Release Notes for Cisco NAC Appliance, Version 4.9(4)

Document Number OL-31231-01 Revised: February 9, 2014

Contents

These release notes provide the latest cumulative release information for Cisco® NAC Appliance, Release 4.9(4). This document describes new features, changes to existing features, limitations and restrictions (“caveats”), upgrade instructions, and related information. These release notes supplement the Cisco NAC Appliance documentation included with the distribution. Read these release notes carefully and refer to the upgrade instructions prior to installing the software.

Cisco Systems, Inc.
www.cisco.com

Cisco NAC Appliance Releases

Cisco NAC Appliance Version	Availability
4.9(4) ED	February 6, 2014

Note Cisco recommends you deploy Cisco NAC Appliance Release 4.9(4) 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 NAC-3415 and NAC-3495 platforms you need get Standalone license for standalone systems and Failover license for HA-pairs.

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 4.9(4) and Hardware Platform Support

FIPS Compliant

You can install or upgrade to Cisco NAC Appliance Release 4.9 on the following FIPS-compliant Cisco NAC Appliance platforms:

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

Note Release 4.9 and 4.8 are the only certified FIPS-compliant Cisco NAC Appliance releases.

Note Cisco NAC Appliance platforms (FIPS or non-FIPS Cisco NAC-3315, NAC-3355, NAC-3395) support fresh installation of Release 4.9(4) or upgrade from Release 4.9(x) or 4.8(x) to Release 4.9(4) only.

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.

Non-FIPS

You can install or upgrade to Cisco NAC Appliance Release 4.9(4) on the following Cisco NAC Appliance platforms:

- NAC-3415, NAC-3495
- NAC-3315, NAC-3355, and NAC-3395

Additionally, Cisco NAC Appliance Release 4.9(4) 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.
- The installation/upgrade CD does not execute if attempting to launch it on a non-supported platform. Refer to Changes for 4.9(4) Upgrade, page 56 for additional details.
- Legacy customers on non-appliance platforms who wish to upgrade to Release 4.9(4) will need to purchase a supported platform to install the Release 4.9(4) software. Refer to Migrating from a NAC-3310/3350/3390 Platform to Release 4.9(4) on a NAC-3315/3355/3395 Platform, page 55 for additional details.

See also Supported AV/AS Product List Enhancements, page 15 for additional information.

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

Release 4.9(4) and Cisco NAC Profiler

All Cisco NAC Appliance releases are shipped with a default version of the Cisco NAC Profiler Collector component. Cisco NAC Appliance 4.9(4) release is shipped with Collector version 3.1.0.24 by default. When upgrading the NAC Server 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 4.8 and Collector 3.1.1, and you upgrade to NAC 4.9(4), the Collector version will be downgraded to 3.1.0.24. You need to manually upgrade the 3.1.0.24 Collector to 3.1.1 again and configure it after the NAC Server upgrade.

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

Note Cisco NAC Profiler and Cisco NAC Guest Server are not supported in FIPS-compliant deployments in Release 4.9 and 4.8.

Configuring AD SSO

If there are multiple AD domain controllers and the CAM/CAS are upgraded to the release (not fresh install), perform the following on the CAM.

Step 1 Navigate to **/perfigo/control/bin/starttomcat**.

Step 2 Search for **CATALINA_OPTS**.

Step 3 Add **-DRMI_READ_TIME_OUT=180000** at the end of CATALINA_OPTS.

Note The above resets the parameter to 3 minutes. This parameter is dependent on the number of domain controllers.

Step 4 Restart the CAM by entering the **service perfigo stop** and **service perfigo start** commands.

Note If you are applying this change to an existing HA pair, you must perform the above update on both the HA-Primary and HA-Secondary CAM just as you would upgrade a pair of HA-enabled CAMs.

FIPS 140-2 Compliance

Note Release 4.9, 4.8 and 4.7(0) are the only certified FIPS-compliant Cisco NAC Appliance releases.

This section describes the following topics:

Overview

Cisco NAC Appliance Release 4.7(0) introduced 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. Release 4.9 and 4.8 now also offer a field-replaceable FIPS card upgrade for Cisco NAC-3310, NAC-3350, and NAC-3390 platforms. In order to provide FIPS compliance in your Cisco NAC Appliance network, both CAM(s) and CAS(s) must be FIPS compliant.

Note Cisco NAC Profiler and Cisco NAC Guest Server are not supported in FIPS-compliant deployments in Release 4.9, 4.8 and Release 4.7(0).

To enable FIPS 140-2 compliance in Cisco NAC Appliance, CAMs and CASs must have an encryption card that handles the primary FIPS "level 2" compliance functions and manages private keys for the system.

In Release 4.9, 4.8 and 4.7(0), if the FIPS card in a Cisco NAC-3315/3355/3395 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 4.9(4) 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.

In addition, in order to ensure FIPS compliance across the entire Cisco NAC Appliance network, users must use the latest Cisco NAC Agent version 4.9.0.33, 4.8.0.35 or 4.7.1.15 on client machines connecting to the Cisco NAC Appliance network. Although Cisco NAC Appliance Releases 4.9, 4.8 and 4.7(0) support other Cisco NAC Appliance Agent versions, users logging in with a different version of the Agent are not FIPS compliant. For more information on the latest Cisco NAC Agent, see Cisco NAC Windows Agent Version 4.9.4.3, page 14.

Note Cisco NAC Appliance network administrators managing the CAM/CAS via web console *and* client machine browsers accessing a FIPS-compliant Cisco NAC Appliance Releases 4.9, 4.8 and 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 79.

Capabilities, Dependencies, and Restrictions

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

1. Key management in Release 4.9, 4.8, and 4.7(0) is different than in non-FIPS Releases. 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 or Windows 7 operating systems 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.
12. NTP server authentication—The CAM and CAS both use MD5 authentication to verify and authenticate Network Time Protocol (NTP) servers in Cisco NAC Appliance Releases 4.9, 4.8, and 4.7(0). MD5 is not a FIPS 140-2 compliant protocol, therefore you must disable the NTP authentication feature in Cisco NAC Appliance to ensure your network remains FIPS compliant.

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

In Cisco NAC Appliance Releases 4.9, 4.8, and 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 in Cisco NAC Appliance Releases 4.9, 4.8, and 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 Releases 4.9, 4.8, and 4.7(0).

IPSec Considerations with FIPS

Cisco NAC Appliance Releases 4.9, 4.8, and 4.7(0) use 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 (Adaptive Security Appliance)-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 Releases 4.9, 4.8, and 4.7(0) provide 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 4.9(x)*.

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 4.9(x)*.

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 or Windows 7 with Cisco NAC Agent version 4.9.0.33, 4.8.0.35, or 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 4.9(x)*.

You cannot perform AD SSO in a FIPS-compliant network using Cisco Wireless LAN Controllers because the 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.

Supported Switches for Cisco NAC Appliance

See *Cisco NAC Appliance Switch and Wireless LAN Controller Support* for complete details on:

- Cisco switch models and Wireless LAN Controllers supported in a Cisco NAC Appliance Wireless OOB environment
- All switch models 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 1 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 1 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 5500 Series Wireless LAN Controllers	N/A
	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 73.
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 4.9(x)* and the *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

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* 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 4.9(4) CAM/CAS Upgrade Compatibility Matrix
- Release 4.9(4) CAM/CAS/Agent Compatibility Matrix
- Release 4.9(4) Agent Upgrade Compatibility Matrix
- Cisco NAC Agent Interoperability Between NAC Appliance and Identity Services Engine (ISE)

Release 4.9(4) CAM/CAS Upgrade Compatibility Matrix

Table 2 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 2 Release 4.9(4) CAM/CAS Upgrade Compatibility Matrix

Clean Access Manager [1]		Clean Access Server [1, 2]	
Upgrade From:	**To:**	**Upgrade From:**	**To:**
4.9(x) 4.8(x)	4.9(4)	4.9(x) 4.8(x)	4.9(4)

1. Cisco NAC Appliance platforms (FIPS or non-FIPS Cisco NAC-3315, NAC-3355, NAC-3395) support fresh installation of Release 4.9(4) or upgrade from Release 4.9(x) or 4.8(x) to Release 4.9(4) only. See Hardware Support, page 3 and Changes for 4.9(4) Upgrade, page 56 for additional details.
2. The Clean Access Server is shipped with a default version of the Cisco NAC Profiler Collector. See Release 4.9(4) and Cisco NAC Profiler, page 4 for details.

