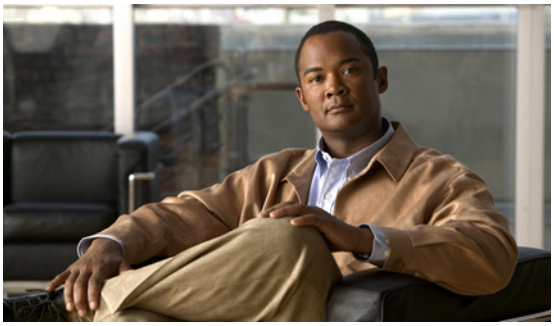

Release Notes for Cisco NAC Appliance, Version 4.7(1)

Document Number OL-22767-01 Revised: September 28, 2011

Contents

These release notes provide the latest cumulative release information for Cisco® NAC Appliance, Release 4.7(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.

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

Cisco NAC Appliance Releases

Cisco NAC Appliance Version	Availability
4.7(1) ED	November 24, 2009
4.7(0) ED	September 29, 2009

Note Cisco recommends you deploy Cisco NAC Appliance Release 4.7(1) in test network before deploying in a production network.

System and Hardware Requirements

This section describes the following:

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. 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 4.7(1) and Hardware Platform Support

FIPS Compliant

You can install or upgrade to Cisco NAC Appliance Release 4.7(1) on the following FIPS-compliant Cisco NAC Appliance platforms:

- NAC-3315, NAC-3355, and NAC-3395

Note Release 4.7(0) is the only certified FIPS-compliant Cisco NAC Appliance release. Although your particular FIPS-compliant deployment may operate normally using Cisco NAC Appliance Release 4.7(1), Cisco does not officially state FIPS-compliance support for Release 4.7(1). For more information, see the *Release Notes for Cisco NAC Appliance, Version 4.7(0)*.

Non-FIPS

You can install or upgrade to Cisco NAC Appliance Release 4.7(1) on the following Cisco NAC Appliance platforms:

- NAC-3315, NAC-3355, and NAC-3395
- NAC-3310, NAC-3350, NAC-3390, CCA-3140 (EOL)

Note Next generation Cisco NAC Appliance platforms (FIPS or non-FIPS Cisco NAC-3315, NAC-3355, NAC-3395) support fresh installation of Release 4.7(1) or upgrade from Release 4.7(0) to Release 4.7(1) only.

Note Cisco NAC Appliance Release 4.7(1) does not support the Cisco NAC Network Module (NME-NAC-K9).

- If the FIPS card in a CAM/CAS ceases to work correctly, make sure the card operation switch is set to "O" (for operational mode), as described in FIPS and SSH, page 8. If the card is still not operational, you will need to RMA the appliance with Cisco Systems and replace it with a new Cisco NAC-3315/3355/3395 platform. Refer to the "Cisco NAC Appliance RMA and Licensing" section of *Cisco NAC Appliance Service Contract/Licensing Support* for details.

Additionally, Cisco NAC Appliance Release 4.7(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 all supported appliance platforms. The installation package detects whether a CAS, CAM or SuperCAM was previously installed along with the software version.

- To upgrade your CAM and CAS from Release 4.5(x), 4.6(1), or 4.7(0), insert the same Cisco NAC Appliance Release 4.7(1) installation CD-ROM (.ISO) into an existing Cisco NAC Appliance CAM or CAS and perform a "clean" or "graceful" shutdown and reboot for the system. The upgrade option from the CD-ROM automatically prompts you to choose whether you want to do a fresh Install or Upgrade to Release 4.7(1). For more information, see Upgrading to Release 4.7(1), page 66 and Known Issues with Web Upgrade in Release 4.1(3), 4.1(6), and 4.1(8), page 82.
- The installation/upgrade CD does not execute if attempting to launch it on a non-supported platform. Refer to Changes for 4.7(1) Installation/Upgrade, page 69 for additional details.
- Legacy customers on non-appliance platforms who wish to upgrade to Release 4.7(1) will need to purchase a supported platform to install the Release 4.7(1) software. Refer to Upgrading from Customer-Supplied Hardware to Release 4.7(1) on a NAC-3310/3350/3390 Platform, page 67 for additional details.

Note You must run the same software version on all CAM/CAS appliances in your network.

Release 4.7(1) and Cisco NAC Profiler

Release 4.7(1) includes version 2.1.8-39 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 4.7(1), the upgrade script will check the version of the Collector and only upgrade it if version 2.1.8-39 is not already installed.

Refer to the *Release Notes for Cisco NAC Profiler* for software compatibility matrixes and additional upgrade and product information.

Note If currently running a Cisco NAC Profiler Server version other than 2.1.8-39, you will need to sync the Collector component version running on the NAC Server to the same version as the Profiler Server for compatibility.

Note Cisco NAC Profiler and Cisco NAC Guest Server are not supported in FIPS-compliant deployments in Release 4.7(0).

FIPS 140-2 Compliance

Note Release 4.7(0) is the only certified FIPS-compliant Cisco NAC Appliance release. Although your particular FIPS-compliant deployment may operate normally using Cisco NAC Appliance Release 4.7(1), Cisco does not officially state FIPS-compliance support for Release 4.7(1). For more information, see the *Release Notes for Cisco NAC Appliance, Version 4.7(0)*.

This section describes the following topics:

Overview

Cisco NAC Appliance Release 4.7(0) introduces Federal Information Processing Standard (FIPS) 140-2 Common Criteria EAL2 compliance for new installations on new Cisco NAC-3315, NAC-3355, and NAC-3395 hardware appliance platforms. In order to provide FIPS compliance in your Cisco NAC Appliance network, both CAM(s) and CAS(s) must use the new hardware platforms and be FIPS compliant. That is, Cisco does not support deployments where a non-FIPS CAM connects to one or more FIPS CASs, or vice-versa.

To enable FIPS 140-2 compliance in Cisco NAC Appliance, the new NAC-3315, NAC-3355, and NAC-3395 feature an encryption card that handles the primary FIPS "level 2" compliance functions and manages private keys for the system.

In addition, in order to ensure FIPS compliance across the entire Cisco NAC Appliance network, users must use the latest Cisco NAC Agent version 4.7.1.15 on client machines connecting to the Cisco NAC Appliance network. Although Cisco NAC Appliance Release 4.7(0) supports older Cisco NAC Appliance Agents, users logging in with an older version of the Agent are not FIPS compliant. For more information on the latest Cisco NAC Agent, see the *Release Notes for Cisco NAC Appliance, Version 4.7(0)*.

In Release 4.7(0), if the FIPS card in the CAM/CAS ceases to work correctly, make sure the card operation switch is set to "O" (for operational mode), as described in FIPS and SSH, page 8. If the card is still not operational, you will need to RMA the appliance with Cisco Systems and replace it with a new Cisco NAC-3315/3355/3395 platform. Refer to the "Cisco NAC Appliance RMA and Licensing" section of *Cisco NAC Appliance Service Contract/Licensing Support* for details. When you configure the replacement appliance, you must also ensure you configure it with the same master password and have imported any required third-party certificates before connecting the appliance to the network. For more information, see Release 4.7(1) and Hardware Platform Support, page 3.

Note Once the FIPS card is Operational on the CAM/CAS, the position of the electromagnetic switch ("O," "M," or "I") on the FIPS card does not impact the performance of the card again until you reboot either the FIPS card or the appliance.

Note Cisco NAC Appliance network administrators managing the CAM/CAS via web console *and* client machine browsers accessing a FIPS-compliant Cisco NAC Appliance Release 4.7(0) network require TLSv1 in order to "talk" to the network, which is disabled by default in Microsoft Internet Explorer Version 6. This option is enabled by default in Microsoft Internet Explorer versions 7 and 8 and Mozilla Firefox has not shown this limitation. For details, see Enabling TLSv1 on Internet Explorer Version 6, page 85.

Note Cisco NAC Profiler and Cisco NAC Guest Server are not supported in FIPS-compliant deployments in Release 4.7(0).

Capabilities, Dependencies, and Restrictions

FIPS 140-2 compliance in Release 4.7(0) introduces the following capabilities, dependencies, and restrictions:

1. Key management is different than in non-FIPS Release 4.7(0). Both CAM and CAS store their private keys in the FIPS card. This private key is used for all Cisco NAC Appliance PKI-based security solutions (i.e. SSL, SSH, and IPSec). In addition, both the CAM and CAS store a master secret in the card. The master secret is used to secure important data, (like other system passwords) stored in the database or on file systems. For more information, see Trusted Certificates and Private Key Management with FIPS, page 7.
2. JSSE (the equivalent of OpenSSL in Java) is used:
   a. On the CAM and CAS during JMX publishing
   b. On the CAS to send HTTP requests to the CAM when users are logging in
   c. On the CAM when using LDAP over SSL for authentication/lookup providers

Note JSSE uses the FIPS card for SSL handshakes and data security.

3. APACHE/MOD_SSL handles HTTP/HTTPS requests from:
   a. User client machines to the CAS
   b. Administrators when using both the CAM and CAS web consoles
   c. The CAS to the CAM when users are logging in

Note MOD_SSL uses the FIPS card during SSL handshakes only. That is, data security is performed outside of the card.

4. IPSec secures:
   a. CAM and CAS HA configurations
   b. RADIUS authentication calls
   c. VPN establishment and maintenance tasks

Note IPSec uses the FIPS card for handshakes only. That is, data security is performed outside of the card.

For more information, see IPSec Considerations with FIPS, page 8.

5. SSH—Just like APACHE and IPSec, SSH uses the FIPS card during SSL handshakes only. For more information, see FIPS and SSH, page 8.

Note When a FIPS card goes down, existing SSH web sessions still work; however, you cannot initiate any new sessions. You are also unable to initiate new SSH sessions if the FIPS card goes into error mode and/or has been erroneously left in Initialization state. In this case, the CAM/CAS console port is the only access method.

6. JGSS—JGSS is used for Kerberos and ADSSO. JGSS uses the FIPS card for securing data.
7. SNMP V3—SNMP V3 uses the FIPS card for securing data. For more information, see FIPS and SNMP Configuration, page 9.
8. SWISS—SWISS uses the FIPS card for securing data. For more information, see FIPS and the Cisco NAC Appliance SWISS Protocol, page 8.
9. Cisco WLCs support RADIUS accounting over IPSec using pre-shared-keys (which are not FIPS compliant) for IKE authentication, and do not support Certificate-based IKE authentication (which *is* FIPS compliant).
10. When AD SSO is configured in the network, Windows XP client machines are not FIPS 140-2 compliant due to XP limitations. You cannot use AES for XP Kerberos, and 3DES encryption is not supported on Windows XP client machines.

Note Windows 2008 Server and the Windows Vista operating system are required to support AD SS0 in a FIPS-compliant Cisco NAC Appliance deployment.

11. LDAP—You must use Windows 2008 when performing LDAP lookups using GSSAPI in a FIPS 140-2 compliant deployment.

FIPS Compliance in HA Deployments

To support FIPS 140-2 compliance, HA CAMs/CASs automatically establish an IPSec tunnel to ensure all communications between the HA pair appliances remains secure across the network.

Trusted Certificates and Private Key Management with FIPS

Starting from Cisco NAC Appliance Release 4.7(0), you can no longer export private keys and you cannot generate CSRs using a FIPS compliant CAM/CAS. To adhere to strict FIPS compliance guidelines, you can only import certificates from trusted third-party resources.

Cisco NAC Appliance uses two types of keys to support FIPS compliance: Private Keys and Shared Master Keys. Both of these key types are managed and stored using the FIPS card installed in the CAM/CAS. During installation, keys are created using the CAM/CAS setup utilities, the keys are then *moved* to the card for security, and key-generation files and/or directories are then removed from the CAM/CAS.

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

- **Administration > Clean Access Manager > SSL > x509 Certificate**
- **Administration > Clean Access Manager > SSL > Trusted Certificate Authorities**
- **Administration > Clean Access Manager > SSL > x509 Certification Request**

FIPS and SSH

SSH connections between FIPS and non-FIPS CAMs/CASs are supported starting from Cisco NAC Appliance Release 4.7(0). However, if the FIPS card in a CAM/CAS fails (or is inadvertently set to the incorrect operational mode), you cannot use SSH to or from that appliance until the issue with the card is resolved.

You can verify FIPS functionality on a CAM/CAS as follows:

a. Ensure the FIPS card operation switch is set to "O" (for operational mode).

b. Log into the CAM console interface as **`root`**.

c. Navigate to the **/perfigo/common/bin/** directory.

d. Enter **`./test_fips.sh info`**. and verify the following output:

```
Installed FIPS card is nCipher
Info-FIPS file exists
Info-card is in operational mode
Info-httpd worker is in FIPS mode
Info-sshd up
```

Note You can also verify whether or not the FIPS card is properly installed and enabled in the Clean Access Manager by looking at the CAM **Monitoring > Summary** web console page. When FIPS is operational, the following status is displayed:

Installed card in the system: nCipher
System is running in FIPS mode

FIPS and the Cisco NAC Appliance SWISS Protocol

To enhance network security and adhere to FIPS 140-2 compliance, Cisco NAC Appliance encapsulates SWISS communications between client machines and CASs, including Discovery Packet transmission/acknowledgement, authentication, and posture assessment results using the HTTPS protocol.

In addition, the CAS SWISS mechanism has been enhanced to feature a new handler that uses 3DES encryption for SWISS protocol functions. Because of these changes, older versions of Cisco NAC Appliance Agents are not compatible with FIPS-compliant CAMs/CASs in Release 4.7(0).

IPSec Considerations with FIPS

Cisco NAC Appliance Release 4.7(0) uses IPSec for the following purposes:

- CAM and CAS HA pairs (both FIPS and non-FIPS modes)
- CAS file synchronization between HA-Primary and HA-Secondary nodes
- CAM and CAS RADIUS server authentication calls in FIPS mode
- ASA-CAS in FIPS mode

When setting up your Cisco NAC Appliance to use IPSec, you must ensure you can set up and import certificates and configure IPSec tunnels between Cisco NAC Appliance and your external authentication resources.

For Active Directory, LDAP, and Kerberos functions with FIPS-compliant CAMs/CASs, you must ensure that hosts are running Windows 2008 Server to support secure authentication sessions between external resources and FIPS-compliant appliances.

FIPS and SNMP Configuration

Cisco NAC Appliance Release 4.7(0) provides support for SHA-1 and 3DES encryption when configuring SNMP management on a FIPS-compliant CAM.

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

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

FIPS and Cisco Secure ACS as RADIUS Authentication Provider

You can configure a FIPS 140-2 compliant external RADIUS Authentication Provider type by setting up a secure IPSec tunnel between your Cisco NAC Appliance system and Cisco ACS 4.x in a Windows environment running Windows Server 2003 or 2008.

For specific configuration instructions, see "Add a FIPS 140-2 Compliant RADIUS Auth Provider Using an ACS Server" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(2)*.

FIPS with VPN SSO

You can configure Cisco NAC Appliance to connect to and manage a Cisco ASA VPN Concentrator in a FIPS 140-2 compliant deployment.

For specific configuration instructions, see the "Configure VPN SSO in a FIPS 140-2 Compliant Deployment" section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(2)*.

FIPS with AD SSO

To maintain FIPS 140-2 compliance and support AD SSO, you *must* use 32-bit Windows Server 2008 with KTPass version 6.0.6001.18000, and client machines must run Windows Vista with Cisco NAC Agent version 4.7.1.15 installed. For specific configuration instructions, see the "Configure Active Directory for FIPS 140-2 Compliant AD SSO" section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(2)*.

