM/CAS Certificate Issues

Refer to the “Troubleshooting Certificate Issues” sections of the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide](#) or [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide](#).

## Troubleshooting Switch Support Issues

To troubleshoot switch issues, see [Switch Support for Cisco NAC Appliance](#).

## Other Troubleshooting Information

For general troubleshooting tips, see the following Technical Support webpage:  
[http://www.cisco.com/en/US/products/ps6128/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html)

# Documentation Updates

**Table 16**      **Updates to Release Notes for Cisco NAC Appliance, Release 4.6(1)**

Date	Description
6/17/10	Added Caveats CSCtg39044 and CSCsx52263 to <a href="#">Open Caveats - Release 4.6(1), page 22</a>
7/1/09	Release 4.6(1)

## Related Documentation

For the latest updates to Cisco NAC Appliance documentation on Cisco.com see:

[http://www.cisco.com/en/US/products/ps6128/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6128/tsd_products_support_series_home.html)

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

- [Cisco NAC Appliance - Clean Access Manger Installation and Configuration Guide, Release 4.6\(1\)](#)
- [Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.6\(1\)](#)
- [Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later](#)
- [Getting Started with Cisco NAC Network Modules in Cisco Access Routers](#)
- [Connecting Cisco Network Admission Control Network Modules](#)
- [Switch Support for Cisco NAC Appliance](#)
- [Cisco NAC Appliance Service Contract / Licensing Support](#)

## Obtaining Documentation and Submitting a Service Request

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

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

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

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

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.

© 2009 Cisco Systems, Inc. All rights reserved.