Release 4.9(4) CAM/CAS/Agent Compatibility Matrix

Table 3 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 3.

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 3 Release 4.9(4) 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**
FIPS 140-2 Compliant [4]				
4.9 4.8	4.9 4.8	4.9.0.33 4.8.0.35	N/A	N/A

Table 3 Release 4.9(4) CAM/CAS/Agent Compatibility Matrix (continued)

Clean Access Manager [1, 2]	Clean Access Server [1, 2]	Cisco NAC Appliance Agents [3]		
		Windows	Mac OS X	Web Agent
English-Only Server		**English-Only Agent**		
4.9(4)	4.9(4)	4.9.4.3 4.9.3.5 4.9.2.8 4.9.1.6 4.9.0.33 4.8.3.1 4.8.2.1 4.8.1.5 4.8.0.35	4.9.4.3 4.9.3.803 4.9.2.703 4.9.1.684 4.9.0.649 4.8.3.594 4.8.2.591 4.8.1.584 4.8.0.569	4.9.4.3

1. Cisco NAC Appliance platforms (FIPS or non-FIPS Cisco NAC-3315, NAC-3355, NAC-3395) support fresh installation of Release 4.9(4) or upgrade from Release 4.9(x) or 4.8(x) to Release 4.9(4) only. See Hardware Support, page 3 and Changes for 4.9(4) Upgrade, page 56 for additional details.
2. Make sure that both CAM and CAS are of same version.
3. See Enhancements in Release 4.9(4), page 14 for details on each version of the Windows/Mac OS X/Web Agents.
4. Release 4.9 and 4.8 are the only certified FIPS-compliant Cisco NAC Appliance releases.

Release 4.9(4) Agent Upgrade Compatibility Matrix

Table 4 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 4 Release 4.9(4) Agent Upgrade Compatibility Matrix

Clean Access Manager [1]	Clean Access Server [1]	Cisco NAC Appliance Agent [2]			
		Upgrade From Cisco NAC Windows Agent:	To Latest Compatible Cisco NAC Windows Agent:	Upgrade From Cisco Mac OS X Agent	To Latest Compatible Mac OS X Agent
4.9(4)	4.9(4)	4.9.3.5 4.9.2.8 4.9.1.6 4.9.0.33 4.8.3.1 4.8.2.1 4.8.1.5 4.8.0.35 [3,4]	4.9.4.3	4.9.3.803 4.9.2.703 4.9.1.684 4.9.0.649 4.8.3.594 4.8.2.591 4.8.1.584 4.8.0.569	4.9.4.3

1. Cisco NAC Appliance platforms (FIPS or non-FIPS Cisco NAC-3315, NAC-3355, NAC-3395) support fresh installation of Release 4.9(4) or upgrade from Release 4.9(x) or 4.8(x) to Release 4.9(4) only. See Hardware Support, page 3 and Changes for 4.9(4) Upgrade, page 56 for additional details.
2. See Enhancements in Release 4.9(4), page 14 for details on each version of the Windows/Mac OS X/Web Agent.
3. 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.
4. To remain FIPS-compliant, users logging into Cisco NAC Appliance via AD SSO must run Windows Vista or Windows 7 and have Cisco NAC Agent version 4.9.0.33 or 4.8.0.35 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.

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**
- CAM web console: **Monitoring > Reporting > System Summary**

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 X, 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**

Cisco NAC Agent Interoperability Between NAC Appliance and Identity Services Engine (ISE)

Cisco supports different versions of the NAC Agent for integration with NAC Appliance. NAC Agent versions 4.9 and later are supported for integration with Cisco ISE.

Starting from Cisco NAC Appliance Release 4.9(4), the NAC Agent versions 4.9.4.3 can be used on Cisco ISE Release 1.2. Refer to *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later* for more information on the latest Agent versions.

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 4.9(4)

Cisco NAC Windows Agent Version 4.9.4.3

Cisco NAC Appliance Release 4.9(4)4.9(4) introduces Cisco NAC Agent version 4.9.4.3.

Refer to Release 4.9(4) CAM/CAS/Agent Compatibility Matrix, page 11 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 4.9(x)*.

Mac OS X Agent Version 4.9.4.3

Cisco NAC Appliance Release 4.9(4) introduces Mac OS X Agent version 4.9.4.3. Refer to Release 4.9(4) CAM/CAS/Agent Compatibility Matrix, page 11 for additional compatibility details.

Cisco Mac OS X Agent version 4.9.4.3 provides updated AV/AS support capabilities on Macintosh client machines as described in Cisco NAC Appliance Supported AV/AS Products, page 15.

Cisco NAC Web Agent Version 4.9.4.3

Cisco NAC Appliance Release 4.9(4) introduces Cisco NAC Web Agent version 4.9.4.3.

For details on Agent functionality, refer to the "Cisco NAC Appliance Agents" chapter of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x)*.

Support for Microsoft Active Directory 2012

Cisco NAC Appliance Release 4.9(4) supports Microsoft Active Directory 2012 server with 2008/2008 R2 and 2012 functional levels.

Cisco NAC Appliance does not support Microsoft Active Directory 2012 server at 2003 functional level for ADSSO. See CSCuh81091, page 49.

Support for Windows 8.1

Cisco NAC Appliance Release 4.9(4) supports Microsoft Windows 8.1.

In a Windows 8.1 client, in the metro mode, the NAC Agent shortcuts are available in the Apps screen instead of the Start screen.

For a Windows 8.1 client machine, while configuring the user pages in CAM web console, if you have selected the web client as 'Java Applet Only' and enabled the 'Use web client to detect client MAC address and Operating System' option, then the client Operating System might be detected as Windows 8. While using Applet for Windows 8.1, configure the user page with WINDOWS_ALL. See Also CSCuj59700, page 49.

Support for Mac OS X 10.9

Cisco NAC Appliance Release 4.9(4) supports Mac OS X 10.9.

In Mac OS X 10.9 client, while using Safari 7.x for Web login, the Java applets would not be able to run the system commands. The applets work fine with Mozilla Firefox. See Also CSCuj17040, page 51.

Support for Catalyst 3850 Switches

Cisco NAC Appliance Release 4.9(4) supports Cisco Catalyst 3850 switches. For more information, refer to *Cisco NAC Appliance Switch and Wireless LAN Controller Support*.

Support for Cisco NAC Network Module Removed

In Cisco NAC Appliance Release 4.9(4), the support for Cisco NAC Network Module for Integrated Services Routers (NME-NAC-K9) has been removed.

Supported AV/AS Product List Enhancements

See Cisco NAC Appliance Supported AV/AS Products, page 15 for the latest AV/AS product charts.

Cisco NAC Appliance Supported AV/AS Products

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

For Windows AV/AS support information on the Cisco NAC Agent (version 4.9.4.3) and Cisco NAC Web Agent (version 4.9.4.3), see the *Cisco NAC Appliance Release 4.9(4) Supported Windows AV/AS Products* document optimized for UTF-8 character display.

Mac OS X

For Mac OS X AV/AS support information on the Cisco Mac OS X Agent (version 4.9.4.3), see the *Cisco NAC Appliance Release 4.9(4) Supported Mac OS X AV/AS Products* document optimized for UTF-8 character display.

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 4.9(x)* 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 4.9(4), page 14 for additional details on Agent versions in this release.

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://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

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

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

Open Caveats - Release 4.9(4)

Table 5 List of Open Caveats (Sheet 1 of 33)

	Software Release 4.9(4)	
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. **Workaround** Reboot the HA-Standby CAM or perform a HA-CAM failover to make the HA-Standby CAM become HA-Active.
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.)

Table 5 List of Open Caveats (Sheet 2 of 33)

DDTS Number	Software Release 4.9(4)	
	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 5 List of Open Caveats (Sheet 3 of 33)

	Software Release 4.9(4)	
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. **Workaround** You can click on the new item on the Windows status bar to bring the new dialog box or window in front of the Cisco NAC Web Agent Summary report. **Note** This problem only happens when a Google tool bar is installed and enabled in Internet Explorer.
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.
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 5 List of Open Caveats (Sheet 4 of 33)

DDTS Number	Software Release 4.9(4)	
	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/Java applet fails to refresh the IP address on 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. **Note** 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 73.

Table 5 List of Open Caveats (Sheet 5 of 33)

	Software Release 4.9(4)	
DDTS Number	**Corrected**	**Caveat**
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. **Note** There is no known workaround for this issue.
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.