Note You cannot perform AD SSO in a FIPS-compliant network using Cisco Wireless LAN Controllers because the WLCs do not support using IPSec to secure session initiation and tear-down, which is *required* in the Cisco NAC Appliance FIPS 140-2 network configuration.

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 4.7(1).

Table 1 Recommended WLC Platforms to Support Wireless OOB in Release 4.7(1)

Cisco Wireless LAN Controller Model	Cisco Wireless LAN Controller Version	Cisco NAC Appliance Version
Cisco 4400 Series Wireless LAN Controllers	5.1 5.2 6.0	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 can update the object IDs (OIDs) of supported WLC platforms by performing a CAM update (under **Device Management > Clean Access > Updates**).

Cisco WLCs do not support IPSec communication with the Cisco NAC Appliance network, so you cannot provide RADIUS SSO capability to users in your FIPS 140-2 compliant environment.

Table 2 lists the IOS versions and switch platforms that are tested and known to work with the Wireless OOB feature in Release 4.7(1). If you encounter issues with WOOB support and are not 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 4.7(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)[1]	N/A
	Cisco ASA 5500 Series Adaptive Security Appliances, Version 8.0(3)7 or later[2]	AnyConnect
	Cisco ASA 5500 Series Adaptive Security Appliances, Version 8.0(3)7 or later	• Cisco SSL VPN Client (Full Tunnel) • Cisco VPN Client (IPSec)
	Cisco WebVPN Service Modules for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers	
	Cisco VPN 3000 Series Concentrators, Release 4.7	
	Cisco PIX Firewall	

1. For additional details, see also Known Issues with Cisco 2200/4400 Wireless LAN Controllers (Airespace WLCs), page 83.
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.

Cisco WLCs do not support IPSec communication with the Cisco NAC Appliance network, so you cannot provide RADIUS SSO capability to users in your FIPS 140-2 compliant environment.

For further details, see the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(2)* and the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(2)*.

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 4.7(1) CAM/CAS Upgrade Compatibility Matrix
- Release 4.7(1) CAM/CAS/Agent Compatibility Matrix
- Release 4.7(1) Agent Upgrade Compatibility Matrix

Release 4.7(1) CAM/CAS Upgrade Compatibility Matrix

Table 4 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 4 Release 4.7(1) CAM/CAS Upgrade Compatibility Matrix

Clean Access Manager [1]		**Clean Access Server** [1, 2]	
Upgrade From:	**To:**	**Upgrade From:**	**To:**
4.7(0) 4.6(1) 4.5(x) [3]	4.7(1)	4.7(0) 4.6(1) 4.5(x)	4.7(1)

1. Next generation Cisco NAC Appliance platforms (FIPS or non-FIPS Cisco NAC-3315, NAC-3355, NAC-3395) support fresh installation of Release 4.7(1) or upgrade from Release 4.7(0) to Release 4.7(1) only. You can also install or upgrade to Release 4.7(1) on the NAC-3310, NAC-3350, NAC-3390, and CCA-3140 (EOL) platforms, but they operate in non-FIPS mode only. See Hardware Support, page 3 and Changes for 4.7(1) Installation/Upgrade, page 69 for additional details.
2. The Clean Access Server is shipped with a default version of the Cisco NAC Profiler Collector. See Release 4.7(1) and Cisco NAC Profiler, page 4 for details.
3. To upgrade from Cisco NAC Appliance Release 4.1(8) or earlier to Release 4.7(1), you must first upgrade your system to Release 4.5(x), 4.6(1), or 4.7(0) and then upgrade to Release 4.7(1).

Release 4.7(1) CAM/CAS/Agent Compatibility Matrix

Table 5 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 5.

For complete support information, including specific client machine operating systems supported with specific Agent versions, refer to the *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*.

Table 5 Release 4.7(1) CAM/CAS/Agent Compatibility Matrix

Clean Access Manager [1, 2]	Clean Access Server [1, 2]	Cisco NAC Appliance Agents [3]		
		Windows	Mac OS X	Web Agent
Non-FIPS				
Localized Server [4]		**Localized Agent [5]**		
4.7(1) 4.7(0)	4.7(1) 4.7(0)	4.7.1.511 [6] 4.7.1.15 4.6.2.113 (All languages)	N/A	N/A
English-Only Server		**English-Only Agent**		
4.7(1) [7]	4.7(1)	4.7.1.511 [6] 4.7.1.15	4.7.1.506 4.7.0.2	4.7.1.504 [8]
		4.6.2.113	4.6.0.3	
		4.5.2.0 [9] 4.5.1.0 4.5.0.0	4.5.0.0 [9]	
		4.1.8.0 [9] 4.1.6.0 4.1.3.2	4.1.3.0 [9]	
English-Only Server		**English-Only Agent**		
4.1(3) and later	4.1(3) and later	4.7.1.511 [6] 4.7.1.15 [10,11]	4.7.1.506 4.7.0.2 [10]	N/A
		4.6.2.113 [10]	4.6.0.3 [10]	

1. Next generation Cisco NAC Appliance platforms (FIPS or non-FIPS Cisco NAC-3315, NAC-3355, NAC-3395) support fresh installation of Release 4.7(1) or upgrade from Release 4.7(0) to Release 4.7(1) only. You can also install or upgrade to Release 4.7(1) on the NAC-3310, NAC-3350, NAC-3390, and CCA-3140 (EOL) platforms, but they operate in non-FIPS mode only. See Hardware Support, page 3 and Changes for 4.7(1) Installation/Upgrade, page 69 for additional details.
2. Make sure that both CAM and CAS are of same version.
3. See Enhancements in Release 4.7(1), page 17 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 4.7(1). See *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later* 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 4.7(1) CAM/CAS network.

6. Cisco NAC Agent version 4.7.1.511 does not support Windows 7 Starter Edition. Client machines with the Windows 7 Starter Edition operating system can only perform web login to verify user credentials. For specific information on enabling web login for client machines running Windows 7 Starter Edition, see Known Issue with Enabling Web Login for Windows 7 Starter Edition Clients, page 81.
7. When upgrading the CAM from version 4.5(x) and later to Release 4.7(1), Agent files are automatically upgraded to the latest Agent version packaged with the CAM software image (e.g. Windows version 4.7.1.511 and Mac OS X version 4.7.1.506).
8. Cisco NAC Web Agent version 4.7.1.504 does not support Windows 7 Starter Edition. Client machines with the Windows 7 Starter Edition operating system can only perform web login to verify user credentials. For specific information on enabling web login for client machines running Windows 7 Starter Edition, see Known Issue with Enabling Web Login for Windows 7 Starter Edition Clients, page 81.
9. CAM/CAS Release 4.7(1) supports 4.1.3.2 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 Agent 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.
10. 4.6.x.x and 4.7.1.x Windows Agents and 4.6.x.x and 4.7.x.y Mac OS X 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 Agent 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.
11. 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 4.7(1) CAM/CAS network.

Release 4.7(1) Agent Upgrade Compatibility Matrix

Table 6 shows Cisco NAC Appliance 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**.

For complete support information, including specific client machine operating systems supported with specific Agent versions, refer to the *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*.

Table 6 Release 4.7(1) Agent Upgrade Compatibility Matrix

Clean Access Manager [1]	Clean Access Server [1]	Cisco NAC Appliance Agent [2]			
		Upgrade From Cisco NAC Appliance Agent:	To Latest Compatible Cisco NAC Windows Agent:	Upgrade From Cisco Mac OS X Agent	To Latest Compatible Mac OS X Agent
4.7(1)	4.7(1)	4.7.1.15 [3] 4.6.2.113 4.5.x.x [4] 4.1.3.2 [5, 6, 7]	4.7.1.511 [8, 9]	4.7.0.2 4.6.0.3 4.5.x.x 4.1.3.0	4.7.1.506

1. Next generation Cisco NAC Appliance platforms (FIPS or non-FIPS Cisco NAC-3315, NAC-3355, NAC-3395) support fresh installation of Release 4.7(1) or upgrade from Release 4.7(0) to Release 4.7(1) only. You can also install or upgrade to Release 4.7(1) on the NAC-3310, NAC-3350, NAC-3390, and CCA-3140 (EOL) platforms, but they operate in non-FIPS mode only. See Hardware Support, page 3 and Changes for 4.7(1) Installation/Upgrade, page 69 for additional details.
2. See Enhancements in Release 4.7(1), page 17 for details on each version of the Windows/Mac OS X/Web Agent.
3. To remain FIPS-compliant, users logging into Cisco NAC Appliance via AD SSO must run Windows Vista and have Cisco NAC Agent version 4.7.1.15 installed on their client machine. Windows XP clients cannot perform AD SSO in a FIPS 140-2 compliant network. See FIPS with AD SSO, page 9 for details.
4. Users without administrator privileges upgrading their Windows client machine from an earlier version of the Clean Access Agent (version 4.5.2.0 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. For more information on Agent Stub installers and requirements/prerequisites, see the appropriate Release Notes for the specific previous version of Cisco NAC Appliance.
5. Auto-upgrade to the latest 4.7.x.x Agent is supported from any 4.1.3.2 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.
6. When upgrading the CAM from version 4.5(x) and later, Agent files are automatically upgraded to the latest Agent version packaged with the CAM software image (e.g. Windows version 4.7.1.511 and Mac OS X version 4.7.1.506).
7. CAM/CAS Release 4.7(1) supports 4.1.3.2 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 Agent 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.
8. Cisco NAC Agent version 4.7.1.511 is the only Cisco NAC Appliance Agent that supports Windows 7 operating systems.
9. 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 and type `cat /perfigo/build`
- CAS web console (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**
- 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 4.7(1)

AD SSO Requirements for Windows 7

In current releases of Windows 7 Enterprise, Ultimate, and Professional, Microsoft has changed what encryption protocols are enabled by default for Active Directory domain authentication. In order to authenticate users via AD SSO, all Windows domain client machines must negotiate a common encryption protocol between themselves and the specific Windows AD server performing authentication.

In previous releases of Cisco NAC Appliance, the AD SSO subsystem required that the Microsoft client machine, CAS, and the authenticating Windows AD Server all use a single common (static) protocol. To ensure that AD SSO could support all customer Active Directory Networks, Cisco NAC Appliance and the AD SSO service account were required to be set to “DES_ONLY” (via KTPass) since all prior Microsoft client machines, as well as the Cisco NAC Appliance system, supported DES encryption.

With Cisco NAC Appliance Release 4.7(1), the CAS has the ability to negotiate any of the standard Kerberos encryption protocols (except for AES 256, due to export restrictions). This new option allows for much improved functionally for customers that wish to migrate between encryption standards without interruption.

For specific configuration details, see the “Configure AD SSO in a Windows 7 Environment” section of the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(2)*.

Cisco NAC Windows Agent Version 4.7.1.511

In Cisco NAC Appliance Release 4.7(1), the Cisco NAC Agent version 4.7.1.511 has been enhanced to feature support for the Windows 7 client machine operating systems:

- Windows 7 Professional (32- and 64-bit)
- Windows 7 Ultimate (32- and 64-bit)
- Windows 7 Enterprise (32- and 64-bit)
- Windows 7 Home Premium (32- and 64-bit)
- Windows 7 Home Basic

Note

- Cisco NAC Agent version 4.7.1.511 does not support Windows 7 Starter Edition. Client machines with the Windows 7 Starter Edition operating system can only perform web login to verify user credentials. For specific information on enabling web login for client machines running Windows 7 Starter Edition, see Known Issue with Enabling Web Login for Windows 7 Starter Edition Clients, page 81.
- To avoid ActiveX initiation issues that could affect Agent download and web login functions, ensure users logging in via Windows 7 client machines maintain "elevated privileges" on the system by keeping the User Access Control (UAC) settings at the "default" level.
- Only the 32-bit version of Microsoft Internet Explorer 8 is supported in Release 4.7(1).
- Accessibility functions with version 10 the JAWS screen reader are not supported on Windows 7 operating systems.

Refer to Release 4.7(1) CAM/CAS/Agent Compatibility Matrix, page 13 for additional compatibility details.

For details on Agent functionality, refer to the "Cisco NAC Appliance Agents" chapter of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(2)*.

Mac OS X Agent Version 4.7.1.506

In Cisco NAC Appliance Release 4.7(1), the Mac OS X Agent version 4.7.1.506 has been enhanced to feature login and posture assessment support for 32- and 64-bit Mac OS 10.6 (Snow Leopard) client machines.

Note The Cisco Mac OS X VPN Client version 4.9.01.0180 and AnyConnect version 2.3.2016 do not work when the client machine is running Mac OS X 10.6 in 64-bit mode. Cisco recommends using the default Mac OS X 10.6 Cisco IPSec client when connecting via VPN.

Cisco NAC Web Agent Version 4.7.1.504

In Cisco NAC Appliance Release 4.7(1), the Cisco NAC Web Agent version 4.7.1.504 has been enhanced to feature support for the Windows 7 client machine operating systems:

- Windows 7 Professional (32- and 64-bit)
- Windows 7 Ultimate (32- and 64-bit)
- Windows 7 Enterprise (32- and 64-bit)
- Windows 7 Home Premium (32- and 64-bit)
- Windows 7 Home Basic

Note

- Cisco NAC Web Agent version 4.7.1.504 does not support Windows 7 Starter Edition. Client machines with the Windows 7 Starter Edition operating system can only perform web login to verify user credentials. For specific information on enabling web login for client machines running Windows 7 Starter Edition, see Known Issue with Enabling Web Login for Windows 7 Starter Edition Clients, page 81.
- To avoid ActiveX initiation issues that could affect Agent download and web login functions, ensure users logging in via Windows 7 client machines maintain "elevated privileges" on the system by keeping the User Access Control (UAC) settings at the "default" level.
- Only the 32-bit version of Microsoft Internet Explorer 8 is supported in Release 4.7(1).
- Accessibility functions with version 10 the JAWS screen reader are not supported on Windows 7 operating systems.

For details on Agent functionality, refer to the "Cisco NAC Appliance Agents" chapter of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(2)*.

Features Optimized/Removed in Release 4.7(1)

Agent Stub Options Removed from Installation Page

The "Agent Stub" installation options have been removed from the CAM **Device Management > Clean Access > Installation** web console page. (These options are deprecated legacy configuration settings for the Clean Access Agent version 4.5.2.0 and earlier.)

Supported AV/AS Product List Enhancements (Windows Version 81, Mac OS X Version 5)

See Cisco NAC Appliance Supported AV/AS Product Lists, page 19 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 Agent, and is used to populate AV/AS Rules and AV/AS Definition Update requirements for 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.

Note In some cases, the specific AV/AS vendor software requires the user to have administrator privileges on the client machine to enable updates.

Windows 7/Vista/XP

For Windows 7/Vista/XP AV/AS support information on the Cisco NAC Agent (version 4.7.1.511) and Cisco NAC Web Agent (version 4.7.1.506), see the *Cisco NAC Appliance Release 4.7(1) Supported Windows AV/AS Products* document optimized for UTF-8 character display.

Mac OS X

- Supported Mac OS X AV/AS Product List Version Summary, page 20
- Mac OS X AV Support Chart, page 21
- Mac OS X AS Support Chart, page 22

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 Configuration Guide, Release 4.7(2)* for configuration details.

Note that Clean Access works in tandem with the installation schemes and mechanisms provided by supported AV/AS vendors. In the case of unforeseen changes to underlying mechanisms for AV/AS products by vendors, the Cisco NAC Appliance team will update the Supported AV/AS Product List and/or 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 4.7(1), page 17 for additional details on Agent versions in this release.

Supported Mac OS X AV/AS Product List Version Summary

Table 7 summarizes enhancements made for each version update of the Supported Antivirus/Antispyware Product List for the Mac OS X Agent. See Mac OS X AV Support Chart, page 21 and Mac OS X AS Support Chart, page 22 for details.