Table 5 List of Open Caveats (Sheet 6 of 33)

	Software Release 4.9(4)	
DDTS Number	**Corrected**	**Caveat**
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.
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.
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

Table 5 List of Open Caveats (Sheet 7 of 33)

	Software Release 4.9(4)	
DDTS Number	**Corrected**	**Caveat**
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.
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.

Table 5 List of Open Caveats (Sheet 8 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	Caveat
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.
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 5 List of Open Caveats (Sheet 9 of 33)

DDTS Number	Software Release 4.9(4)	
	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 5 List of Open Caveats (Sheet 10 of 33)

DDTS Number	Software Release 4.9(4)	
	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.
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
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 70.

Table 5 List of Open Caveats (Sheet 11 of 33)

	Software Release 4.9(4)	
DDTS Number	**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 5 List of Open Caveats (Sheet 12 of 33)

DDTS Number	Software Release 4.9(4) Corrected	Caveat
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.
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.
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.
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**.

Table 5 List of Open Caveats (Sheet 13 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	Caveat

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.
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.

Table 5 List of Open Caveats (Sheet 14 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	Caveat
CSCsz55538	No	IP refresh message shows up in L3OOBRIP with IP Un-numbered scenario When L3OOBRIP with IP un-numbered is configured, the IP refresh message shows up even if IP refresh does not happen. **Workaround** In the CAM web console, go to **Profiles > SNMP Receiver > Advanced Settings**. Enter "0" in the **DHCP Release Delay** and **DHCP Renew Delay** fields.
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.
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 5 List of Open Caveats (Sheet 15 of 33)

DDTS Number	Software Release 4.9(4)	
	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.
CSCta12544	No	Server communication error upon web and Agent login This issue can occur when a brand new Release 4.5 or later 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 HA pair and the new 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.
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 in a FIPS 140-2 compliant network, 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.

Table 5 List of Open Caveats (Sheet 16 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	**Caveat**
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.
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.
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.

Table 5 List of Open Caveats (Sheet 17 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	**Caveat**
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 5 List of Open Caveats (Sheet 18 of 33)

DDTS Number	Software Release 4.9(4) 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).
CSCtb44223	No	Mac OS X Agent gets presented with incorrect login page and providers The Mac OS X Agent is presented with providers from a configured "MAC_ALL" OS login page rather than the intended "MAC_OSX" login page. This issue has been observed on Mac OS X 10.4 and 10.5 running Agent version 4.6.0.3 in a Cisco NAC Appliance Release 4.6(1) deployment. **Workaround** Configure MAC_ALL page identically to MAC_OSX page.
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.

Table 5 List of Open Caveats (Sheet 19 of 33)

DDTS Number	Software Release 4.9(4)	
	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.
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**.
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** Use one of the following options: • Stop and restart the Mac OS X Agent after installation. • Reboot the client machine. • Make the requirement optional (opens the network up to an old AV definition file version).
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.

Table 5 List of Open Caveats (Sheet 20 of 33)

DDTS Number	Software Release 4.9(4) Corrected	Caveat
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.
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 5 List of Open Caveats (Sheet 21 of 33)

	Software Release 4.9(4)	
DDTS Number	**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.
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.
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.

Table 5 List of Open Caveats (Sheet 22 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	Caveat
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.
CSCtc90964	No	Inaccuracy in AV/AS support info Latest Virus Definition version/date for Selected Vendor under AV/AS support info does not display the updated version/date for some AV/AS vendors.
CSCtc91616	No	Inconsistent support for Internationalized characters in usernames It is unclear if Internationalized characters are supported for uncommon user names in Cisco NAC Appliance. For example, some internationalized characters (like è) are allowed when creating a username on the CAM, but user login fails. Other character sets (like Japanese) also 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. **Note** There is no known workaround for this issue.
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.
CSCte55522	No	The Cisco NAC Agent for Release 4.7(2) does not update ZoneAlarm 7.1.078.000 in Windows Vista Ultimate This particular update works in Windows Vista Ultimate SP0. **Workaround** The user can upgrade to ZoneAlarm Version 8 when running Windows Vista Ultimate SP1.
CSCte64337	No	Unexpected switch to UDP discovery mechanism There are unexpected SSM events found in the Agent log. These events are caused by unexpected switch to UDP discovery after SwissUdpExchange starts sending Swiss requests.

Table 5 List of Open Caveats (Sheet 23 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	**Caveat**
CSCte76636	No	L3 MAC unable to refresh on Vista (32-bit/64-bit) w/ UAC w/o port bounce Windows Vista users are not able to get an IP address from the DHCP pool for the access VLAN with web login or web agent. **Workaround** Run the browser (Internet Explorer or Firefox) as administrator.
CSCtf02702	No	After deleting and re-adding a CAS, the CAM web console displays that AD SSO is started This issue does not impact Cisco NAC Appliance functionality. After deleting and re-adding a CAS, the administrator must also reboot the CAS. Once you reboot the CAS (or perform "service perfigo restart"), everything works as designed. **Workaround** Restart the CAS to avoid this symptom appearing.
CSCtf69345	No	Agent reports incorrect update details for McAfee 8.7.0i on Win7 x64 NAC Agent reports incorrect McAfee virus definition update date and version, while McAfee shows the right date. This occurs because Windows registry is blocked with permissions issue and prevents McAfee from overwriting the appropriate date and version information to registry. **Workaround** Perform the following steps: 1. Uninstall McAfee. 2. Delete the following key and sub keys from registry: **HKEY_LOCAL_MACHINE\SOFTWARE\McAfee** 3. Re-install McAfee and confirm that the entry is recorded in the registry with proper details. 4. Perform updates in McAfee. 5. Verify that both NAC Agent and McAfee show the same dates and definition versions.
CSCtf99678	No	Enable OOB logoff msg for Windows not grayed out in Firefox browser The **Enable OOB logoff for Windows NAC Agent and Mac OS X Agent** checkbox is not grayed out in Mozilla Firefox version 3.5.8, even with the "Use 'WINDOWS_ALL' settings for this OS version" option checked. **Note** This issue appears in Mozilla Firefox and has not been observed in other browser types.

Table 5 List of Open Caveats (Sheet 24 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	Caveat
CSCtg01263	No	Invalid provider name seen between multi-NIC transition with OOB Logoff This problem is happening because while the role based (with IP refresh) wired NIC is transition from logged in, through IP refresh on logout, then the wireless NIC has the better metric so the wireless side responds, once the ip is refreshed on the wired side an invalid provider is seen and then wired login continues normally.
CSCtg06599	No	IP refresh on Win 7 after successful auth is very slow After a successful login, it takes 1-4 minutes for a machine to complete the IP refresh. This happens with Windows 7 and Vista machines moving from authentication to access networks (with an IP address change). This occurs because the Network Connectivity Status Indicator, which is part of the Network Location Awareness in Windows, tries to reach the **msftncsi.com** web page while performing IP refresh. If it is not able to reach this website, then Microsoft takes longer to sense the machine's status and results in slower applications that require internet access. For more information, see Known Issue with Delayed IP Address Refresh for Windows 7/Vista Clients Running Cisco NAC Agent, page 70.
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.
CSCtg45522	No	Delay in Agent logging out in Vista 64-bit Found that after authentication when click logout on a Vista 64bit machine, it takes a while before CAM receives the logout message and hence client takes a while to switch back from access to auth.
CSCtg45741	No	IP address release takes a while in Windows 7 32-bit using taskbar logout option IP release takes a long time to complete on Windows 7 32-bit clients for Cisco NAC Agent. As a result, the delay between release and renew is around 50sec.

Table 5 List of Open Caveats (Sheet 25 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	Caveat
CSCtg45753	No	Cisco NAC Agent won't pop-up with multi-NIC same metric /auth/discovery 404 This issue can occur when Agent runs on a client machine with two NICs using the same metric. (For example, the wired interface has NAC, while the wireless interface has no NAC.) **Note** This was observed on 100MB wired and 300MB wireless interfaces where the wireless speed signal dropped close to 100 resulting in two NICs with the same metric.
CSCtg57758	No	Error in Mac OS X Agent while editing Filters
CSCth61503	No	Duplicate kernel status message appears during CD installation The "Memory for crash kernel (0x0 to 0x0) not within permissible range" message appears twice in a row during CD installation.
CSCtg61995	No	Mac OS X Agent SWISS discovery back-off algorithm When Mac Agent is not connected to a NAC network, the Agent will never give up on trying to contact the last known CASes. It will continuously send UDP SWISS packet every ~17 seconds forever.
CSCtg69836	No	HTML Canned Report Missing AV gives blank report, but is ok for PDF
CSCtg65859	No	The Cisco NAC Agent is not able to logout in an OOB deployment Cisco NAC Appliance generates a "Rogue Client Agent Report" after the user performs web login and then launches the NAC Agent (or closes the NAC Agent dialog window if already launched), and then tries to log out using the NAC Agent in an OOB environment. **Workaround** Use the Cisco NAC Agent to log in to such networks.
CSCth17804	No	VPN SSO presents a blank Cisco NAC Agent login dialog Following a VPN disconnect, the client machine renegotiates for VPN to connect through the network and the user is presented with a blank Agent login dialog.
CSCth73774	No	McAfee Virus scan 14.0 remediation fails This issue has been observed during client remediation of McAfee VirusScan 14.0. **Workaround** Set McAfee to automatically update during the time the user is logged in. (The user can also manually update while logged in or while in the Agent Temporary role.)
CSCth85390	No	Certificate dialog appears multiple times when certificate is not valid **Workaround** Ensure valid certificates are available on the client machine.
CSCth88009	No	The Mac OS X Agent's **Popup Login Window** option does not work during SSO

Table 5 List of Open Caveats (Sheet 26 of 33)

DDTS Number	Software Release 4.9(4) Corrected	Caveat
CSCth98219	No	Agent appears when user is logged in via restricted network access role When a user logs into an Out-of-Band network and accepts Restricted network access after failing a mandatory requirement. the Cisco NAC Agent appears a second time (and continues to appear each time) when the user either logs in again without remediating, or closes the Agent login dialog. **Workaround** The Cisco NAC Appliance administrator can manually add text to the Restricted Access dialog box advising the user to iconize the Agent and must perform manual remediation. Once the user remediates the client machine, they can double-click the Agent icon and log in again.
CSCti35086	No	Disable Fast SSID change for NAC Wireless OOB setup Wireless clients without the Cisco NAC Agent installed can associate to a "guest" WLAN where NAC is not enabled. When FAST SSID Change is enabled globally on a Wireless LAN Controller, wireless clients (without the Cisco NAC Agent installed can then disassociate from the "guest" WLAN and immediately associate to the corporate WLAN (where NAC functionality is enabled), resulting in the client machine being placed directly into the network Access VLAN without being redirected to the Quarantine role. **Workaround** Disable the Fast SSID function on the Wireless LAN Controller.
CSCti03955	No	The Agent login dialog becomes unresponsive when the Temporary role timer runs out This situation can occur if the Temporary role timer expires during a long remediation like WSUS or AV/AS update. **Workaround** To avoid this issue, make sure the Temporary role timer is set to a value that will not expire during "worst case" remediations. **Note** If this problem occurs, users can clear the NAC Agent login dialog by selecting **Exit** from the Cisco NAC Agent systray icon or rebooting the client machine. If the user chooses to **Exit**, the user must also then manually launch the Cisco NAC Agent again.

Table 5 List of Open Caveats (Sheet 27 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	Caveat
CSCtj53399	No	Clean Access Server can bridge traffic in RIP mode There are intermittent issues in which traffic is bridged across a Clean Access Server in RIP mode. Despite being in routed mode, the CAS bridges traffic on the native VLAN, arriving to the CAS untagged. **Workaround** Explicitly configure the native VLAN on the switch interface connected to the CAS to a disabled / unused VLAN.
CSCtj65580	No	DHCP Requests Fail After Failover to Secondary CAM In HA setup, when DHCP is working failover to secondary, DHCP Requests are not sent or answered through CAS.
CSCtj81251	No	NAC Agent upgrade files missing on the CAS NAC Agent installation and upgrade files are deleted from the CAS when the User Interface is toggled from **Full UI** to **None** on the Clean Access Agent installation page from the CAM.
CSCtj81255	No	Two MAC addresses detected on neighboring 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.

Table 5 List of Open Caveats (Sheet 28 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	Caveat
CSCtl24190	No	Getting messages in CAS console when upgrading from 4.7.3 to 4.8.1 While upgrading NAC version 4.7(3) to 4.8(1), the following message is displayed in the CAS web console: "value missing in 'icmp type' directive" **Note** The upgrade happens successfully, and the messages can be ignored.
CSCth00256	No	Cert error seen on Mac Agent during login on multinic setup After importing self-signed certificate in the trusted Root CA on Mac OSX client machine, while logging in using wireless, a message pops up stating that the certificate is incorrect. **Workaround** When the Agent login fails for the first time and the Agent pops up again, try logging in again by entering user credentials and user should be able to login.
CSCtl59461	No	CAM shows old AV dates even with latest checks set Even if the CAM Updates are pulling down the latest Checks & Rules, the CAM still shows the latest definition dates for many vendors like AVG, Microsoft, McAfee, and Symantec **Workaround** Perform a clean update which deletes all Cisco checks and re-downloads all of them from the server. The Update number will be the same, but the correct dates will be stored in the CAM. To perform a clean update, in the CAM web console, navigate to **Device Management > Clean Access > Updates > Update** and click **Clean Update**.
CSCtl85558	No	Nessus scanning doesn't finish completely and doesn't generate logs When Nessus scanning is enabled for web-logins, the scan is not completed and no logs are generated in the NAC. **Workaround** Instead of Nessus scanning, web agent can be used.
CSCsy52241	No	Change host traffic control to allow different types of traffic Currently, traffic control host options only allow HTTP (ports 80 and 443) traffic. Need to allow other traffic, such as SMTP or FTP. **Workaround** Use the IP-based traffic control options.
CSCti25483	No	Request for option to customize the CAS redirection page.
CSCtj31886	No	Heartbeat to check for LDAP server connectivity During client authentication with LDAP server that is not responding, the CAM UI is not accessible.

Table 5 List of Open Caveats (Sheet 29 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	Caveat
CSCtr16957	No	Hub detection on CAT 6k switches blocks SNMP threads When using wireless OOB, L2 VGW, with AD SSO and Wireless SSO enabled, random NAC OOB authentication fails, when the user is moving from one floor to other. **Workaround** Force the client to re-authenticate on the WLC.
CSCts73863	No	Getting Error Messages for SSH while upgrading from 4.7.5 to 4.9.0 When CAS or CAM is upgraded from 4.7.5 to 4.9.0 and `/perfigo/common/bin/showstate.sh` is run to check the system conformity, open ssh library may be reported with incorrect version. **Note** This is a false warning, as open ssh already has the correct version. The message can be ignored.
CSCts80116	No	Compliance Module 3.4.27.1 causes memory leak on some PCs Clients that have version 8.2.0 of Avira AntiVir Premium or Personal may face excessive memory usage. **Workaround** Install later version of Avira AntiVir Premium or Personal.
CSCtu40313	No	Getting SNMPD service error when upgrading from 4.6.x > 4.8.x > 4.9.x While upgrading from 4.6(1) to 4.8(x) and then to 4.9, the following error message is displayed: "Stopping snmpd: [FAILED]" **Workaround** Restart the CAM after upgrading and it works fine. The error message can be ignored.
CSCtz21327	No	Install, un-install wizard for Polish, Czech languages The download file (update.exe) is installing the Agent in Czech language if language is Czech, but for Polish language, the Agent is installed in English.
CSCto45199	No	In Wired NAC network with IP change that is taking longer then normal, the message "Failed to obtain a valid network IP" is displayed. This message window does not close even after you click OK. **Workaround** Wait for the IP refresh to complete and network to stabilize in the background.
CSCtr28150	No	The server.error.5508 is translated incorrectly to hungarian locale.

Table 5 List of Open Caveats (Sheet 30 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	Caveat
CSCtx49261	No	When the ISR is cold-started with a NAC NME module in it running 4.9.0, the module eth0 interface becomes unresponsive. **Workaround** • Re-image the module OR • You can tweak the boot configuration and reboot the cas as follows: Enter '***' to change boot configuration: *** ServicesEngine Bootloader Version: 2.1.15.0 ServicesEngine boot-loader> reboot Rebooting !Ã¿Nmi Npx0 Dly P92 Sha0 Kbd0 Cmos Pci Dma0 PrtB Tim Exp Rfsh Geom
CSCty29608	No	SNMP monitoring does not work on 4.9 CAS in VGW mode. CAS is setup in a Virtual gateway mode and the native VLAN on the switch port connected to the Eth 0 interface of the CAS is set to a random VLAN. SNMP monitoring does not work on CAS running version 4.9. The Sever gets the requests, but it does not respond. **Workaround** Set the native VLAN on the Eth 0 interface to the management VLAN of the CAS.
CSCuc25238	No	In a Windows 8 Client machine, if Notifications for "NACToastNotification" application is turned OFF and then turned ON, then Toast Notifications will not be displayed immediately. **Workaround** Move to Desktop Mode at least once.
CSCue90040	No	NAC should recognize on board NIC cards as eth0 and eth1 regardless of NIC vendors.
CSCue89963	No	NAC should detect all available NICs in UCS hardware to set asONBOOT=yes, instead of booting only on board NIS as eth0 & eth1.