Table 7 Supported Mac OS X AV/AS Product List Versions

Version	Enhancements
Release 4.7(1)—4.7.1.506 Mac OS X Agent	

Table 7 Supported Mac OS X AV/AS Product List Versions (continued)

Version	Enhancements
Version 5	**Added AV def version**: • avast! Antivirus 2.x **Added new AV products**: • ClamXav 2.x • BitDefender 1.x

Mac OS X AV Support Chart

Table 8 lists Mac OS X Supported AV Products for Release 4.7(1) of the Cisco NAC Appliance software.

Table 8 Mac OS X Antivirus Product Support Chart
Version 5, 4.7.1.506 Mac OS X Agent, CAM/CAS Release 4.7(1) (Sheet 1 of 2)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update [2]
		Installation	Virus Definition	
ALWIL Software				
avast! Antivirus	2.x	yes (4.1.4.0)	yes (4.1.4.0)	-
ClamWin				
clamXav	0.x	yes (4.1.4.0)	yes (4.1.4.0)	yes
ClamXav	1.x	yes (4.1.4.0)	yes (4.1.4.0)	yes
ClamXav	2.x	yes (4.7.1.500)	yes (4.7.1.500)	yes
Computer Associates International, Inc.				
eTrust Antivirus	7.x	yes (4.1.4.0)	yes (4.1.4.0)	-
eTrust ITM Agent	8.x	yes (4.1.4.0)	yes (4.1.4.0)	-
Intego				
VirusBarrier X	10.x	yes (4.1.4.0)	yes (4.1.4.0)	-
VirusBarrier X4	10.4.x	yes (4.1.4.0)	yes (4.1.4.0)	-
VirusBarrier X5	10.5.x	yes (4.1.4.0)	yes (4.7.0.0)	-
McAfee, Inc.				
Virex 7.2	7.2.x	yes (4.1.4.0)	yes (4.1.4.0)	-
Virex 7.5	7.5.x	yes (4.1.4.0)	yes (4.1.4.0)	-
Virex 7.7	7.7.x	yes (4.1.4.0)	yes (4.1.4.0)	-
VirusScan	8.5.x	yes (4.1.4.0)	yes (4.1.4.0)	-
VirusScan	8.6.x	yes (4.1.4.0)	yes (4.1.4.0)	-
PC Tools Software				

Table 8 Mac OS X Antivirus Product Support Chart Version 5, 4.7.1.506 Mac OS X Agent, CAM/CAS Release 4.7(1) (Sheet 2 of 2)

Product Name	Product Version	AV Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Virus Definition	
iAntiVirus	1.x	yes (4.7.0.0)	yes (4.7.0.0)	-
SOFTWIN				
BitDefender	1.x	yes (4.7.1.500)	-	-
Sophos Plc.				
Sophos Anti-Virus	4.x	yes (4.1.4.0)	yes (4.1.4.0)	-
Symantec Corp.				
Norton AntiVirus	10.x	yes (4.1.4.0)	yes (4.1.4.0)	-
Norton AntiVirus	11.x	yes (4.1.4.0)	yes (4.1.4.0)	-
Norton AntiVirus	8.x	yes (4.1.4.0)	yes (4.1.4.0)	-
Norton AntiVirus	9.x	yes (4.1.4.0)	yes (4.1.4.0)	-
Trend Micro, Inc.				
Trend Micro Security for Macintosh	1.x	yes (4.7.0.0)	yes (4.7.0.0)	-
Trend Micro Security for Macintosh	3.x	yes (4.1.4.0)	yes (4.1.4.0)	-

1. "Yes" in the AV Checks Supported columns indicates the Agent supports the AV Rule check for the product starting from the version of the Agent listed in parentheses (CAM automatically determines whether to use Def Version or Def Date for the check).
2. The Live Update column indicates whether the Agent supports live update for the product via the 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 9 lists Supported Mac OS X Antispyware Products for Release 4.7(1) of the Cisco NAC Appliance software.

Table 9 Mac OS X Antispyware Product Support Chart Version 5, 4.7.1.506 Mac OS X Agent/CAM/CAS Release 4.7(1) (Sheet 1 of 2)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
SecureMac.com, Inc.				
MacScan	2.x	yes (4.1.4.0)	yes (4.1.4.0)	-

Table 9 Mac OS X Antispyware Product Support Chart
Version 5, 4.7.1.506 Mac OS X Agent/CAM/CAS Release 4.7(1) (Sheet 2 of 2)

Product Name	Product Version	AS Checks Supported (Minimum Agent Version Needed)[1]		Live Update[2]
		Installation	Spyware Definition	
Trend Micro				
Trend Micro Security for Macintosh	1.x	yes (4.7.0.0)	-	-

1. "Yes" in the AS Checks Supported columns indicates the Agent supports the AS Rule check for the product starting from the version of the Agent listed in parentheses (CAM automatically determines whether to use Def Version or Def Date for the check).
2. The Live Update column indicates whether the Agent supports live update for the product via the 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:

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 4.7(1)

Table 10 List of Open Caveats (Sheet 1 of 36)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsd03509	No	The Time Servers setting is not updated in HA-Standby CAM web console 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.

Table 10 List of Open Caveats (Sheet 2 of 36)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsg07369	No	Incorrect "IP lease total" displayed on editing manually created subnets Steps to reproduce: 1. Add a Managed Subnet having at least 2500+ IP addresses (for example 10.101.0.1/255.255.240.0) using CAM web page **Device Management > Clean Access Servers > Manage [IP Address] > Advanced > Managed Subnet**. 2. Create a DHCP subnet with 2500+ hosts using CAM web page **Device Management > Clean Access Servers > Manage [IP Address] > Network > DHCP > Subnet List > New**. 3. Edit the newly created subnet using CAM web page **Device Management > Clean Access Servers > Manage [IP Address] > Network > DHCP > Subnet List > Edit**. 4. Click **Update**. The CAM 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. The issue is judged to be cosmetic and does not affect DHCP functionality.
CSCsg66511	No	Configuring HA-failover synchronization settings on Secondary CAS takes an extremely long time Once you have configured the Secondary CAS HA attributes and click **Update**, 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.)
CSCsh77730	No	Agent locks up when greyed out **OK** button is pressed The 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. If the **Automatically close login success screen after** <*x*> **secs** option is enabled and the duration set to 0 (instantaneous) in the **Clean Access > General Setup > Agent Login** page and the user clicks on the greyed out **OK** button while the IP address is refreshing, the 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 Agent without exiting via the system tray icon, thus "killing" the Agent process. **Workaround** 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.

Table 10 List of Open Caveats (Sheet 3 of 36)

DDTS Number	Software Release 4.7(1) Corrected	Caveat
CSCsi07595	No	DST fix will not take effect if generic MST, EST, HST, etc. options are specified Due to a Java runtime implementation, the DST 2007 fix does not take effect for Cisco NAC Appliances that are using generic time zone options such as "EST," "HST," or "MST" on the CAM/CAS UI time settings. **Workaround** If your CAM/CAS machine time zone setting is currently specified via the UI using a generic option such as "EST," "HST," or "MST." change this to a location/city combination, such as "America/Denver." **Note** CAM/CAS machines using time zone settings specified by the "service perfigo config" script or specified as location/city combinations in the UI, such as "America/Denver" are not affected by this issue.
CSCsj46232	No	Agent should NOT pop-up during CAS HA failover Agent pops up during CAS HA failover. The user ISD still appears in the Online User List and the client machine still appears in the Certified Devices List. **Workaround** The user simply needs to close the Agent dialog and it does not pop up again.
CSCsk55292	No	Agent not added to system tray during boot up 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. 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. **Workaround** There are two methods to work around this issue: • Allow AD traffic through the CAS for clients in the Unauthenticated role. • Try to start the Agent manually after the install and auto load process fails.

Table 10 List of Open Caveats (Sheet 4 of 36)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsl13782	No	Microsoft Internet Explorer 7.0 browser pop-ups on Windows Vista launched from the Summary Report appear behind the Summary Report window 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. **Note** This problem only happens when a Google tool bar is installed and enabled in Internet Explorer.
CSCsl17379	No	Multiple Agent pop-ups with Multi NIC in L2 Virtual Gateway OOB role-based VLAN The user sees multiple Agent login dialogs with two or more active NICs on the same client machine pointing to the Unauthenticated network access point (eth1 IP address). After the first 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. **Workaround** The user can manually Disable Agent login pop-up after authentication.
CSCsl40626	No	Cisco NAC Web Agent should handle certificate revocation dialogs similar to persistent Agent 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 approximately 40 to 50 times. If the user clicks **Yes** to proceed enough times, the Web Agent fails to login and displays a "You will not be allowed to access the network due to internal error. Please contact your administrator." message to the user. **Workaround** Export the CAS's root CA certificate and install it in the trusted store on the client machine.
CSCsl40812	No	The **Refresh Windows domain group policy after login** option is not functioning for Cisco NAC Web Agent (It is working fine with the Clean Access Agent.) 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.

Table 10 List of Open Caveats (Sheet 5 of 36)

DDTS Number	Software Release 4.7(1) Corrected	Caveat
CSCsl75403	No	Mac OS X Agent does not detect VPN interface-fails MAC filters/L3 strict mode This caveat addresses two issues: 1. MAC filter does not work for Mac OS X client machines connected to the network in a VPN environment. 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. 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. **Workaround** To work around these issues: • For issue 1, use IP based filters for Mac OS X client machines in VPN environment. • For issue 2, Disable L3 strict mode on the CAS. **Note** This issue does not affect Windows client machines in VPN environment.
CSCsl77701	No	Network Error dialog appears during CAS HA failover 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." This is not an error message and the user is still logged in to the system. The user simply needs to click on the **Close** button to continue normal operation.
CSCsl88429	No	User sees Invalid session after pressing [F5] following Temporary role time-out 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.
CSCsl88627	No	Description of **removesubnet** has "updatesubnet" in op field The **removesubnet** API function description has "updatesubnet" listed in its operations field. The description should read "removesubnet."

Table 10 List of Open Caveats (Sheet 6 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCsm20254	No	CAS duplicates HSRP packets with Cisco NAC Profiler Collector Modules enabled. **Symptom** 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. **Conditions** Real-IP Gateway and Collector modules enabled on a CAS with ETH0 and or ETH1 configured for NetWatch. **Workaround** 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.
CSCsm61077	No	ActiveX fails to perform IP refresh on Windows Vista with User Account Control (UAC) turned on. 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. **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. Alternatively, the Cisco NAC Web Agent can be used with no posture requirements enabled. See also Known Issue for Windows Vista and IP Refresh/Renew, page 84.

Table 10 List of Open Caveats (Sheet 7 of 36)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCso15754	No	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 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. **Workaround** 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 **Remediate** button again after seeing the requirement fail in the first round of remediation tasks, it works just fine.
CSCso49473	No	"javax.naming.CommunicationException" causes no provider list ADSSO with LDAP Lookup If the LDAP connection to Active Directory fails during the lookup process (because the lookup takes a long time or the connection is suddenly lost), the Agent does not receive the list of authentication providers from the CAS. As a result, the user is presented with a blank provider list. 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. There is no known workaround for this issue. **Note** CSCso61317 is a duplicate of this caveat.

Table 10 List of Open Caveats (Sheet 8 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCso50613	No	Mac OS X Agent DHCP refresh fails if **dhcp_refresh** file does not exist DHCP refresh will fail with no notice (to the user or to the logs) if the **dhcp_refresh** file does not exist. The **dhcp_refresh** tool is required for all versions of Mac OS X Agents, so it always fails if the **dhcp_refresh** tool is missing regardless the Mac OS version. **Workaround** There are three ways to work around this issue: 1. Reinstalling the Mac OS X Agent automatically reinstalls the missing **dhcp_refresh** file. 2. Users can sign on to Cisco NAC Appliance via web login. The Java applet installs the **dhcp_refresh** tool if the **Install DHCP Refresh tool into Linux/MacOS system directory** option is checked under **User Page > Login Page > Edit > General**. 3. When using the Apple Migration Assistant, the user can try to include **/sbin/dhcp_refresh** in the migration list.
CSCso61317	No	When LDAP lookup fails for an AD SSO user, the Provider list in the Agent dialog is empty **Scenario 1** AD SSO configured with LDAP lookup 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. **Scenario 2 (less common)** The user is logged in to a machine that is not part of the domain, but the user does have an AD account. Steps that occur: 1. A TGT, obtained with the AD account, is granted. 2. The ST for the CAS is granted. 3. Agent passes the local account information since the user has logged in locally to the machine. 4. Authorization fails which causes the blank provider list. **Note** This bug is a duplicate of CSCso49473.

Table 10 List of Open Caveats (Sheet 9 of 36)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsr50995	No	Agent doesn't detect Zone Alarm Security definitions correctly Symptom: User fails posture assessment when checking for AV definitions for Zone Alarm Security Suite 7.0. Conditions: This occurs using either the Any AV check or the Checkpoint Any check. **Workaround** Create a custom check for Zone Alarm Security Suite definition.
CSCsr52953	No	RMI error messages periodically appear for deleted and/or unauthorized CASs in CAM event logs 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: • “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” • “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” **Workaround** • Reboot the CAS and wait for the CAM to re-establish connection. • Reboot the CAM after deleting and removing the CAS from the Authorized CCA Server list using the CAM **Device Management > CCA Servers > Authorization** admin web console page.

Table 10 List of Open Caveats (Sheet 10 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCsr90712	No	Symantec Antivirus delays Clean Access Agent startup The Agent takes a long time to pop up on a client machine with real-time antivirus scanning enabled and operating. **Workaround** Exclude the Clean Access Agent AV411 directory from Symantec Antivirus scanning. See http://service1.symantec.com/support/ent-security.nsf/docid/2002092413394848. **Note** The step to configure Extensions can be omitted. For Vista, refer to http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2008111414031848.

CSCsr95757	No	CAM intermittently stops processing SNMP MAC notification traps from the switch
		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.
		Note There is no **perfigo-log0.log.0** information, but a **tcpdump** from a CAM CLI session indicates that the CAM is receiving SNMP MAC notification traps.
		Workaround To re-establish correct SNMP trap handling on the CAM, open a CAM CLI session and enter the following commends:
		`service perfigo stop`
		`service perfigo start`
		The CAM immediately starts processing the SNMP MAC notification traps from the problem switch(es).
		Note After a period of time, however, this problem may appear again.

CSCsu47350	No	Invalid version number displayed in CAM backup snapshot web page When the administrator navigates to another page in the CAM web console during the backup snapshot process, the resulting snapshot version number is invalid.

Table 10 List of Open Caveats (Sheet 11 of 36)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsu63247	No	DHCP IP refresh not working for some Fedora core 8 client machines 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. **Note** There is no known workaround for this issue
CSCsu63619	No	Out-of-Band switch port information from OUL/CDL missing upon login after upgrade OOB switch port information in Online Users List/Certified Devices List is missing upon login after upgrading to Release 4.5. 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. **Workaround** 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. **Note** This issue is cosmetic and does not affect Cisco NAC Appliance functionality.
CSCsu78379	No	Bandwidth settings for Receiver CAM roles should not change after Policy Sync Steps to reproduce: 1. Create role on Master CAM, r1 2. Edit Upstream and Downstream Bandwidth fields of r1 to equal 1Kbps 3. Create role on Receiver CAM, r2 4. Edit Upstream and Downstream Bandwidth fields of r2 to equal 2 Kbps 5. Select role-based Master Policies to Export and perform manual sync 6. Upstream and Downstream Bandwidth fields for role r1 on Receiver CAM are changed to -1 (not 2 Kbps and not 1 Kbps). **Note** Receiver's Up/Down Kbps, Mode, Burst should either not change or should be the same as the Master.