Table 5 List of Open Caveats (Sheet 31 of 33)

DDTS Number	Software Release 4.9(4) 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.
CSCts37221	No	Help Desk and Read-only users added in ISE are able to update endpoints When the admin users are assigned to the group "Help Desk" and "Read-only", and added to ISE, the endpoints created in ISE are getting added to the CAM Filter list. The Help Desk and Read-only users added in ISE under NAC Managers are able to update the endpoints. Only the Admin users under "Full Control Admin" should be able to add, edit, or delete the endpoints in CAM.
CSCuc74934	No	HSRP causes CAS to echo HSRP and multicast traffic When the CAS is connected to a switch running HSRP, it causes the CAS to echo all HSRP and other multicast traffic. This generates additional traffic and logging messages on the switch. **Workaround** Disable HSRP.
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.

Table 5 List of Open Caveats (Sheet 32 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	Caveat
CSCtx30981	No	Mac OS X Agent hangs awaiting posture report response from server. The issue occurs with Mac OS X 10.7.2 clients. **Workaround** Kill the CCAAgent Process and then start CCAAgent.app. Perform the following: 1. Go to Keychain Access. 2. Inspect the login Keychain for corrupted certificates, like certificates with the name "Unknown" or without any data 3. Delete any corrupted Certificates 4. From the pull-down menu, select Preferences and click the Certificates tab 5. Set OCSP and CRL to off.
CSCty51216	No	Upgrading Mac OS X Agent version 4.9.0.638 or 4.8.2.594 to later versions fails. **Workaround** 1. Remove the "CCAAgent" folder from temporary directory 2. Reboot the client 3. Connect to Web login page and install the Agent from there
CSCuh72873	No	Keep online user, change to Auth Vlan is removing the user from OUL. When **Keep Online Users option** is enabled, the **Change to Auth VLAN** option clears the OUL once the IP is refreshed from Auth VLAN in OOB RIP.
CSCuh75710	No	User summary graph is not populating in the Reporting page Under high login rate (20 logins per second), the weekly and monthly User Summary graphs are not displayed.
CSCuh74881	No	Delay of 6 minutes when launching Agent via Java applet using Java 7 Update 25 If Java 7 update 25 or above is installed, launching of Agents on clients would take about 6 minutes as this Java update has Perform revocation checks enabled by default. **Workaround** If you are using Java 7 update 25, make sure to turn off Perform certificate revocation checks in Java. Open Java Control Panel, click the **Advanced** tab, go to **Perform certificate revocation checks on** and select **Do not check**.

Table 5 List of Open Caveats (Sheet 33 of 33)

DDTS Number	Software Release 4.9(4)	
	Corrected	Caveat
CSCuj59700	No	For a Windows 8.1 client machine, while configuring the user pages in CAM web console, if you have selected the web client as 'Java Applet Only' and enabled the 'Use web client to detect client MAC address and Operating System' option, then the client Operating System might be detected as Windows 8. **Workaround** While using Applet for Windows 8.1, configure the user page with WINDOWS_ALL. This is applicable for all the browsers.
CSCul07861	No	NAC Agent not able to install from 4.9.3.x to 4.9.3.9 After uploading NAC Agent 4.9.3.9 through Agent Distribution option in CAM and enabling the Mandatory Upgrade option, NAC Agent prompts for upgrade. When the user clicks to upgrade, the NAC Agent Windows Installer shows the following error and the Agent is not installed: “Error opening installation log file. verify that the specified file location exists and is writable” **Workaround** Log off and log in to the Windows client and this resolves the issue.

Resolved Caveats - Release 4.9(4)

Refer to Enhancements in Release 4.9(4), page 14 for additional information.

Table 6 List of Resolved Caveats (Sheet 1 of 3)

DDTS Number	Software Release 4.9(4)	
	Corrected	Caveat
CSCtq74462	Yes	CAS cannot block CAM configuration update even if SSKEY mis-match occurs. When SSKEY mis-atch occurs between CAM and CAS, CAS should deny configuration updates from CAM. But CAS accepts the configuration updates from all CAMs, even if the CAM DB is not updated with the SSKEY. **Workaround** When the CAS configuration is updated with mismatched SSKEY, manually remove the CAM that is not updated with the right SSKEY.
CSCuh81091	Yes	NAC ADSSO - 2012 server with 2003 functional level is not supported The support for Microsoft Active Directory 2012 server at 2003 functional level for ADSSO has been addressed. Follow the configuration steps provided in the ‘Enable Additional Algorithms on Existing AD Servers’ section of *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x).*

Table 6 List of Resolved Caveats (Sheet 2 of 3)

	Software Release 4.9(4)	
DDTS Number	**Corrected**	**Caveat**
CSCtw47039	Yes	NAC Manager functionality to generate Uncontrolled ports report Enhancement to generate a cusotm report of Uncontrolled Ports.
CSCud17978	Yes	CAM displays negative hours for the user summary graph After upgrading to NAC Appliance Release 4.9(1), the user summary graph in the CAM GUI displays negative values in the Time axis.
CSCug22361	Yes	Custom Reports- Role Specific reports fields mismatch In the custom report for Role Specific Requirements, the Requirement Status and Login Status fields position in the table are interchanged.
CSCug74304	Yes	HA reporting tab does not report correct status of CAS HA In High Availability mode, in spite of both nodes communicating, the reporting tab does not reflect this and shows the peer node as down.
CSCug82141	Yes	Custom Reports not getting deleted When the Delete option is clicked to remove the custom reports from CAM GUI, the reports are not getting deleted.
CSCuh15403	Yes	SSKEY overwritten to unwanted value according to .GUSSK.old After upgrading to NAC Appliance release 4.9(x) from previous releases, the SSKEY value is stored in the .GUSSK and .GUSSK.old files. When the hardware is replaced, the SSKEY is reset and it is stored in the .GUSSK file. When the secondary CAS is rebooted, the SSKEY value changes to the old value stored in the .GUSSK.old file. **Workaround** • Remove /etc/.GUSSK.old [OR] • Modify sskey value in /etc/.GUSSK.old to match the right key.
CSCuh94210	Yes	SNMP community string on Secondary CAM in HA pair defaults to 'public' When the SNMP community string in the active CAM is updated while the standby machine is booting, the string is not reflected in the standby machine once it comes up.
CSCui04199	Yes	Windows 8.1 support in NAC server Enhancement to provide support for Windows 8.1.
CSCuj67086	Yes	Failed to add MAC,CAS combination into filter list For large deployments, some of the MAC and CAS combinations are not getting added to the filter list successfully.
CSCul62365	Yes	Windows 8.1 RT Tablets identified as Windows 8.1 desktops Windows 8.1 RT Tablet is identified as PC. This has been fixed.

Table 6 List of Resolved Caveats (Sheet 3 of 3)

	Software Release 4.9(4)	
DDTS Number	**Corrected**	**Caveat**
CSCui04248	Yes	Support for Windows 8 variants (media center packs) in NAC Server Support for Windows 8 variants (media center packs) has been added to NAC Server.
CSCui60009	Yes	Cisco catalyst 3850 switch support in CAM Support for Cisco catalyst 3850 switch has been added.
CSCuj17040	No	Web login fails to detect MAC address in Mac OS X 10.9 While using Safari 7.x for Web login, the Java applets are not able to run the system commands. The applets work fine with Mozilla Firefox. **Workaround** In Safari 7.x, whitelist the specific URLs to run the Java applets in unsafe mode. You can modify the preferences as follows: Go to **Preferences > Security > Website Settings > Java**, click the corresponding CAS URL and then click **Run in unsafe mode**. This enables the client to run the system commands using Java applet.
CSCuj71360	Yes	NAC installation failed on UCS with new series of seagate HDDs Installation of NAC fails on UCS shipped with new series of Seagate Hard Disk Drives and this has been fixed in Cisco NAC Appliance Release 4.9(4).
CSCum40163	Yes	Database causes upgrade failure from 4.8.2 to 4.9.x series While upgrading from 4.8(2) to 4.9(x), the upgrade script reports the database schema to be valid. After the upgrade is complete and showstate.sh is run, the database schema fails. This has been fixed in Cisco NAC Appliance Release 4.9(4).

Resolved Caveats - Cisco NAC Agent Vers 4.9.4.3/Mac OS X Vers 4.9.4.3

Refer to Enhancements in Release 4.9(4), page 14 for additional information.

Table 7 List of Resolved Caveats (Sheet 1 of 2)

	Cisco NAC Agent Version 4.9.4.3/Mac OS X Version 4.9.4.3	
DDTS Number	**Corrected**	**Caveat**
CSCuh21531	Yes	NAC Agent - Compliance module update fails every day
CSCuh64285	Yes	NAC Agent does not support Windows 8 with Media Center pack When trying to integrate with Windows 8 with Media Center pack, NAC Agent displays the following error: “Agent user operating system is not supported”. This happens with NAC Agent versions 4.9.0.x and 4.9.2.x. The issue has been resolved in NAC Agent versions 4.9.3.x and 4.9.4.3.

Table 7 List of Resolved Caveats (Sheet 2 of 2)

	Cisco NAC Agent Version 4.9.4.3/Mac OS X Version 4.9.4.3	
DDTS Number	**Corrected**	**Caveat**
CSCuh64358	Yes	Insufficient packages error on NAC agent with WSUS check In WSUS check, when attempting to validate posture, NAC Agents displays the following error: "Insufficient Clean Access Packages Installed" **Workaround** Disconnect and Reconnect the NAC Agent
CSCui42225	Yes	Add support for Windows 8.1 OS in NAC agent
CSCui73412	Yes	NAC Agent to elevate command prompt from admin user NAC Agent to allow UAC Elevation for all remediation actions.
CSCuj60553	Yes	Cisco Nac Agent wipes out Jabber Registry keys under HKEY_CURRENT_USER, when user logs off & logs in again. NAC Agent uses HKEY_CURRENT_USER section for temporary usage, it creates the HKCU\Software\Cisco folder as volatile. The other Cisco applications such as Cisco Jabber save keys into the same above HKCU\Software\Cisco folder. They get deleted when the user logs off / reboots the system. **Workaround** Install Jabber first, then Cisco NAC Agent.
CSCuj87393	Yes	Add support for Windows 8 N / 8.1 N OS in NAC Agent Support for Windows 8 N / 8.1 N OS has been added to NAC Agent.
CSCuj99389	Yes	NAC Agent drops packets when connected via CVO When connected to NAC Appliance using Cisco Virtual Office (CVO) setup, NAC Agent does not function properly and drops the packets.
CSCuh81023	Yes	Agent Should support Windows 8 Enterprise N / Professional N Edition Support for Windows 8 Enterprise N / Professional N Edition has been added to NAC Agent.
CSCul90129	Yes	Agent install wizard via Applet displays in English for foreign language The NAC Agent Installation Wizard is displayed in English even when the system locale language has been changed to any other language. Java 1.6 retrieves the language from "Control Panel > Region and Language > Keyboards and Languages > Display Language". The "Display language" (MUI Pack) is available only for Windows 7/Vista Enterprise and Ultimate editions. There is no official support for other Operating Systems.
CSCui44534	Yes	MAC 10.9 (Mavericks) OS support in MAC Agent for NAC Support for Mac OS X 10.9 (Mavericks) has been added.

New Installation of Release 4.9(4)

The following steps summarize how to perform new CD software installation of Release 4.9(4) on supported Cisco NAC Appliance hardware platforms (see Release 4.9(4) 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 4.9(4), page 54.

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 4.9(4), 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 59.

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 4.9(4) on each Clean Access Server and Clean Access Manager, as follows:

a. Log in to the Cisco Software Download Site at http://software.cisco.com/download/navigator.html. You will likely be required to provide your CCO credentials.

b. Navigate to **Security> Access Control and Policy> Network Admission Control > Cisco NAC Appliance (Clean Access) > Cisco NAC Appliance 4.9**.

c. Download the latest Release 4.9 .ISO image (e.g. **nac-4.9_4-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 nac-4.9_4-K9.isoAfter 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 Perform initial configuration of your CAM/CAS according to the instructions in the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

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 4.9(x)*
- *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*

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 4.9(4).

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 4.9(4) is bundled with version 4.9.4.3 of the Cisco NAC Agent and version 4.9.4.3 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 4.9(4)

Note To upgrade from Cisco NAC Appliance Release 4.1(8) or earlier to Release 4.9(4), you must first upgrade your system to Release 4.8(x) and then upgrade to Release 4.9(4).
You cannot upgrade Cisco NAC Appliance Release 4.1(8) or earlier to Release 4.8(x). You need to upgrade your system to Release 4.5(x), 4.6(1), or 4.7(0) and then upgrade to Release 4.8(x).

Note Starting from Cisco NAC Appliance Release 4.9, if there are inconsistencies in the database schema of the CAM, the upgrade process may be aborted. It is recommended to upgrade the CAM first and then the CAS. Otherwise, the CAS would have been upgraded but not the CAM. See also Troubleshooting CAM Database During Upgrade, page 84.

This section provides instructions for how to upgrade your existing supported Cisco NAC Appliance platform to Release 4.9(4). If you need to perform a new CD software installation, refer instead to New Installation of Release 4.9(4), page 53.

Refer to the following information prior to upgrade:

- Paths for Upgrading to Release 4.9(4)
- Changes for 4.9(4) 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 4.9(4) release includes Cisco NAC Profiler Collector version 3.1.0.24 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 4.8(1) and Collector 3.1.1, and you upgrade to NAC 4.9(4), the Collector version will be downgraded to 3.1.0.24. Refer to the corresponding *Release Notes for Cisco NAC Profiler* for software compatibility matrixes and additional upgrade and product information.

Paths for Upgrading to Release 4.9(4)

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:

- Migrating from a NAC-3310/3350/3390 Platform to Release 4.9(4) on a NAC-3315/3355/3395 Platform
- Migrating from a NAC-3315/3355/3395 Platform to Release 4.9(4) on a NAC-3415/3495 Platform

Note If you are upgrading from an earlier Cisco NAC Appliance release on non-Cisco hardware to a Cisco NAC-3315/3355/3395 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)* and then upgrade your system(s) to Release 4.9(4) according to the guidelines in Upgrade Instructions for Standalone Machines, page 60.

Migrating from a NAC-3310/3350/3390 Platform to Release 4.9(4) on a NAC-3315/3355/3395 Platform

Note This procedure only applies to customers upgrading from NAC-3310/3350/3390 (non-FIPS) platforms to NAC-3315/3355/3395 platform and assumes you are upgrading from Release 4.8(x) or 4.9(x) to Release 4.9(4).

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 NAC-3315/3355/3395 hardware you must first upgrade your existing system to Release 4.6(1) 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 NAC-3315/3355/3395 hardware, Cisco recommends that you:

Step 1 Ensure you have upgraded to Release 4.8(x) and created a backup snapshot for your system.

Step 2 Download and install the same 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 60 or Upgrade Instructions for HA Pairs, page 65 (depending on your deployment) to upgrade Cisco NAC Appliance from Release 4.8(x) or 4.9(x) to Release 4.9(4).

Step 5 Create a backup snapshot of your upgraded system.

Migrating from a NAC-3315/3355/3395 Platform to Release 4.9(4) on a NAC-3415/3495 Platform

Note This procedure only applies to customers upgrading from NAC-3315/3355/3395 platforms to a NAC-3415/3495 platform and assumes you are upgrading from Release 4.8(x) or 4.9(x) to Release 4.9(4).

If you are running the Cisco NAC Appliance software Release 4.8(x) or earlier on a NAC-3315/3355/3395 hardware, you must first upgrade your existing system to Release 4.9(4) using the **UPGRADE.sh** file. Once you obtain your NAC-3415/3495 hardware, Cisco recommends that you perform the following:

Step 1 Ensure you have upgraded to Release 4.9(4) and created a backup snapshot for your system.

Step 2 Download and install the same software version on your new NAC-3415/3495 platform.

Step 3 Restore the snapshot from your existing NAC-3315/3355/3395 to your new NAC-3415/3495 hardware.

Step 4 Create a backup snapshot of your upgraded system.