Table 10 List of Open Caveats (Sheet 12 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCsu84848	No	CAM should set the switch port to Authentication VLAN before removing from OUL and DCL 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. **Workaround** Bounce the switch port to clear the OUL and DCL.
CSCsv18261	No	HA Failover database sync times out in event log after reboot 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. **Note** 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.
CSCsv18995	No	Three requirement types allow administrators to select single Windows XP/Vista operating systems when “All” is checked 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). **Note** This issue is not seen on the other requirement types. There is no known workaround for this issue
CSCsv20270	No	Conflicting CAM’s eth1 HA heartbeat address with Release 4.5.0 after upgrade 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. 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. **Workaround** Change to use the manual setting for eth1 on the fresh CD installed node or re-apply the HA config on the upgraded node.

Table 10 List of Open Caveats (Sheet 13 of 36)

DDTS Number	Software Release 4.7(1) Corrected	Caveat
CSCsv22418	No	CAS service IP not reachable after standby reboot due to race condition The Active CAS's service IP become unreachable after standby CAS reboot. In a rare race condition, the standby CAS temporarily becomes active for very short period of time after reboot. **Workaround** 1. Increase the "Heartbeat Timeout" value from the recommended 15 seconds to 30 seconds. 2. Or, run the heartbeat interface on Interface 3 (eth2 or eth3).
CSCsv78301	No	VPN SSO login does not work with VPN in managed subnet after upgrade to Cisco NAC Appliance Release 4.5 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). 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. **Workaround** 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.

Table 10 List of Open Caveats (Sheet 14 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCsv92867	No	DB conversion tool (Latin1 to UTF8)-iconv cannot work with † format Release 4.5 and earlier Clean Access Managers with foreign characters in the database cannot be upgraded to Release 4.6(1) and later. **Workaround** To upgrade from Release 4.1(6) or 4.5: • Perform a fresh install of Release 4.6(1) or later (recommend). • Remove any foreign characters from the database prior to upgrade.
CSCsw39262	No	Agent cannot be launched when switching between users in Vista The Cisco NAC Agent does not support Windows Fast User Switching. The effect is that the primary user is the only user that: • Can log into the Clean Access Server and based on the level of authentication will dictate the system's access to the network. • Will see the NAC Agent tray icon. • Will be able to re-authenticate if kicked off the network via the Clean Access Server. **Note** 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. **Workaround** Logging out the first user or closing the Cisco NAC Agent before Fast Switching eliminates this problem.
CSCsw45596	No	Username text box should be restricted with max no of characters 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.
CSCsw67476	No	Mac OS X Agent upgrade cannot be restarted once stopped User is not able to log in again (no agent screen or icon available) when they cancel the Mac OS X Agent upgrade process. **Note** This issue has been observed when upgrading from Release 4.5 to 4.6(1) and later. **Workaround** Manually start the agent which then started the upgrade portion.

Table 10 List of Open Caveats (Sheet 15 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCsw88911	No	Mac Agent freezes on login dialog, but remains operational 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). **Workaround** Operationally, everything is running normally (the machine is OOB and logged in per CAM and client) just the user interface is locked up.
CSCsw89027	No	Mac OS X Agent logs can grow too large in debug and do not clean up When Agent logging is set to "Defect", Mac OS X Agent logs grow too large. **Workaround** Do not compile Mac OS X Agent logs in debug mode for extended periods of time.
CSCsx03338	No	HTTP packet to a host using reversed IP address after connection on Mac OS X client The Mac Agent sends a packet to UDP port 80 to the reversed IP address of the client's default gateway every 5 seconds. **Note** 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). **Workaround** Disable the access-to-auth vlan-detection by following the instructions at http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/461/cam/m_oob.html.
CSCsx05054	No	DHCP does not work with IGNORE fallback policy and CAS Failover 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. **Workaround** 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.
CSCsx18496	No	Cisco Log Packager crashes on XP Tablet PC with Restricted User credentials

Table 10 List of Open Caveats (Sheet 16 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCsx27857	No	With session timer disabled for the Agent Temporary role, version 4.6.0.3 of the Mac OS X Agent times out If the Temporary role timer disabled on the CAM, the Mac Agent times out right away. **Note** There is no known workaround for this issue.
CSCsx29191	No	Mac OS X Agent has no 'APPLE'+TAB presence When using the Mac OS X Agent, the GUI focus can get lost and is hard to regain. This issue was observed during upgrade. **Workaround** Using hot corners to show all applications. With this tool, users can find the Agent and continue the process.
CSCsx35438	No	Clean Access Manager read timeout reached when deleting many DHCP IPs at once 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. **Workaround** Please see Known Issue with Mass DHCP Address Deletion, page 81.
CSCsx35911	No	Mac OS X Agent does not pop up for login and click-focus does not get user's attention 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. **Workaround** Click on the upper right icon that is saying click focus and then login.

Table 10 List of Open Caveats (Sheet 17 of 36)

DDTS Number	Software Release 4.7(1) Corrected	Caveat
CSCsx37073	No	Cisco NAC Agent does not pop-up if authentication server name is \\ Steps to reproduce: 1. Create a Kerberos authentication server named \\ in addition to Local DB. 2. Go to **Login Page > Content** and check Provider Label, **Local DB**, \\ (def provider). 3. Let the Cisco NAC Agent pop-up. User sees \\ and Local DB as Server options. (This is as expected.) 4. Go to **Login Page > Content** and uncheck **Local DB**. 5. Let the Cisco NAC Agent pop-up again. This time, user sees only the \\ Server option. (This is also as expected.) 6. Go to **User Management > Auth Servers** and delete \\. 7. Close the Cisco NAC Agent window, which does not pop-up again. 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. **Workaround** Avoid non-alphabetic naming conventions when configuring authentication servers in Cisco NAC Appliance.
CSCsx45051	No	Agent may proceed with AV/AS auto remediation while it's not supported 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. **Note** This issue is observed with MS Live One 2.x. Auto Remediation fails when configured for MS Live One 2.x. **Workaround** Remediate AV manually while in the temporary role.

Table 10 List of Open Caveats (Sheet 18 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCsx47987	No	Incorrect behavior when client wired/wireless NIC on same subnet as CAS Scenario to reproduce: • Client is connected through both wired and wireless port to the same OOB CAS. • Wireless NIC IP address is on the same subnet as that of CAS. • Wired port is assigned a lower metric compared to wireless, so wired is the preferred port. • 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. As a result, the client is not able to ping the CAM or access any outside network.
CSCsx49160	No	Cisco NAC Agent shows one less authentication provider if one of the provider names is \ Steps to reproduce: 1. Create a Kerberos authentication server called my_krbr. 2. Create a login page and check the **Local DB** and **my_krbr** (def provider) Provider Labels. 3. Let the Cisco NAC Agent pop-up. Both my_krbr (def provider) and the Local DB provider options are available. 4. Go to the list of Authentication Servers and rename my_krbr to \. 5. Go to the Login page. \ appears as the new Kerberos name. 6. Close the Cisco NAC Agent and let it automatically pop-up again. This time, the authentication provider list only shows Local DB—\ is missing. **Workaround** Avoid non-alphabetic naming conventions when configuring authentication servers in Cisco NAC Appliance.
CSCsx78577	No	ClamAV not showing def date ClamAV does not provide the definition date to the Agent. **Workaround** There is no workaround at this time. This is a known issue.

Table 10 List of Open Caveats (Sheet 19 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCsx81395	No	Sophos AV Definition rule fails even if Mac OS Agent has the latest definition The remediation window pops up for updating the Sophos definition files on the Mac OS Agent even though Sophos is updated. This occurs if Sophos is installed on the Mac OS client and an AV definition check for Sophos is configured on the CAM. **Workaround** There is no workaround at this time.
CSCsx95230	No	Length of token is not printed in the ADSSO logs When ADSSO logging is changed to DEBUG for troubleshooting purposes, the ADSSO logs display the token but not the token size. **Workaround** None.
CSCsy00609	No	Role mapping uses cached entry on quick reconnects 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. 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. **Workaround** This issue is not actually a bug. Caching behavior is configurable using the **Authentication Cache Timeout** setting available on the CAM **User Management > Auth Servers > List/New** web console page. If it is desired to never cache user login, set this timer to 0. **Note** This workaround may affect CAM performance due to increased authentication traffic for multiple users logging into Cisco NAC Appliance.
CSCsy32119	No	Cisco NAC Appliance CAM/CAS need ability to set port speed/duplex manually 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. **Note** There is no known workaround for this issue.
CSCsy45807	No	Mac OS X Agent does not pop up using Sprint Wireless This issue has been encountered using Sprint Wireless Novatel U727 on 2 different Mac OS X client machines.

Table 10 List of Open Caveats (Sheet 20 of 36)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsz19346	No	Korean log packager GUI translations/buttons are garbled & some missing **Workaround** Some of the buttons are still readable. Click **Collect Data > Locate File** and then click **Exit**.

CSCsz19912	No	Log Packager CiscoSupportReport file shows ##### in place of system info
		
		The system logs created by the log packager are showing ##### instead of actual data, as in the following examples:
		
		`04/23/2009 10:49:22 W32Time (ID=0x825a0083): NtpClient# 'CCAVPN-AD'# DNS ## ### ## ## #### ### ### ### #### #####. NtpClient# 15# ## ## #### # ### ### ### # ## ###. ##: ### #### ####. (0x80072AF9).`
		
		`04/23/2009 10:49:21 W32Time (ID=0x825a0083): NtpClient# 'CCAVPN-AD'# DNS ## ### ## ## #### ### ### ### #### #####. NtpClient# 15# ## ## #### # ### ### ### # ## ###. ##: ### #### ####. (0x80072AF9).`
		
		This issue occurs on Japanese, Korean, and Chinese systems using Cisco Log Packager.
		
		Note There is no known workaround for this issue. Log Packager is still functioning, but it is missing some non-critical system troubleshooting information.

CSCsz38970	No	Accessibility: login displays not announced 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. **Note** This issue has been observed in a deployment where JAWS is set to run at system startup. **Workaround** You have to select the Cisco NAC Agent from the taskbar to have the Agent display announced.
CSCsz48766	No	MAC Agent VLAN change detection logic causes AnyConnect to disconnect Anyconnect client constantly loses connection to VPN network when using the Mac OS X Agent with the VlanDetectInterval set to 5 seconds. **Workaround** The **settings.plist** 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.

Table 10 List of Open Caveats (Sheet 21 of 36)

DDTS Number	Software Release 4.7(1) Corrected	Caveat
CSCsz48847	No	Accessibility: after successful log-in, JAWS is still on Cisco NAC Agent page JAWS stays on The Cisco NAC Agent window even though no Agent window is displayed. **Workaround** Press the Windows key to go back to the Windows desktop.
CSCsz49147	No	Accessibility: JAWS does not announce installer after upgrade During upgrade of the Cisco NAC Agent, the MS installer window is not announced. **Note** This does not impact the upgrade process. **Workaround** A blind user will need to check the running applications in the Windows taskbar.
CSCsz80035	No	"ANY" AV remediation for Trend Micro 17.1 fails The AV update for Trend Micro version 17.1.1250 shows a failure in the Cisco NAC Agent window, but the update is successful. **Workaround** Click **OK** on the error display. The AV update is actually successful.
CSCsz83270	No	Agent file download fails at lower speed WAN links between CAS and CAM 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. This happens during agent upgrade or download from web page when CAS and CAM are separated by a WAN link (512kbps/256kbps). **Workaround** 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. **Note** Problem usually corrects itself after a while, but if it does not, Cisco recommends following this workaround.

Table 10 List of Open Caveats (Sheet 22 of 36)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsz85892	No	Web login display Guest ID instead of Username Steps to reproduce: 1. Add a Kerberos auth server named “k1.” 2. Enable the Local DB and “k1” providers on the Login Page, and make “k1” the default provider. 3. Open a browser and check that Username is there and “k1” is the default provider. 4. Delete “k1” from the roster of Auth Servers. 5. Open another browser and note that the user name is now “Guest ID.”

Table 10 List of Open Caveats (Sheet 23 of 36)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsz88018	No	Clean Access Agent installs on Windows 7 beta, fails remediation, then sends Success to CAM Clients running Windows 7 Beta are able to successfully download and install the Clean Access Agent and log in to the Cisco NAC Appliance network. However, AntiVirus posture assessment checks do not appear to be working and if users pass authentication, they are not cleared for network access when the AntiVirus information is not correct on the current Agent version. This issue has been observed is a Cisco NAC Appliance Release 4.5 deployment. **Workaround** There are two possible workarounds for this issue: • Windows 7 is included in the OS group "Windows All." By setting the Cisco NAC Web Agent to work with "Windows All" operating systems, but still requiring the full Agent under Windows XP, Vista, and 2000, the Web Agent acts as an installation workaround. • Create a custom registry check to deny access from Windows 7 systems: – Check Category: Registry Check – Check Type: Registry Value – Check Name: Windows_7 – Registry Key: HKLM:SOFTWARE\Microsoft\Windows NT\CurrentVersion\ – Value Name: ProductName – Value Data: String – Operator: Does not contain – Value Data: Windows 7 – Check Description: – Operating System: Windows All

Table 10 List of Open Caveats (Sheet 24 of 36)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsz92761	No	CAM GUI and publishing behavior during DB restore 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. This issue occurs when the CAM and CAS are connected via WAN links (T1/256k/512k) with several CASs experiencing at least 400ms delay. **Note** 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. **Workaround** DBrestore happens and CAS do get connected and publishing completed.
CSCsz97199	No	McAfee AV_TotalProtectionforSmallBusiness_4_7_x upgrade to 5.0 issues 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. **Note** There is no known workaround for this issue.
CSCta03527	No	Discovery Host can not be changed by uploading XML on CAM 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. **Workaround** Manually edit the XML file on the client machine or keep using the Discovery Host address specified on the CAM.
CSCta12544	No	Server communication error upon web and Agent login 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.
CSCta19323	No	Memory for crash kernel message seen during 4.7.0 CD install The message is benign, it is displayed when memory is not configured/allocated for a crash kernel to aid in crash dump. This is displayed by Red Hat and CentOS 5 releases while booting on any system.

Table 10 List of Open Caveats (Sheet 25 of 36)

DDTS Number	Software Release 4.7(1) Corrected	Caveat
CSCta35732	No	Deleting subnet filters causes CASs to disconnect When you delete the subnet filter one after another from the CAM, the web console slows down and looses connection to the associated CAS. 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. **Note** After a few minutes, CASs come back online.
CSCta35741	No	Agent not Popping up for First time for TLS not enabled on IE 6.0 If TLS 1.0 is not enabled on Microsoft Internet Explorer browsers when the user launches the Cisco NAC Agent, the Agent dialog/login screen does not appear. **Workaround** The user must Exit the Cisco NAC Agent using the Windows Systray icon and launch the Agent again.
CSCta43634	No	JSF library throws duplicated ID in faces tree exception occasionally This condition can occur if the user inadvertently double-clicks a hyperlink, resulting in the CAM web console returning an exception error. **Workaround** Log out and log back into the CAM web console.
CSCta85491	No	Cisco API: addmac is susceptible to XSS on the CAS when using local device filter Steps to reproduce: 1. Call addmac for a global device filter where the description contains <script>alert('CAS specific XSS'); </script>. No pop-up alert box is observed. 2. Call addmac for a CAS-specific local device filter where the description contains <script>alert('CAS specific XSS'); </script>. 3. Go to the CAM web console and click the manage icon for the CAS in question and then go to **Filter > Devices**, You should see a pop-up alert box with a CAS-specific XSS message. **Note** This is not an issue for global device filters calling addmac.
CSCta97229	No	Collector Modules show “Stopping” instead of “Stopped” in Profiler UI This issue happens when the administrator manually stops the Profiler Collector. **Workaround** Services are actually stopped. You can enter `service collector status` in the CAS CLI to verify the current state.

Table 10 List of Open Caveats (Sheet 26 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	**Caveat**
CSCtb02366	No	"ANY" AS update does not work for MS Defender on 64-bit Vista **Workaround** Set up the check using Microsoft as the AS vendor. **Note** The same requirement works correctly on a Vista Home Professional PC.
CSCtb17138	No	CAM or CAS UI not reachable after failover pair recover from network partition If a CAM HA pair loses connectivity and connectivity is subsequently restored, in some cases the CAS service IP address is not reachable and CAM-CAS communication fails. **Workaround** Bring up eth0 connectivity before bringing up any other heartbeat interface. **Note** Cisco strongly recommends configuring the HA Linkdetect feature on the CAM's eth0 interface. If this is done, the above issue does not occur.
CSCtb30587	No	Clearing CAM CDL upon intra-subnet roaming keeps client in Access VLAN This issue has been seen on WLC1 managing AP1 and WLC2 managing AP2 have same SSID with WLANs on both the controllers mapped to interface which are on the same subnet. (Both controllers are running version 6.0.182.0.) Steps to reproduce: 1. Client is initially associated to AP1. Do a posture validation on the client and client entry is shown on WLC1. 2. Now disable AP1. The client machine is associated to AP2, the client entry is deleted from WLC1, and the client entry is now available only on WLC2. Client is now in Access VLAN and client entry shown on WLC2. However, the CAM still lists WLC1 IP address with client entry. 3. Clear the CDL and OUL from the CAM. The client still appears in the Access VLAN, has complete access to the internet, and an error appears in the CAM's **nac-manager.log** file after clearing the CDL and OUL on the CAM.

Table 10 List of Open Caveats (Sheet 27 of 36)

DDTS Number	Software Release 4.7(1) Corrected	Caveat
CSCtb30691	No	Agent pops up from and active wired NIC after user is already authenticated via a wireless NIC in the same client machine After authenticating using the wireless NIC with a higher preference than the wired NIC on the same client machine, the Agent pops up again, prompting the user to enter authentication credentials. This happens on Windows XP SP3 client machines. (This issue has not been observed in Windows XP SP2.) **Workaround** The problem is caused by a Windows TCP/IP feature called "Dead Gateway Detection." To disable this feature, set the "EnableDeadGWDetect" registry value under HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters to 0, then reboot the client machine.
CSCtb32797	No	LDAP GSSAPI with SSL lookup and authentication fails The Cisco NAC Appliance network returns the following message: "Unsupported Ldap Operation ([LDAP: error code 53 - 00002029: LdapErr: DSID-0C09048A, comment: Cannot bind using sign/seal on a connection on which TLS or SSL is in effect, data 0, v1771])" or "Naming Error (dcchild.child.2k8.com:636; socket closed)" **Note** Microsoft has documented this error on its support site at http://support.microsoft.com/kb/957072. Unfortunately, Windows 2008 server SP2 with the latest Windows updates as of 8/20/09 did not resolve this problem. **Note** There is no known workaround for this issue.
CSCtb38026	No	Scripting error with database restore with modified DB snapshot name If the database snapshot name is altered to include some string after the version number and before the .gz suffix like the following: `08_12_09-23-48_snapshot_VER_4_7_0_A23_upgraded_from_4-1-3.gz` the database restoration process returns a scripting error. This issue is only cosmetic and does not affect the database restore functionality. **Workaround** Do not rename the database snapshot (for identification purposes, for example) after it has been created.

Table 10 List of Open Caveats (Sheet 28 of 36)

DDTS Number	Software Release 4.7(1) Corrected	Caveat
CSCtb43264	No	Both HA-CAS nodes stuck in active-active state Steps to reproduce: 1. Do a fresh install of both CAS nodes and the CAM. 2. Configure high availability for the CAS HA-pair. 3. Reboot both the HA-CAS nodes at the same time. 4. Add the primary CAS to the CAM. The CAM reports the CAS to be disconnected. 5. Click **Manage** where the CAM web console reports "SSKEY on server does not match the value in database." 6. Click **Advanced > Managed Subnet** and add a managed subnet. Both CASs appear to be active-active. This is a dangerous scenario creating a Layer 2 broadcast loop that almost immediately brings down the network. **Workaround** There are two possible remedies for this issue: • Configure a longer heartbeat timeout interval for the HA-pair. • Add an additional heartbeat Ethernet interface link (eth2, eth3).
CSCtb55184	No	Web Agent download fails if the CAS IP address in the trusted certificate is different from the CAS domain IP address. This situation can occur when the CAS is in Layer 2 In-Band Real-IP gateway mode, and IP used for initial SSL cert during install is different from that imported using the web console. **Workaround** Enter `service perfigo restart` on the CAS to resolve this issue.
CSCtb58837	No	Database write to HA-Secondary CAM fails Standby CAM can occasionally fall out of sync with Active under stress load condition where there is a lot of very rapid individual update to the HA-Standby appliance for a very long period of time (i.e. users logging on and off and many changes to the device filter list, for example). **Workaround** Restart the Standby node to bring it back in sync with Active.

Table 10 List of Open Caveats (Sheet 29 of 36)

DDTS Number	Software Release 4.7(1) Corrected	Caveat

CSCtb61012	No	Web Console should show the correct status of an HA-Standby CAM/CAS
		
		When you go into the failover section in the GUI to check the status, it only shows the other CAM or CAS as active but not the actual state of the local appliance.
		
		Note You can use the CLI to display the correct state of the HA-Secondary as follows:
		
		`[root@NACM-1 bin]# ./fostate.sh`
		`My node is standby, peer node is active`

CSCtb63619	No	Cannot manage a CAS over JMX
		
		This situation can happen when there are multiple large publishing requests over a slow link connection and the system demands exceed the publishing queue. (The default max publishing queue size is set to 10.)
		
		Workaround Retry the operation again when the queue frees up or increase the max queue size. To increase the queue size:
		
		1. Modify the **/perfigo/control/bin/starttomcat** file by adding the following at the end of the `CATALINA_OPTS=<...>` line:
		
		`-DJMX.WRITELOCK.QUEUEDEPTH=<any number>`
		
		For example:
		
		`CATALINA_OPTS="-server -Xms64m -Xmx${MAX}m -Dcom.ncipher.provider.announcemode=off -Dcom.ncipher.provider.enable=Signature.NONEwithRSA,KeyFactory.RSA,Cipher.RSA -DJMX.WRITELOCK.QUEUEDEPTH=20"`
		
		2. Enter **`service perfigo restart`** to enable the change.

CSCtb66010	No	**NACAgentCFG.xml** file is not preserved after CAM upgrade The Agent configuration XML file packaged with the Cisco NAC Agent is not preserved after upgrading from Release 4.6(1) to 4.7. **Workaround** Upload a new **NACAgentCFG.xml** file.

Table 10 List of Open Caveats (Sheet 30 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCtb92910	No	Need to reflect all the states of FIPS card in the UI and CLI Currently, the web console page only reflects whether or not the FIPS card is operational, but states like maintenance or initialization are not reflected. **Workaround** If the CAM **Monitoring > Summary** page does not show that the FIPS card is operational, assume it is in one of the other states (Maintenance or Initialization). You can also manually verify the electromagnetic switch position ("O," "M," or "I") on the FIPS card, itself when you look at the back of the NAC-3315/3355/3395 chassis. **Note** Once the FIPS card is Operational on the CAM/CAS, the position of the electromagnetic switch on the FIPS card does not come into play again until you reboot either the FIPS card or the appliance.
CSCtb95381	No	Cisco NAC Appliance certificates not signed and/or expiring soon Cisco NAC Appliance Release 4.7.0 comes with the following files that are either not signed or expire in March 2010: • CCALogin.cab Cisco certs expires 3/10 versign 6/12 (CCAWebLogin.ocx 2.3.0.0 not signed) • CiscoNACLoginFacilitator Java signature expiring in march/2010 (taweb.jar expires 3/10 please see attached file) • CCALogin.jar entry was signed on 10/3/08 1:10 PM (X.509, CN=Cisco Systems, OU=INFORMATION SECURITY, O=Cisco Systems, L=San Jose, ST=California, C=US [certificate is valid from 2/25/08 7:00 PM to 3/31/10 7:59 PM])
CSCtb98457	No	Posture Assessment requirements for Vista machines results in the user being placed in the temporary role. This has been observed in Windows Vista Home operating systems running version 4.6.2.113 of the Cisco NAC Agent. **Workaround** Disable compatibility mode for **Nacagent.exe**. Compatibility mode can be disabled by un-checking (disabling) the "Run this program in compatibility mode for" option in the file properties for **NACagent.exe**.

Table 10 List of Open Caveats (Sheet 31 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCtc00668	No	Mac Agent trying to update Avast even though application is up-to-date Following login, the Mac Agent pops up prompting user to update "ANY" AV. **Workaround** To work around this issue: 1. Change the Mac OS X Agent LogLevel in the settings.plist file to "Error." 2. Log out of the Cisco NAC Appliance network, and exit the Agent to ensure the new LogLevel will take effect. 3. Log back into the network. The problem should now be gone.
CSCtc01957	No	Firefox 3.5.2 Freezes and user cannot enter user credentials After the applet loads in the Firefox browser, the user login page locks up and the user is unable to enter login credentials.This situation can occur when a user is attempting web login with a FireFox 3.5.2 browser for the very First time. **Workaround** The workaround for this issue is to minimize the Browser or open a new browser window.
CSCtc41408	No	Windows 7 tray icon default should be show icon and notifications According to Microsoft, there is no way for a program to promote itself by setting the "Show Icon and Notifications" option. This can be done only by the user and only manually. Default behavior is to hide all icons. **Workaround** The Windows 7 client machine user can change this behavior by either drag-and-dropping the hidden icon or by changing the "Show Icon and Notifications" setting.

Table 10 List of Open Caveats (Sheet 32 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCtc46376	No	Windows WSUS update (Microsoft rules) is not working for KB890830 When a WSUS update is performed on a new installation of Windows 7 (where no updates have been applied), and the **No UI** option is selected for the requirement, the WSUS update can fail. The portion of the Windows update that fails to install is the KB890830 update (Windows Malicious Software Removal Tool, http://support.microsoft.com/?kbid=890830). This upgrade must be installed with admin privileges and there is a one time EULA that the user must accept during installation. After KB890830 is installed, there are monthly updates that are pushed out from Microsoft on patch Tuesday. The subsequent updates of KB890830 do not require admin privileges and they work fine on a client where the user is not a member of the admin group. If users manually install KB890830 on a client system as a non-admin user using Windows Update, they are prompted for the administrator password and then get the EULA. **Workaround** Ensure new installations of Windows are brought up to date by a user with administrator privileges prior to turning the client machine over to users without administrator privileges.
CSCtc52252	No	Cannot uninstall the Agent using MSI executable with full quiet mode selected If you open a Command Prompt window and run the MSI install/uninstall commands using the quiet option, the command fails. **Workaround** You must open the Command Prompt window using the "Run as Administrator" option, even if you are administrator on the system.

Table 10 List of Open Caveats (Sheet 33 of 36)

DDTS Number	Software Release 4.7(1) Corrected	Caveat
CSCtc59248	No	The Agent does not launch if IE has never been launched or the CA certificate is not installed The Cisco NAC Agent login window does not pop up (or takes a long time to pop up) during initial login because: • The CA cert that signs the CAS server cert has not been installed • IE has never been launched before by the user This problem could also occur when the administrator kicks the user out of the NAC Appliance network after logging in via and OOB session. **Workaround** - Deploy the CA cert that signs the CAS server cert before user loges in and instruct the user to start IE after experiencing this problem. **Note** The Cisco NAC Agent running in a Windows 7 environment allows the user to install the CA certificate at initial login.
CSCtc66277	No	IP refresh takes a minute and Agent vanishes after that This issue can come up in a network where spanning tree merge has been configured on the switch. Configuring portfast minimizes the IP refresh time. **Note** Cisco recommends enabling port-fast switch configuration whenever appropriate to do so.
CSCtc66798	No	Agent refreshing IP continuously, even though there is no change in VLAN The Mac OS X console displays a lot of messages saying that the Mac OS X Agent is Refreshing the client machine IP address, even though the client machine is logged in via In-Band where there is no need to look for VLAN change detection and the IP address has actually not changed at all. **Workaround** There is no known workaround for this issue.
CSCtc68565	No	Web Agent does not launch using ActiveX on a client machine where the administrator UAC is “default” When using Windows 7 as a local machine administrator and a proxy server, Internet Explorer places the CAS into the intranet settings category, which automatically disables “Protected Mode.” **Workaround** Enable “Protected Mode” in Internet Explorer for intranet sites.

Table 10 List of Open Caveats (Sheet 34 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCtc86765	No	The Cisco NAC Agent does not pop up in a VPN environment upon re-connecting to the VPN server This issue has been observed when power cycling a SOHO (Small office home office) DSL/Cable modem router, thus terminating the VPN connection. **Workaround** Exit and re-launch the Cisco NAC Agent.
CSCtc90896	No	For McAfee Total Protection 5.0, you need to change firewall setting AV definition file update for McAfee Total Protection 5.0 does not work with the default McAfee firewall settings. **Workaround** For AV definition file update to work for McAfee Total Protection 5.0, you need to change the McAfee firewall setting from "Untrusted Network" to "Trusted Network" or "Custom" and allow the McAfee program to access the update site.
CSCtc91616	No	Support for Internationalized characters in usernames It is unclear if Internationalized characters are supported in usernames for NAC. For example, some internationalized characters (like è) are allowed when creating a username, but user login fails. Other character sets (like Japanese) fail when attempting to create the user in the Local DB.
CSCtc92037	No	Mac agent in L2 non-strict mode does not pop up behind NAT router. With L2 non-strict mode and Mac client behind NAT router, Mac agent does not pop up.
CSCtd07929	No	Anchor does not forward DHCP Packets in NAC OOB with Inter Subnet Mobility Windows 7 client machines have complete network access only for a short time following authentication and posture assessment when they then roam to a foreign WLC. The result is that the client machine is automatically moved to the quarantine VLAN, and the Cisco NAC Agent reappears prompting the user for login credentials.
CSCtd04881	No	Serbian web install shows error and installer is English A popup window appears with an error message in Serbian, which approximately translates to, "Writing error in applied transformation. Recommend to use a valid transformation path." After clicking **OK** the installer launches in English, yet the application launches and is fully functional in Serbian. **Note** There is no known workaround for this issue.
CSCtd12250	No	Incorrect AntiVirus def date is displayed in CAM reports This issue has been observed on client machines with an iAntiVirus def date of 11/05, but the CAM report displays some day in August. **Note** There is no known workaround for this issue.