Changes for 4.9(4) Upgrade

Cisco NAC Appliance Release 4.9(4) 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 4.9(4), note the following:

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

- Password Changes

Hardware Considerations

- You can install Cisco NAC Appliance Release 4.9(4) on the following Cisco NAC Appliance platforms:
  - NAC-3415, NAC-3495

Note Cisco NAC Appliance platforms NAC-3415 and NAC-3495 support only fresh installation of Release 4.9(4) or upgrade from Release 4.9(2) and 4.9(3) to Release 4.9(4).

  - NAC-3315, NAC-3355, and NAC-3395 (FIPS or non-FIPS mode)

Note Cisco NAC Appliance platforms (FIPS or non-FIPS Cisco NAC-3315, NAC-3355, NAC-3395) support fresh installation of Release 4.9(4) or upgrade from Release 4.8(x) or 4.9(x) to Release 4.9(4) only.

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 4.6(1) 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 4.6(1) and later, refer to the *How to Fix Certificate Errors on the CAM/CAS After Upgrade* Troubleshooting Tech Note.**

- Starting from Release 4.7(1), the 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 4.9(4) .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.)
- Starting from Release 4.7(1), the 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 4.9(4) .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.)
- The **NACAgentCFG.xml** Agent configuration XML file packaged with the Cisco NAC Agent is not preserved after upgrading to 4.9(4). You must manually re-import the Agent configuration XML file to maintain client machine login behavior.

- The Cisco NAC Agent does not support Nessus-based network scanning. Nessus-based network scanning capabilities only apply to web login users and Clean Access Agent (Agent version 4.5.2.0 and earlier) users for whom a combination of client network scanning and Agent login functionality has been configured.
- 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.
- Users without administrator privileges upgrading their Windows client machine from an earlier version of the Clean Access Agent (version 4.5.2.0 and earlier or version 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 4.9(4), the installation process prompts you to upgrade the Agent files to the latest Windows Cisco NAC Agent and Mac OS X Agent versions packaged with the CAM software image (e.g. Cisco NAC Agent version 4.9.4.3, and Mac OS X Agent version 4.9.4.3).
- Release 4.9(4) includes version 3.1.0.24 of the Cisco NAC Profiler Collector component that resides on the CAS installations. When upgrading CAS appliances (standalone or HA) to Release 4.9(4), the upgrade script will check the version of the Collector and only upgrade it if version 3.1.0.24 is not already installed. Refer to the *Release Notes for Cisco NAC Profiler* for software compatibility matrixes and additional upgrade and product information.

Note Cisco NAC Profiler and Cisco NAC Guest Server are not supported in FIPS-compliant deployments in Release 4.9, 4.8, and 4.7(0).

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 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 4.9(x)*.
- 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**. You can find these settings at **Device Management > CCA Servers > Manage [CAS_IP] > Filter > Fallback.**
  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 4.9(4), 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 71.

Password Changes

- To offer increased security against potential unauthorized access to Cisco NAC Appliance, the CAM and CAS root admin password you specify during initial system configuration (when performing fresh install or Release 4.9(4) or reconfiguring the appliance via **`service perfigo config`**) must now meet strong password standards. However, any existing CAM/CAS root passwords are preserved during upgrade.
- For new installations of Cisco NAC Appliance, there is no longer a default **`cisco123`** CAM web console password. Administrators must specify a unique password for the CAM web console. However, any existing CAM web console passwords (including the old default **`cisco123`**) are preserved during upgrade.

For additional details, see also:

- Hardware Support, page 3
- Known Issues for Cisco NAC Appliance, page 69

General Preparation for Upgrade

Cisco strongly recommends you review this section carefully before commencing any Cisco NAC Appliance upgrade.

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.

- **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 4.9(4) software and some running 4.8(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 Managers Before Clean Access Servers**

  Starting with Cisco NAC Appliance Release 4.9(4), the Clean Access Manager must be upgraded before upgrading Clean Access Servers. Starting from Cisco NAC Appliance Release 4.9(4), there is a mechanism to rectify the Clean Access Manager's database if it is has errors. In case the erroneous database requires manual intervention for data correction, CAM upgrade process is aborted. Not upgrading CAM before CAS may lead to a situation wherein the NAC setup would have the CAS upgraded to 4.9(4) and CAM is still on lower version causing CAM-CAS communication failure and network down for long time. See Also Troubleshooting CAM Database During Upgrade, page 84.

- **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.

  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(x) database snapshot to a 4.9(4) CAM.**

- **Backup of necessary files**

  Cisco recommends to backup all the necessary files that are not related to the database configuration from the system before running upgrade. For example, any previous database backups and CAM/CAS log files can be backed up.

- **Software Downgrade**

  Once you have upgraded your software to Release 4.9(4), 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 4.9(4). See Upgrade Instructions for Standalone Machines, page 60 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 4.8(x) or 4.9(x) to Release 4.9(4), and only applies to Cisco NAC-3315/3355/3395 or Cisco NAC-3415/3495 platforms. If you have HA CAM/CAS pairs, refer instead to Upgrade Instructions for HA Pairs, page 65.

In Cisco NAC Appliance release 4.9(4), you can now use a .tar.gz upgrade process similar to that used for upgrading CAM/CAS appliances in earlier releases of Cisco NAC Appliance (like the process used in Release 4.7(2)) instead of having to perform “in-place” upgrades via an .ISO image on a CD-ROM, as is required to upgrade to Cisco NAC Appliance release 4.7(0) and 4.7(1).

After you have downloaded and copied the upgrade file to the CAM/CAS, you must use the CAM/CAS CLI to extract the upgrade image files and perform the upgrade procedure as described in Run the Upgrade Script on a Release 4.8(x) CAM/CAS, page 63.

Note You cannot use the Release 4.9(4) .ISO CD-ROM to perform an upgrade. You must use the .tar.gz upgrade file method.

Review Changes for 4.9(4) Upgrade, page 56 and General Preparation for Upgrade, page 59 before proceeding with these upgrade instructions.

Summary of Steps for Standalone Upgrade

The steps to upgrade standalone 4.9(4) systems are as follows:

1. Create CAM DB Backup Snapshot, page 61
2. Download the Upgrade File, page 62
3. Copy the Upgrade File to the CAS/CAM, page 62
4. Run the Upgrade Script on a Release 4.8(x) CAM/CAS, page 63

Create CAM DB Backup Snapshot

This section describes how to back up your current system so that you can retrieve your previous configuration in case there is an issue with the upgrade process.

Note Release 4.9(4) upgrades rewrite the appliance's hard-disk. Therefore, Cisco recommends backing up any non-essential data you may have manually archived (like syslog messages, event logs, etc.) onto another machine before beginning the upgrade process.

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. 05_11_10-15-47_snapshot). You can also either accept the default name or type another.

Step 3 Click **Create Snapshot**. The CAM generates a snapshot file and adds it to the snapshot list at the bottom of the page. The file physically resides on the CAM machine for archiving purposes. The Version field and the filename display the software version of the snapshot for convenience (e.g. **05_11_10-15-47_snapshot_VER_4_9_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 five entries. For further details, see "Database Recovery Tool" in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x)*.

Download the Upgrade File

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

Step 1 Log in to the Cisco Software Download Site at http://software.cisco.com/download/navigator.html. You will likely be required to provide your CCO credentials.

Step 2 Navigate to **Security> Access Control and Policy> Network Admission Control > Cisco NAC Appliance (Clean Access) > Cisco NAC Appliance 4.9**.

Step 3 Navigate to the Cisco NAC Appliance 4.9 subdirectory, download the latest 4.9 upgrade file (**cca_upgrade-4.9.4-from-4.8.x-4.9.x.tar.gz**), and save this file to the local computer from which you are accessing the CAM web console.:

Copy the Upgrade File to the CAS/CAM

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

If Using the Release 4.8(x) CAM/CAS Web Console

Step 1 Access the CAM software update web console page by navigating to **Administration > CCA Manager > Software Upload** and/or the CAS software upgrade web console page by navigating to **Administration > Software Upload**.

Step 2 Click **Browse** to navigate to the directory on your local machine where you have stored the Release 4.9(4) .tar.gz upgrade file. Download the **cca_upgrade-4.9.4-from-4.8.x-4.9.x.tar.gz**upgrade file.

Step 3 Click **Upload**. After a brief time, the web console screen automatically refreshes, displaying the newly uploaded Release 4.9(4) upgrade image and the date/time when it was uploaded to the CAM/CAS.

If Using WinSCP or SSH File Transfer

Step 1 Access the CAM via WinSCP or SSH File Transfer.