Table 10 List of Open Caveats (Sheet 35 of 36)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCtd14712	No	CAS info missing from new Active CAM when master secret different When the master secret is different on two CAMs in an HA deployment, some critical CAS information may be missing on the secondary (standby) node. **Workaround** Restore the correct master secret on the incorrect CAM.
CSCtd16666	No	Mac Agent installer is not creating preference.plist file The Mac Agent automatically creates a **preference.plist** file when either or both of the "Auto Popup Login Window" or "Remember Me" options are enabled for the Mac Agent. If neither of these options are enabled for the Agent, the user would have to manually produce a preferences.plist file on the Mac OS X client machine.
CSCtd23998	No	Uploading large distribution files should not corrupt the database When files larger than 50MB are uploaded to the CAM for File Distribution requirement types, the database snapshot could become corrupted. This issue has been observed on NAC-3140 CAMs where a distribution file larger than 50MB has been uploaded. **Workaround** Remove the large distribution file from the CAM and use a Link Distribution requirement type to point users to a download domain where they can retrieve the file.
CSCtd37076	No	Missing "Referral" option for LDAP type Under **User Management > Auth Servers** for LDAP authentication type, the "Referral" option is missing in the web console for a pull-down menu with options "Manage(Ignore)" and "Handle(Follow)".
CSCtd39544	No	In certain cases, root CA certificate is categorized as CCA cert in SSL user interface The SSL user interface for an X509 certificate chain is used with a multi-tier hierarchy may not display the Root CA cert. **Note** This issue is only cosmetic and does not impact SSL functionality.
CSCsx52263	No	NAC Appliances always assume USA keyboard layout 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. **Workaround** Use a US layout keyboard or ensure that you know the key mapping if you are connecting a keyboard of different layout.

Table 10 List of Open Caveats (Sheet 36 of 36)

DDTS Number	Software Release 4.7(1)	
	Corrected	Caveat
CSCtg39044	No	Running Internet Explorer in offline more effects Cisco NAC Agent auto-upgrade function 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 4.7.2.10 and earlier. The login session appropriately prompts the user to upgrade the Agent, but clicking **OK** brings up the login screen instead of launching the Agent installer.
CSCtj81255	No	Two MAC addresses detected on neighbooring switch of ACS 1121 Appliance. **Symptom** Two MAC addresses are detected on the switch interface connected to an ACS 1121 Appliance although only one interface is connected on the ACS 1121 Server eth 0. **Conditions** Only one Ethernet interface, eth 0 is connected between ACS and Switch. **Workaround** Disable BMC (Baseboard Management Controller) feature using BIOS setup. ⚠ **Caution** To help prevent a potential network security threat, Cisco strongly recommends physically disconnecting from the Cisco NAC console management port when you are not using it. For more details, see http://seclists.org/fulldisclosure/2011/Apr/55, which applies to the Cisco ISE, Cisco NAC Appliance, and Cisco Secure ACS hardware platforms.

Resolved Caveats - Release 4.7(1)

Refer to Enhancements in Release 4.7(1), page 17 for additional information.

Table 11 List of Resolved Caveats (Sheet 1 of 3)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsu69247	Yes	ERROR: File type requirements does not exist During CD installation of Cisco NAC Appliance Release 4.5, users can see the following error message in the nac_manager.log file: "2008-09-21 19:25:55.592 -0700 ERROR com.perfigo.wlan.web.admin.DMSoftwareManager - DMSM syncDMSoftware: Directory('/perfigo/control/tomcat/webapps/packages/') for file type requirements does not exist" 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.
CSCsu84977	Yes	CAS: ERROR /proc/click/intern_filter_group/failsafe The following error message can appear to users during CD installation of Cisco NAC Appliance Release 4.5 in Clean Access Servers: "com.perfigo.wlan.jmx.Shell - /proc/click/intern_filter_group/failsafe (No such file or directory)" This error message is related to a recently-removed file failsafe and has no impact on CD installation.
CSCsu88594	Yes	Removal of www.perfigo.com Root CA from GUI The www.perfigo.com Root CA should be removed from the GUI. 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). **Workaround** To change this behavior go to **Administration > User Pages > Login Page > Edit > Content** and deselect the **Root CA** table entry.
CSCsw30518	Yes	IP address renewal not working on most Linux distributions using web login in Release 4.5(x) Web login on Linux clients does not refresh the client IP address. If users refresh the client IP address themselves, they are authenticated fine. **Note** Web login also prompts the user to enter login credentials for the root password even if the CAM is configured not to ask for it.

Table 11 List of Resolved Caveats (Sheet 2 of 3)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCsx44912	Yes	The CAS ignores part of large role policy list and blocks traffic Some rules in a user role's traffic policy list may not function if the list is too large. There is a cut-off point and every rule below that point fails. Moving a rule up above that point (changing the rule's position in the priority list) causes it to start working again. **Workaround** Consolidate traffic policies to smaller amount, or move all essential policies up above the cutoff point. **Note** This issue has been observed with 102 rules as the cut-off, however this figure does not appear to be a static cut-off point.
CSCta53492	Yes	Device management filter description misleading The following text appears in the **Device Management > Filter > Devices** page: "By default, Cisco Clean Access (CAS) forces user devices (identified by MAC address and IP address combination) on the untrusted side of the CAS to authenticate in order to access the network. This page allows you to specify options to bypass authentication and posture assessment on devices's MAC address (and/or IP address)." In the last sentence, it should read "This page allows you to specify options to bypass authentication and posture assessment on devices depending the deployment: Out-of-Band: MAC address only L2 In-Band: MAC address, MAC address and IP address"
CSCtb32045	Yes	Message while preparing root file system during installation misleading Fresh image installation on a NAC-3395 takes at least 30 minutes for preparation.
CSCtb54272	Yes	Microsoft Forefront Client Security AV Def Date not supported Users fail the following check for the AV Def Date, which was working in previous Cisco NAC Appliance releases: av_defn_MicrosoftForefrontClientSecurity_1_5_x, Antivirus Check [Microsoft Forefront Client Security 1.5.x up to date]
CSCtb71856	Yes	Cisco API doc: Missing ssip is required for removesubnet removesubnet API function returns "<!--error=Subnet could not be found-->". There is no mention of ssip in removesubnet description in Cisco NAC Appliance Release 4.7.

Table 11 List of Resolved Caveats (Sheet 3 of 3)

	Software Release 4.7(1)	
DDTS Number	**Corrected**	**Caveat**
CSCtc01871	Yes	Reports page returns error Steps to reproduce: 1. Generate around 80 Agent reports. 2. Go to **Device Management > Clean Access > Clean Access Agent > Reports**. 3. Display n either 10, 25, or 100 reports and click on the **Reports** tab. The Reports page displays a pop-up window with the following message: "SubmitOnEvent: can't find button or link 'reportsForm:filterButton'"
CSCtd20889	Yes	Provide a warning to clean up large distribution files from the database During an image upgrade, Cisco NAC Appliance should check the database for very large files and prompt the administrator to remove them prior to upgrade to avoid corrupting the database.
CSCtd61649	Yes	CAM DB fails to upgrade to 4.7(1) and may be lost with reports larger than 30K **Note** This issue only affects Cisco NAC Appliance users moving from their existing non-Cisco hardware platforms to the new next generation Cisco NAC-3315/3355/3395. If, before beginning the migration from release 4.1(8) to release 4.7(1), the Agent reports and/or event log stores are very large, administrators are not able to log in to the CAM GUI and (in some cases) data may be missing from the CAM database. **Workaround** To recover from this issue, administrators must re-image the affected appliance(s) to the original snap shot version, archive and then purge (delete) Agent reports and/or event logs, and re-apply the upgrade.
CSCtd76200	Yes	The following upgrade changes should implemented in Release 4.7(1) • Warn the administrator during the upgrade process if the file for a "File Distribution" requirement type in the CAM database exceeds 50MB. • Warn the administrator during the upgrade process if the maximum uploaded file size in the CAM database exceeds 50MB. (Although the CAM web console does not currently allow files greater than 10MB in size, files carried forward form older releases could possible exceed the 10MB threshold.)
CSCtd93159	Yes	Upgrade should pause when max file distribution > 50 and eject CD Upgrade should pause when the maximum file distribution file size is larger than 50MB is detected and the CD-ROM should automatically eject.

Resolved Caveats - Cisco NAC Agent Vers 4.7.1.511/Mac OS X Vers 4.7.1.506

Refer to Enhancements in Release 4.7(1), page 17 for additional information.

Table 12 List of Resolved Caveats (Sheet 1 of 2)

	Cisco NAC Agent Version 4.7.1.511/Mac OS X Version 4.7.1.506	
DDTS Number	**Corrected**	**Caveat**
CSCsz68781	Yes	Compliance Module needs to support JTrend VBcorp8.0 running on English MS Windows. The Cisco NAC Agent currently supports both Virus Buster Corporate Edition 8.0 and OfficeScan. However, the Agent cannot update Virus Definition files of Virus Buster Corporate Edition 8.0 running on an English Windows environment. **Note** There is no known workaround for this issue.
CSCta00073	Yes	Agent does not recognize Office Scan version 10 **Workaround** Use a custom check to verify installation and/or updates.
CSCta97156	Yes	Symantec/Norton 10.2 virus Def Date is not recognized on Mac OS X Symantec/Norton 10.2 virus definitions are not recognized correctly by the Mac OS X Agent. **Note** There is no known workaround for this issue.
CSCtb60168	Yes	Trend AV 8 not being recognized on 64-bit operating systems Client posture assessment fails when Trend AV 8 is installed on 64-bit operating systems. This issue has been observed when using 4.6.x.y Agent versions. **Workaround** Filter the clients or bypass the AV checks.
CSCtc36475	Yes	Java needs to be linked to browser for web applet to load The Java applet is required for OS detection, L3 (MAC & DHCP discovery), OOB or scenarios using the Web Agent. When Java applet is used for web login, it fails to load. This issue can happen if a user has installed Mozilla Firefox after having successfully used IE for Web Agent download previously. Upon installation, Firefox does not automatically link with the existing Java installation, and therefore cannot accommodate the Java Applet to install the Win Agent files on the client machine. **Workaround** If the user's browser has been installed after the Java installation, you can re-install Java to establish the link with the new browser.

Table 12 List of Resolved Caveats (Sheet 2 of 2)

	Cisco NAC Agent Version 4.7.1.511/Mac OS X Version 4.7.1.506	
DDTS Number	**Corrected**	**Caveat**
CSCtc77544	Yes	Incorrect multi-NIC behavior seen with Cisco NAC Agent version 4.7.1.511 on Windows 7 clients The deployment on which this situation has been observed includes a Windows 7 client connected via a wired NIC to an In-Band CAS and a wireless NIC connected to an Out-of-Band CAS. The following two issues are seen on Windows 7 and XP SP3 client machines: **Issue 1** (Set wireless as the preferred NIC over the wired NIC. Wireless and wired NIC both enabled.) The Agent pops up and the user is logged in through the wired NIC, despite specifying that the wireless NIC is "preferred." The client machine is listed in the CDL and In-Band OUL, however, the client has no network access and browser sessions are redirected to the default login page when the user tries to access the internet. No Agent pop up is seen following redirection. **Issue 2** (Set wireless as the preferred NIC over the wired NIC. Start with wireless NIC enabled and wired NIC disabled.) 1. The user logs in through the wireless NIC. Agent is logged in and user is given complete network access. 2. Now enable the wired NIC on the client machine. The Agent pops up via the wired NIC, but the user still has complete access to the internet, and when the user logs in via the wired NIC, they are listed in the CDL and In-Band OUL.
CSCtc79883	Yes	Mac OS X agent crash using VPN-SSO The Mac OS X Agent crashes during initial login when using VPN-SSO. This issue is not reproducible at every login, but has been observed more than once on multiple client machines. **Note** This issue has been observed on Intel 10.5 and 10.6 client machines switching between SSO and non-SSO as well as during Agent upgrade. **Workaround** Exit and re-launch the Agent to see if the situation resolves itself.
CSCtd47642	Yes	IP Refresh in OOB deployment fails on Macintosh 10.4 PowerPC IP Refresh on Macintosh OS 10.4 PowerPC client machines fails in OOB deployments. This issue is not reproducible on the Intel 10.4/10.5/10.6 version platforms. **Note** There is no known workaround for this issue.

New Installation of Release 4.7(1)

The following steps summarize how to perform new CD software installation of Release 4.7(1) on supported Cisco NAC Appliance hardware platforms (see Release 4.7(1) and Hardware Platform Support, page 3 for additional support details).

To upgrade on an existing Cisco NAC Appliance, refer to the instructions in Upgrading to Release 4.7(1), page 66.

Note The click in the NAC is configured with default settings like default priority, CPU usage etc. The driver loop of the click thread uses the full CPU whenever other processes are idle. The CPU usage of click can reach 99% . As the thread runs with default priority, other processes like tomcat can take over whenever requests come for them. The high CPU usage of click will not lead to any performance issues.

For New Installation:

With Release 4.7(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 NAC Appliance, 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 72.

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 Release 4.7(1) on each Clean Access Server and Clean Access Manager, as follows:

a. Log in to the Cisco Software Download Site at http://www.cisco.com/public/sw-center/index.shtml. You will likely be required to provide your CCO credentials.

b. Navigate to **Security > Endpoint Security > Cisco Network Access Control > Cisco NAC Appliance > Cisco NAC Appliance 4.7**.

c. Download the latest Release 4.7(1) .ISO image (e.g. **nac-4.7_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.

d. 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 Guide, Release 4.7*.

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 Configuration Guide, Release 4.7(2)*
- *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(2)*

Note As of Release 4.7(0), Cisco NAC Appliance no longer contains the "www.perfigo.com" Certificate Authority in the .ISO or upgrade image. Administrators requiring the "www.perfigo.com" CA in the network must manually import the CA from a local machine following installation or upgrade to Release 4.7(1).

In order to establish the initial secure communication channel between a CAM and CAS, you must import the root certificate from each appliance into the other appliance's trusted store so that the CAM can trust the CAS's certificate and vice-versa.

Note Clean Access Manager 4.7(1) is bundled with version 4.7.1.511 of the Cisco NAC Agent and version 4.7.1.506 of the Mac OS X Agent.

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 4.7(1)

Note To upgrade from Cisco NAC Appliance Release 4.1(8) or earlier to Release 4.7(1), you must first upgrade your system to Release 4.5(x), 4.6(1), or 4.7(0) and then upgrade to Release 4.7(1).

This section provides instructions for how to upgrade your existing supported Cisco NAC Appliance platform to Release 4.7(1). If you need to perform a new CD software installation, refer instead to New Installation of Release 4.7(1), page 65.

Refer to the following information prior to upgrade:

- Paths for Upgrading to Release 4.7(1)
- Changes for 4.7(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 4.7(1) release includes Cisco NAC Profiler Collector version 2.1.8-39 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 4.7(0) and Collector 3.1.0-24, and you upgrade to NAC 4.7(1), the Collector version will be downgraded to 2.1.8-39. Refer to the *Release Notes for Cisco NAC Profiler* for software compatibility matrixes and additional upgrade and product information.

Paths for Upgrading to Release 4.7(1)

Depending on the type of upgrade you are performing, use one of the following sets of guidelines to successfully upgrade your Cisco NAC Appliance release image, Cisco NAC Appliance hardware, or both:

- Upgrading from Customer-Supplied Hardware to Release 4.7(1) on a NAC-3310/3350/3390 Platform
- Upgrading an Existing NAC-3310/3350/3390 Platform to Release 4.7(1)
- Upgrading from a NAC-3310/3350/3390 Platform to Release 4.7(1) on a NAC-3315/3355/3395 Platform

Note If you are upgrading from an earlier Cisco NAC Appliance release on non-Cisco hardware to a next generation Cisco NAC-3315/2255/3395 platform, you must use the new Cisco Migration Utility available on CCO and follow the migration instructions in *Cisco NAC Appliance Migration Guide - Release 4.1(8) to Release 4.7(0)*.

Upgrading from Customer-Supplied Hardware to Release 4.7(1) on a NAC-3310/3350/3390 Platform

Note This procedure only applies to customers upgrading non-Cisco hardware to NAC-3310/3350/3390 platforms.

If you are running the Cisco NAC Appliance software (Release 4.1(x) or earlier) on a non-Cisco NAC Appliance platform, you must purchase Cisco NAC Appliance hardware before you can upgrade your system to Release 4.5(x) or later. You may additionally need to obtain proper FlexLM product licenses. Once you obtain your new Cisco NAC Appliance hardware, Cisco recommends that you:

Step 1 Create a backup snapshot for the current software version you are running (e.g. 4.1(x) or earlier).

Step 2 Download and install the same software version on your new Cisco NAC-3310/3350/3390 platform.

Step 3 Restore the snapshot to your new Cisco NAC Appliance.

Step 4 If necessary (depending on your existing release version), upgrade your appliance to 4.0(x) or 4.1(x) and *then* to Release 4.5(x), 4.6(1), or 4.7(0).

Note If you are upgrading 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 Release 4.7(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 before upgrading your production system.

Step 5 Follow the guidelines in Upgrade Instructions for Standalone Machines, page 74 or Upgrade Instructions for HA Pairs, page 77 (depending on your deployment) to upgrade Cisco NAC Appliance from Release 4.5(x), 4.6(1), or 4.7(0) to Release 4.7(1).

Step 6 Create a backup snapshot of your upgraded system.

Upgrading an Existing NAC-3310/3350/3390 Platform to Release 4.7(1)

Note This procedure only applies to customers upgrading their existing NAC-3310/3350/3390 platforms to Release 4.7(1).

The Release 4.7(1) .ISO installation/upgrade image only supports upgrade from Release 4.5(x), 4.6(1), and 4.7(0). If you are running an older software version (e.g. Release 4.1(8) or earlier), you must first upgrade your system to one of the supported base releases for Release 4.7(1) upgrade.

Step 1 Ensure you have upgraded to Release 4.5(x), 4.6(1), or 4.7(0) and create a backup snapshot for your system.

Step 2 Follow the guidelines in Upgrade Instructions for Standalone Machines, page 74 or Upgrade Instructions for HA Pairs, page 77 (depending on your deployment) to upgrade Cisco NAC Appliance from Release 4.5(x), 4.6(1), or 4.7(0) to Release 4.7(1).

Step 3 Create a backup snapshot of your upgraded system.

Upgrading from a NAC-3310/3350/3390 Platform to Release 4.7(1) on a NAC-3315/3355/3395 Platform

Note This procedure only applies to customers upgrading from NAC-3310/3350/3390 (non-FIPS) platforms to a next generation (NAC-3315/3355/3395) platform and assumes you are upgrading from Release 4.5(x), 4.6(1), or 4.7(0) to Release 4.7(1).

If you are running the Cisco NAC Appliance software (Release 4.1(x) or earlier) on a NAC-3310/3350/3390 platform and are planning to upgrade to next generation NAC-3315/3355/3395 hardware you must first upgrade your existing system to Release 4.5(x) or later before shifting to a new hardware platform. You may additionally need to obtain proper FlexLM product licenses for your new hardware before upgrading, as well. Once you obtain your next generation NAC-3315/3355/3395 hardware, Cisco recommends that you:

Step 1 Ensure you have upgraded to Release 4.7(0) and create a backup snapshot for your system.

Step 2 Download and install the same (Release 4.7(0)) software version on your new NAC-3315/3355/3395 platform.

Step 3 Restore the snapshot from your existing NAC-3310/3350/3390 to your new NAC-3315/3355/3395 hardware.

Step 4 Follow the guidelines in Upgrade Instructions for Standalone Machines, page 74 or Upgrade Instructions for HA Pairs, page 77 (depending on your deployment) to upgrade Cisco NAC Appliance from Release 4.7(0) to Release 4.7(1).

Step 5 Create a backup snapshot of your upgraded system.

Changes for 4.7(1) Installation/Upgrade

Cisco NAC Appliance Release 4.7(1) is an Early Deployment software maintenance release. 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 Release 4.7(1), note the following:

- Hardware Considerations
- Features That May Change With Upgrade
- Upgrade Changes

Hardware Considerations

- You can install Cisco NAC Appliance Release 4.7(1) on the following Cisco NAC Appliance platforms:
  - NAC-3315, NAC-3355, and NAC-3395 (FIPS or non-FIPS mode)

  Note Next generation Cisco NAC Appliance platforms (FIPS or non-FIPS Cisco NAC-3315, NAC-3355, NAC-3395) support fresh installation of Release 4.7(1) or upgrade from Release 4.7(0) to Release 4.7(1) only.

  - CCA-3140, NAC-3310, NAC-3350, and NAC-3390 (non-FIPS mode only)

  You cannot install any Cisco NAC Appliance release other than Release 4.7(0) or later on the NAC-3315, NAC-3355, and NAC-3395. and you cannot upgrade to or install Release 4.5 and later on any non-Cisco platform. See Hardware Support, page 3 for additional details.
- Cisco NAC Appliance Release 4.7(1) does not support the Cisco NAC Network Module (NME-NAC-K9). If you are currently using the Cisco NAC Network Module with a previous release of Cisco NAC Appliance in your network, do not upgrade to Release 4.7(1).
- With Release 4.7(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.
- To upgrade your CAM and CAS from Release 4.5(x), 4.6(1), or 4.7(0), insert the same Cisco NAC Appliance Release 4.7(1) installation CD-ROM (.ISO) into an existing Cisco NAC Appliance CAM or CAS and perform a “clean” or “graceful” shutdown and reboot for the system. The upgrade option

from the CD-ROM automatically prompts you to choose whether you want to do a fresh Install or Upgrade to Release 4.7(1). For more information, see Known Issues with Web Upgrade in Release 4.1(3), 4.1(6), and 4.1(8), page 82.

Warning **If you do not perform a "clean" or "graceful" shutdown (using the "shutdown -r now" command, for example) in the CAM/CAS CLI, the appliance does not present the upgrade option.**

- 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 Cisco NAC Appliance CAM/CAS Boot Settings.

Features That May Change With Upgrade

- If you employed any of the previous Windows registry settings to adjust Windows Clean Access Agent behavior on client machines, you must to specify the same settings in the XML Agent configuration file to preserve Agent behavior using the Cisco NAC Agent. For more information, see the "Cisco NAC Agent XML Configuration File Settings" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(2)*.
- 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 4.7(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 82.

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 To upgrade your CAM and CAS from Release 4.5(x), 4.6(1), or 4.7(0), insert the same Cisco NAC Appliance Release 4.7(1) installation CD-ROM (.ISO) into an existing Cisco NAC Appliance CAM or CAS and perform a "clean" or "graceful" shutdown and reboot for the system. The upgrade option from the CD-ROM automatically prompts you to choose whether you want to do a fresh Install or Upgrade to Release 4.7(1). For more information, see Known Issues with Web Upgrade in Release 4.1(3), 4.1(6), and 4.1(8), page 82.

- The Release 4.7(1) upgrade process now warns the administrator if the uploaded file for a "File Distribution" requirement type in the CAM database exceeds 50MB. If file size is too large, the upgrade process returns a warning to the administrator, aborts, ejects the Release 4.7(1) .ISO CD-ROM, and reboots the appliance. Before attempting to perform the upgrade again, the

administrator must manually purge "File Distribution" files larger than 50MB from the database using the CAM **Device Management > Clean Access > Clean Access Agent > Requirements > Requirement List** web console page, or move the uploaded file to a network server and create a "Link Distribution" requirement to replace the oversized "File Distribution" requirement. (This issue only affects the CAM, thus there are no changes in upgrade behavior on the CAS.)

- The Release 4.7(1) upgrade process now warns the administrator if the total compressed size of the CAM database cannot fit in available memory. If the compressed file size is too large, the upgrade process returns a warning to the administrator, aborts, ejects the Release 4.7(1) .ISO CD-ROM, and reboots the appliance. Before attempting to perform the upgrade again, the administrator must manually purge large files (like large collections of Agent Reports or Event Logs) from the CAM database. Before attempting to perform the upgrade again, the administrator must manually purge large database stores like Agent reports and Event Logs from the database using the CAM **Device Management > Clean Access > Clean Access Agent > Reports > Report Viewer** and **Monitoring > Event Logs > Log Viewer** web console pages, respectively. (This issue only affects the CAM, thus there are no changes in upgrade behavior on the CAS.)
- Cisco NAC Appliance Release 4.7(1) does not support the Cisco NAC Network Module (NME-NAC-K9). If you are currently using the Cisco NAC Network Module with a previous release of Cisco NAC Appliance in your network, do not upgrade to Release 4.7(1).
- The **NACAgentCFG.xml** Agent configuration XML file packaged with the Cisco NAC Agent is not preserved after upgrading from Release 4.6(1) to 4.7(1). You must manually re-import the Agent configuration XML file to maintain client machine login behavior.
- 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.
- 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 4.7(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.
- 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 4.7(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 4.7(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 4.7(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 4.5.2.0 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. For more information on Agent Stub installers and requirements/prerequisites, see the appropriate Release Notes for the specific previous version of Cisco NAC Appliance.
- 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 you upgrade the CAM to Release 4.7(1), the installation process automatically upgrades the Agent files to the latest Cisco NAC Agent version packaged with the CAM software image (e.g. Windows Cisco NAC Agent version 4.7.1.511, and Mac OS X Agent version 4.7.1.506).
- 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.
- Release 4.7(1) includes version 2.1.8-39 of the Cisco NAC Profiler Collector component that resides on the CAS installations. When upgrading CAS appliances (standalone or HA) to Release 4.7(1), the upgrade script will check the version of the Collector and only upgrade it if version 2.1.8-39 is not already installed. Refer to the *Release Notes for Cisco NAC Profiler* for software compatibility matrixes and additional upgrade and product information.

Note If currently running a Cisco NAC Profiler Server version other than 2.1.8-39, you will need to sync the Collector component version running on the NAC Server to the same version as the Profiler Server for compatibility.

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.

Note Cisco NAC Profiler and Cisco NAC Guest Server are not supported in FIPS-compliant deployments in Release 4.7(0).

General Preparation for Upgrade

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

- **Homogenous Clean Access Server Software Support**

You must upgrade your Clean Access Manager and all your Clean Access Servers concurrently. The Cisco NAC Appliance architecture is not designed for heterogeneous support (i.e., some Clean Access Servers running 4.7(1) software and some running 4.7(0), 4.6(1), or 4.5(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 Cisco NAC Appliance CAMs/CASs, and for any other server hardware platform that supports the BIOS redirection to serial port functionality.

- **Save a Local Copy of the Cisco NAC Agent Configuration XML File**

  The **NACAgentCFG.xml** Agent configuration XML file packaged with the Cisco NAC Agent is not preserved after upgrading from Release 4.6(1) to 4.7(1). You must manually re-import the Agent configuration XML file to maintain client machine login behavior.

  Note If you are upgrading from a Cisco NAC Appliance release older than Release 4.6(1), this upgrade preparation step does not apply.

- **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.

Warning **You cannot restore a CAM database from a snapshot created using a different release. For example, you cannot restore a 4.5(x), 4.6(1), or 4.7(0) database snapshot to a 4.7(1) CAM.**

- **Software Downgrade**

  Once you have upgraded your software to Release 4.7(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 4.7(1). See Upgrade Instructions for Standalone Machines, page 74 for additional details.

- **Passwords**

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

Upgrade Instructions for Standalone Machines

This section describes how to upgrade standalone (i.e. non-HA) CAM/CAS machines from Release 4.5(x), 4.6(1), or 4.7(0) to Release 4.7(1), and only applies to Cisco NAC-3310/3350/3390 or Cisco NAC-3315/3355/3395 platforms.

Note To upgrade from Cisco NAC Appliance Release 4.1(8) or earlier to Release 4.7(1), you must first upgrade your system to Release 4.5(x), 4.6(1), or 4.7(0) and then upgrade to Release 4.7(1).

To upgrade your CAM and CAS from Release 4.5(x), 4.6(1), or 4.7(0), insert the same Cisco NAC Appliance Release 4.7(1) installation CD-ROM (.ISO) into an existing Cisco NAC Appliance CAM or CAS and perform a “clean” or “graceful” shutdown and reboot for the system. The upgrade option from the CD-ROM automatically prompts you to choose whether you want to do a fresh Install or Upgrade to Release 4.7(1). For more information, see Upgrading to Release 4.7(1), page 66 and Known Issues with Web Upgrade in Release 4.1(3), 4.1(6), and 4.1(8), page 82.

Review Changes for 4.7(1) Installation/Upgrade, page 69 and General Preparation for Upgrade, page 72 before proceeding with these upgrade instructions.

Summary of Steps for Standalone Upgrade

The steps to upgrade standalone 4.5(x), 4.6(1), or 4.7(0) systems are as follows:

1. Create CAM DB Backup Snapshot, page 74
2. Download the Install/Upgrade File, page 75
3. Upgrade Your CAS, page 75
4. Upgrade Your CAM, page 76

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 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. **09_06_09-15-47_snapshot_VER_4_7_0.gz**).

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

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

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 Configuration Guide, Release 4.7(2)*.

Download the Install/Upgrade File

To upgrade your CAM and CAS from Release 4.5(x), 4.6(1), or 4.7(0), insert the same Cisco NAC Appliance Release 4.7(1) installation CD-ROM (.ISO) into an existing Cisco NAC Appliance CAM or CAS and perform a "clean" or "graceful" shutdown and reboot for the system. The upgrade option from the CD-ROM automatically prompts you to choose whether you want to do a fresh Install or Upgrade to Release 4.7(1). For more information, see Known Issues with Web Upgrade in Release 4.1(3), 4.1(6), and 4.1(8), page 82.

Step 1 Log in to the Cisco Software Download Site at http://www.cisco.com/public/sw-center/index.shtml. You will likely be required to provide your CCO credentials.

Step 2 Navigate to **Security > Endpoint Security > Cisco Network Access Control > Cisco NAC Appliance > Cisco NAC Appliance 4.7**.

Step 3 Download the latest Release 4.7(1) .ISO image, (e.g. **nac-4.7_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.

Upgrade Your CAS

Before upgrading your CAS be sure you obtain the Cisco NAC Appliance Release 4.7(1) install/upgrade image and burn it to a CD-ROM according to the instructions in Download the Install/Upgrade File, page 75.

Step 1 Insert the CD into the CD-ROM drive of each CAS you want to upgrade.

Step 2 Perform a "clean" or "graceful" shutdown on the CAS by logging into the CAS console CLI as "root" and entering `shutdown -r now`.

Warning **You must enter the "shutdown -r now" command in the CAM/CAS CLI to perform this upgrade. Simply power cycling the appliance does not bring up the upgrade option.**

Step 3 At the installation welcome ("boot:") prompt, press Enter.

Step 4 Choose option **2** at the following prompt:

```
Checking for existing installations.
Clean Access Server 4.7.0 installation detected.
Please choose one of the following actions:
1) Install.
2) Upgrade.
3) Exit.

2
```

Step 5 When upgrade is done, reboot the CAS at the prompt:

```
reboot
```

Step 6 In order to maintain a secure communication channel between a CAM and CAS, ensure the root certificate from each appliance appears in the other appliance's trusted store so that the CAS can trust the CAM's certificate and vice-versa.

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

Upgrade Your CAM

Note The Release 4.7(1) upgrade process now warns the administrator if the uploaded file for a "File Distribution" requirement type exceeds 50MB and/or the compressed size of the CAM database cannot fit in available memory during the upgrade. If file sizes are too large, the upgrade process returns a warning to the administrator, aborts, ejects the Release 4.7(1) .ISO CD-ROM, and reboots the appliance. For more information, see Upgrade Changes, page 70.

Before upgrading your CAM be sure you obtain the Cisco NAC Appliance Release 4.7(1) install/upgrade image and burn it to a CD-ROM according to the instructions in Download the Install/Upgrade File, page 75.

Step 1 Insert the CD into the CD-ROM drive of each CAM you want to upgrade.

Step 2 Perform a "clean" or "graceful" shutdown on the CAM by logging into the CAM console CLI as "root" and entering **shutdown -r now**.

Warning **You must enter the "shutdown -r now" command in the CAM/CAS CLI to perform this upgrade. Simply power cycling the appliance does not bring up the upgrade option.**

Step 3 At the installation welcome ("boot:") prompt, press Enter.

Step 4 Choose option **2** at the following prompt:

```
Checking for existing installations.
Clean Access Server 4.7.0 installation detected.
Please choose one of the following actions:
1) Install.
2) Upgrade.
3) Exit.

2
```

Step 5 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 4.7.1...done.
...Upgrading CCA files...done
Windows Agent version upgraded to 4.7.1.511.
Mac Agent was upgraded to version 4.7.1.506.
Clearing Tomcat cache...checking ssl configuration...done.
[root@cam1]#
```

Step 6 When upgrade is done, reboot the CAM at the prompt:

```
reboot
```

Step 7 In order to maintain a secure communication channel between a CAM and CAS, ensure the root certificate from each appliance appears in the other appliance's trusted store so that the CAM can trust the CAS's certificate and vice-versa.

Note The **NACAgentCFG.xml** Agent configuration XML file packaged with the Cisco NAC Agent is not preserved after upgrading from Release 4.6(1) or 4.7(1). You must manually re-import the Agent configuration XML file to maintain client machine login behavior.

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 4.5(x), 4.6(1), or 4.7(0) to Release 4.7(1), and only applies to Cisco NAC-3310/3350/3390 or Cisco NAC-3315/3355/3395 platforms.

If you have standalone CAM/CAS servers, refer instead to Upgrade Instructions for Standalone Machines, page 74.

Note To upgrade from Cisco NAC Appliance Release 4.1(8) or earlier to Release 4.7(1), you must first upgrade your system to Release 4.5(x), 4.6(1), or 4.7(0) and then upgrade to Release 4.7(1).

To upgrade your CAM and CAS from Release 4.5(x), 4.6(1), or 4.7(0), insert the same Cisco NAC Appliance Release 4.7(1) installation CD-ROM (.ISO) into an existing Cisco NAC Appliance CAM or CAS and perform a "clean" or "graceful" shutdown and reboot for the system. The upgrade option from

the CD-ROM automatically prompts you to choose whether you want to do a fresh Install or Upgrade to Release 4.7(1). For more information, see Known Issues with Web Upgrade in Release 4.1(3), 4.1(6), and 4.1(8), page 82.

Note To support FIPS 140-2 compliance, HA CAMs/CASs automatically establish an IPSec tunnel to ensure all communications between the HA pair appliances remains secure across the network.

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 Cisco NAC Appliance CAMs/CASs, and for any other server hardware platform that supports the BIOS redirection to serial port functionality.

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

Review Changes for 4.7(1) Installation/Upgrade, page 69 and General Preparation for Upgrade, page 72 before proceeding with these upgrade instructions.

Upgrading HA-CAM and HA-CAS Pairs

Note The Release 4.7(1) upgrade process now warns the administrator if the uploaded file for a "File Distribution" requirement type exceeds 50MB and/or the compressed size of the CAM database cannot fit in available memory during the upgrade. If file sizes are too large, the upgrade process returns a warning to the administrator, aborts, ejects the Release 4.7(1) .ISO CD-ROM, and reboots the appliance. For more information, see Upgrade Changes, page 70.

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.**

Step 1 Before upgrading your CAM/CAS HA pair, be sure you obtain the Cisco NAC Appliance Release 4.7(1) install/upgrade image and burn it to a CD-ROM according to the instructions in Download the Install/Upgrade File, page 75.

Step 2 Determine the failover state on each machine by running the **fostate.sh** command on each CAM/CAS in the HA pair:

```
/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 Configuration Guide, Release 4.7(2)* and the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(2)*.
- 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 3 Shut down the standby CAM/CAS.

Step 4 Insert the install/upgrade CD into the active CAM/CAS you want to upgrade.

Step 5 Perform a “clean” or “graceful” shutdown on the active CAM/CAS by entering **`shutdown -r now`**.

Warning **You must enter the “shutdown -r now” command in the CAM/CAS CLI to perform this upgrade. Simply power cycling the appliance does not bring up the upgrade option.**

Step 6 At the installation welcome (“boot:”) prompt, press Enter.

Step 7 Choose option **`2`** at the following prompt:

```
Checking for existing installations.
Clean Access Server 4.7.0 installation detected.
Please choose one of the following actions:
1) Install.
2) Upgrade.
3) Exit.

2
```

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 4.7.1...done.
...Upgrading CCA files...done
Windows Agent version upgraded to 4.7.1.511.
Mac Agent was upgraded to version 4.7.1.506.
Clearing Tomcat cache...checking ssl configuration...done.
[root@cam1]#
```

Step 9 After the upgrade is complete, shut down the active CAM/CAS.

Step 10 Insert the install/upgrade CD into the standby CAM/CAS you want to upgrade.

Step 11 Perform a “clean” or “graceful” shutdown on the standby CAM/CAS by entering **`shutdown -r now`**.

Warning **You must enter the "shutdown -r now" command in the CAM/CAS CLI to perform this upgrade. Simply power cycling the appliance does not bring up the upgrade option.**

Step 12 At the installation welcome ("boot:") prompt, press Enter.

Step 13 Choose option **2** at the following prompt:

```
Checking for existing installations.
Clean Access Server 4.7.0 installation detected.
Please choose one of the following actions:
1) Install.
2) Upgrade.
3) Exit.

2
```

Step 14 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 4.7.1...done.
...Upgrading CCA files...done
Windows Agent version upgraded to 4.7.1.511.
Mac Agent was upgraded to version 4.7.1.506.
Clearing Tomcat cache...checking ssl configuration...done.
[root@cam1]#
```

Step 15 After the upgrade is complete, shut down the standby appliance.

Step 16 Reboot the active appliance and wait until it is running normally and you are able to connect to the web console.

Step 17 Reboot the standby appliance and when it is up and running normally, verify connectivity between the CAMs/CASs.

Note The **NACAgentCFG.xml** Agent configuration XML file packaged with the Cisco NAC Agent is not preserved after upgrading from Release 4.6(1) to 4.7(1). You must manually re-import the Agent configuration XML file to maintain client machine login behavior.

Step 18 Verify the failover state on each machine again with the **fostate.sh** command on each machine:

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

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 Enabling Web Login for Windows 7 Starter Edition Clients

The Cisco NAC Agent and Cisco NAC Web Agent do not support Windows 7 Starter Edition. Client machines with the Windows 7 Starter Edition operating system can only perform web login to verify user credentials. The solution to simultaneously provide Cisco NAC Appliance support for web login on Windows 7 Starter Edition client machines as well as Agent login for other Windows operating systems requires the administrator to add a web login page that classifies Windows 7 Starter Edition in a "WINDOWS_ALL" operating system context. To enable web login functions for client machines running Windows 7 Starter Edition:

- Users must perform web login using Internet Explorer version 8.0 with ActiveX only (Java Applet is not supported)
- The Cisco NAC Appliance administrator must use the CAM **Administration > User Pages > Login Page** web console page to create a login page for the "WINDOWS_ALL" operating system that:
  - Requires the "ActiveX Only" Web Client setting
  - Enables the "Use web client to detect MAC address and Operating System" option to appropriately reflect the Windows 7 Starter Edition operating system on the client machine

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) and later, 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 39.

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(3), 4.1(6), and 4.1(8)

In Cisco NAC Appliance Release 4.7(1), web upgrade is no longer supported and cannot be used to upgrade Cisco NAC Appliances on Release 4.1(3) and later. To upgrade your Cisco NAC Appliances from Release 4.1(3) and later, you must run the upgrade script via the in-place Install/Upgrade CD method, as described in Upgrading to Release 4.7(1), page 66.

Note To upgrade from Cisco NAC Appliance Release 4.1(8) or earlier to Release 4.7(1), you must first upgrade your system to Release 4.5(x), 4.6(1), or 4.7(0) and then upgrade to Release 4.7(1).

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 Cisco NAC Appliance CAM/CAS Boot Settings

When performing CD software installation, if a Cisco NAC Appliance CAM/CAS 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 the Cisco NAC Appliance CAM/CAS" section of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.7*.

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 Configuration Guide, Release 4.7(2)*.

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.

Troubleshooting

This section provides troubleshooting information for the following topics:

Note For additional troubleshooting information, see also New Installation of Release 4.7(1), page 65.

Enabling TLSv1 on Internet Explorer Version 6

Cisco NAC Appliance network administrators managing the CAM/CAS via web console *and* client machine browsers accessing a FIPS-compliant Cisco NAC Appliance Release 4.7(0) network require TLSv1 in order to "talk" to the network, which is disabled by default in Microsoft Internet Explorer Version 6.

To locate and enable this setting in IE version 6:

Step 1 Got to **Tools > Internet Options**.

Step 2 Select the **Advanced** tab.

Step 3 Scroll down to locate the **Use TLS 1.0** option under **Security**.

Step 4 Click on the checkbox to enable the **Use TLS 1.0**. option and click **Apply**.

Step 5 If necessary, close the browser and open a new one where the TLS 1.0 option should now be automatically enabled.

Note This option is enabled by default in Microsoft Internet Explorer versions 7 and 8 and Mozilla Firefox has not shown this limitation.

Windows Vista and Windows 7—IE 7 and IE 8 Certificate Revocation List

Note In Internet Explorer versions 7 and 8, the "Check for server certificate revocation (requires restart)" checkbox is enabled **by default** under IE's Tools > Internet Options > Advanced | Security settings.

In Release 4.6(1) and later, you can use the "AllowCRLChecks" attribute in the **NACAgentCFG.xml** file to turn off Certificate Revocation List (CRL) checking for the Cisco NAC Agent during discovery and negotiation with the CAS. For details, see the "Cisco NAC Agent XML Configuration File Settings" section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(2)*.

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 version 7 or 8 and/or the Windows Vista or Windows 7 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 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 this issue, 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, 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.

HA Active-Active Situation Due to Expired SSL Certificates

HA communication for both HA-CAMs and HA-CASs is handled over IPSec tunnels to secure all communications between the two HA pair appliances. This IPSec tunnel is negotiated based on the SSL certificates uploaded to the HA pairs for both CAM and CAS. In case the SSL certificates are not trusted by the two HA peers, have expired, or are no longer valid, the HA heartbeat communication between the two HA pairs breaks down, leading both HA pair appliances to assume the Active HA-Primary) role.

For CASs deployed in VGW mode, this can potentially create a Layer 2 loop that could bring down the network. HA-CAMs with expired or invalid SSL certificates could lead to an Active-Active situation where the database is not synced between the two HA-CAM appliances. Eventually, this situation leads to the CAMs losing all recent configuration changes and/or all recent user login information following an HA-CAM failover event.

As HA communication over IPSec tunnels requires valid SSL certificates on both the CAM and CAS, the CAM-CAS communication also breaks down if the SSL certificate expires on either the CAM or CAS. This situation leads to end user authentications failures and the CAS reverting to fallback mode per CAS configuration.

Administrators can minimize HA appliance Active-Active situations due to expired SSL certificates by using SSL certificates with longer validity periods and/or using serial port connection (if available and not used to control another CAM or CAS) for HA heartbeat. However, when you configure HA-CAMs to perform heartbeat functions over the serial link and the primary eth1 interface fails because of SSL certificate expiration, the CAM returns a database error indicating that it cannot sync with its HA peer and the administrator receives a "WARNING! Closed connections to peer [standby IP] database! Please restart peer node to bring databases in sync!!" error message in the CAM web console.

Note Starting with Cisco NAC Appliance Release 4.7(0), the CAM or CAS generates event log messages to indicate the certificate expiry in addition to the message displayed in the CAM/CAS web console.

Note The self-signed SSL certificate expires after 90 days from the date of generation.

Agent AV/AS Rule Troubleshooting

When troubleshooting AV/AS Rules:

- View administrator reports for the 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 Agent (see Determining the Software Version, page 16).
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 87.
9. If necessary, provide CAM support logs as described in Creating CAM/CAS Support Logs, page 89.

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:

- Generate Cisco NAC Agent Debug Logs
- Cisco NAC Web Agent Logs
- Generate Mac OS X Agent Debug Log

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

Generate Cisco NAC Agent Debug Logs

To generate Cisco NAC Agent logs using the Cisco Log Packager utility, refer to the “Create Agent Log Files Using the Cisco Log Packager” section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(2)*.

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 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 exiting value with one of the following:

- **Info**—Include only informational messages in the event log
- **Warn**—Include informational and warning messages in the event log
- **Error**—Include informational, warning, and error messages in the event log
- **Debug**—Include all Agent messages (including informational, warning, and error) in the event log

Note The **Info** and **Warn** entry types only feature a few messages pertaining to very specific Agent 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/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 Configuration Guide, Release 4.7(2)* or *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(2)*.

Recovering Root Password for CAM/CAS

Refer to the "Password Recovery" chapter of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.7*.

Troubleshooting CAM/CAS Certificate Issues

Refer to the "Troubleshooting Certificate Issues" sections of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(2)* or *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(2)*.

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

Documentation Updates

Table 13 Updates to Release Notes for Cisco NAC Appliance, Release 4.7(1)

Date	Description
9/28/11	Added HA Active-Active Situation Due to Expired SSL Certificates, page 86
6/2/11	Added CSCtj81255 to Open Caveats - Release 4.7(1), page 24

Table 13 Updates to Release Notes for Cisco NAC Appliance, Release 4.7(1)

Date	Description
6/17/10	Added Caveat CSCsx52263 to Open Caveats - Release 4.7(1), page 24
5/17/10	Restricted information to Release 4.7(1) content only. Refer to http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html for all Release 4.7(x) release notes.
12/21/09	• Added CSCtd93159 to Resolved Caveats - Release 4.7(1), page 59 • Moved CSCtd61649 to Resolved Caveats - Release 4.7(1), page 59 • Updated Upgrade Changes, page 70 • Updated Upgrade Your CAM, page 76 • Updated Upgrading HA-CAM and HA-CAS Pairs, page 78
12/16/09	• Added Known Issue with Enabling Web Login for Windows 7 Starter Edition Clients, page 81 • Updated notes in Cisco NAC Windows Agent Version 4.7.1.511, page 17 and Cisco NAC Web Agent Version 4.7.1.504, page 18 to clarify Windows 7 Starter Edition support message • Added CSCtd61649 to Open Caveats - Release 4.7(1), page 24
11/25/09	• Added CSCtd20889 to Resolved Caveats - Release 4.7(1), page 59 • Added CSCtd47642 to Resolved Caveats - Cisco NAC Agent Vers 4.7.1.511/Mac OS X Vers 4.7.1.506, page 63
11/24/09	Release 4.7(1) • Updated Software Compatibility, page 12 • Added Enhancements in Release 4.7(1), page 17 • Updated Cisco NAC Appliance Supported AV/AS Product Lists, page 19 • Updated Open Caveats - Release 4.7(1), page 24 • Added Resolved Caveats - Release 4.7(1), page 59 and Resolved Caveats - Cisco NAC Agent Vers 4.7.1.511/Mac OS X Vers 4.7.1.506, page 63 • Updated Upgrading to Release 4.7(1), page 66 • Added Paths for Upgrading to Release 4.7(1), page 67

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

- *Cisco NAC Appliance Hardware Installation Guide, Release 4.7*
- *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.7(2)*
- *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.7(2)*
- *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*
- *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.