Step 2 Copy the **cca_upgrade-4.9.4-from-4.8.x-4.9.x.tar.gz** file from your local machine to the **/store** directory on the Clean Access Manager.

Step 3 Access each CAS via WinSCP or SSH File Transfer.

Step 4 Copy the **cca_upgrade-4.9.4-from-4.8.x-4.9.x.tar.gz** file from your local machine to the **/store** directory on *each* Clean Access Server.

If Using PSCP

Step 1 Open a command prompt on your Windows computer.

Step 2 Cd to the path where your PSCP resides (e.g, C:\Documents and Settings\desktop).

Step 3 Enter the following command to copy the file to the **/store** directory on the CAM:

```
pscp cca_upgrade-4.9.4-from-4.8.x-4.9.x.tar.gz root@<ipaddress_manager>:/store
```

Step 4 Enter the following command to copy the file to the **/store** directory on the CAS (copy to each CAS):

```
pscp cca_upgrade-4.9.4-from-4.8.x-4.9.x.tar.gz root@<ipaddress_server>:/store
```

Run the Upgrade Script on a Release 4.8(x) CAM/CAS

This section describes how to untar the upgrade file and run the script to upgrade standalone CAM/CAS machines from release 4.8(x) to release 4.9(4). You will need to login with your CAM and CAS **root** user passwords and access the command line of the CAM or CAS machine using one of the following methods:

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

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

Note The 4.9(4) upgrade script only executes if the current system is a supported Cisco NAC Appliance platform. Otherwise, the script exits with message "Unable to upgrade, not a recommended hardware platform for 4.9(4)".

Step 1: Upgrade the Release 4.8(x) CAS

Step 1 Connect to the Clean Access Server to upgrade using a console connection, or Putty or SSH.

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

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

```
cd /store
```

Step 4 Locate the upgrade file. If you used WinSCP, SSH File Transfer, or PSCP, the upgrade filename is **cca_upgrade-4.9.4-from-4.8.x-4.9.x.tar.gz**.

```
ls -l
```

Step 5 Extract the contents of the downloaded upgrade file:

```
tar xzvf cca_upgrade-4.9.4-from-4.8.x-4.9.x.tar.gz
```

The extraction process automatically places the upgrade files and necessary upgrade script in the **/cca_upgrade-4.9.1** directory.

Step 6 Change to the **/cca_upgrade-4.9.1** directory and execute the upgrade process:

```
cd cca_upgrade-4.9.1
./UPGRADE.sh
```

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

```
Finished upgrading the system to 4.9.1
Upgrade is complete.
```

```
Changes require a REBOOT
```

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

```
reboot
```

Step 9 Verify whether or not the upgrade was successful by logging into the CAS CLI and entering the following commands:

```
cd /perfigo/common/bin/
./showstate.sh | grep INCORRECT
```

If you do not see any output from the "grep INCORRECT" portion of the command, then your appliance has been upgraded successfully.

If your system returns any "INCORRECT" statements from the upgrade process, enter **`./showstate.sh`** again to capture the entire upgrade process output (including all CORRECT and INCORRECT entries) and save it to an easily accessible location on your local machine along with your backup snapshot you created in Create CAM DB Backup Snapshot, page 61 to help debug any upgrade issues.

Step 10 Repeat steps 1 through 9 for each CAS managed by the CAM.

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

Step 2: Upgrade the Release 4.8(x) CAM

Step 1 Connect to the Clean Access Manager to upgrade using a console connection, or Putty or SSH.

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

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

```
cd /store
```

Step 4 Locate the upgrade file. If you used WinSCP, SSH File Transfer, or PSCP, the upgrade filename is **cca_upgrade-4.9.4-from-4.8.x-4.9.x.tar.gz.**

```
ls -l
```

Step 5 Extract the contents of the downloaded upgrade file:

```
tar xzvf cca_upgrade-4.9.4-from-4.8.x-4.9.x.tar.gz
```

The extraction process automatically places the upgrade files and necessary upgrade script in the **/cca_upgrade-4.9.4** directory.

Step 6 Change to the **/cca_upgrade-4.9.4** directory and execute the upgrade process:

```
cd cca_upgrade-4.9.4
./UPGRADE.sh
```

Step 7 When prompted to update the Windows Agent, specify **`y`** or **`n`** to upgrade the Agent or retain the current Agent version.

```
Stopping the perfigo service...
Currently installed Windows NAC Agent version is 4.8.1.5. Do you want to change the
Windows NAC Agent to version 4.9.4.3 (y/n)? [y] y
Currently installed Mac Agent version is 4.8.1.584. Do you want to change the Mac Agent to
version 4.9.4.3 (y/n)? [y] y
```

```
Going to upgrade the manager rpm

Windows NAC Agent version updated to 4.9.1.6.
Mac Agent version updated to 4.9.1.684.
```

Step 8 Wait for the upgrade to complete. This will take several minutes.

```
Finished upgrading the system to 4.9.1
Upgrade is complete.
Changes require a REBOOT
```

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

```
reboot
```

Step 10 Verify whether or not the upgrade was successful by logging into the CAM CLI and entering the following commands:

```
cd /perfigo/common/bin/
./showstate.sh | grep INCORRECT
```

If you do not see any output from the "grep INCORRECT" portion of the command, then your appliance has been upgraded successfully.

If your system returns any "INCORRECT" statements from the upgrade process, enter **`./showstate.sh`** again to capture the entire upgrade process output (including all CORRECT and INCORRECT entries) and save it to an easily accessible location on your local machine along with your backup snapshot you created in Create CAM DB Backup Snapshot, page 61 to help debug any upgrade issues.

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

Upgrade Instructions for HA Pairs

In Cisco NAC Appliance release 4.9(4), you can now use a .tar.gz upgrade process similar to that used for upgrading CAM/CAS appliances in earlier releases of Cisco NAC Appliance (like the process used in Release 4.6(1) and Release 4.7(2)) instead of having to perform "in-place" upgrades via an .ISO image on a CD-ROM, as is required to upgrade to Cisco NAC Appliance release 4.7(0) and 4.7(1).

See Release 4.9(4) Upgrade Instructions for HA Pairs, page 65 to upgrade your HA Pair CAM/CAS appliances.

Release 4.9(4) Upgrade Instructions for HA Pairs

This section describes how to upgrade high-availability (HA) pairs of CAM or CAS servers from Release 4.8(x) or 4.9(x) to Release 4.9(4), and only applies to Cisco NAC-3315/3355/3395 or Cisco NAC-3415/3495 platforms. If you have standalone CAM/CAS servers, refer instead to Upgrade Instructions for Standalone Machines, page 60.

Note You cannot use the Release 4.9(4) .ISO CD-ROM to perform an upgrade. You must use the .tar.gz upgrade file method.

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 If you are changing the master secret for the CAM, ensure that both the CAMs are configured with the same master secret. If the master secret is different, when the standby CAM tries to come up, the perfigo service is stopped. Refer to CSCtd14712 for more details.

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 4.9(4) Upgrade, page 56 and General Preparation for Upgrade, page 59 before proceeding with these upgrade instructions.

Upgrading HA-CAM and HA-CAS Pairs

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

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

Step 1 Download and save the upgrade file to your local PC, as described in Download the Upgrade File, page 62. Download the **cca_upgrade-4.9.4-from-4.8.x-4.9.x.tar.gz** upgrade file

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

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

Step 3 Copy the upgrade image to each CAM/CAS machines' **/store** directory as described in Copy the Upgrade File to the CAS/CAM, page 62.

Step 4 Login as the `root` user with the root password.

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

```
cd /store
```

Step 6 Locate the upgrade file. If you used WinSCP, SSH File Transfer, or PSCP, the upgrade filename is **cca_upgrade-4.9.4-from-4.8.x-4.9.x.tar.gz**.

```
ls -l
```

Step 7 Extract the contents of the downloaded upgrade file:

```
tar xzvf cca_upgrade-4.9.4-from-4.8.x-4.9.x.tar.gz
```

The extraction process automatically places the upgrade files and necessary upgrade script in the **/cca_upgrade-4.9.4** directory.

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

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

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

Note The `fostate.sh` command is part of the upgrade script. 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" chapter in the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.
- SSH to the Service IP of the CAM/CAS pair, and type `ifconfig eth0`. The Service IP will always access the active CAM or CAS, with the other pair member acting as standby.

Step 9 Stop services on the standby appliance by entering the following command via the console/SSH terminal:

```
service perfigo stop
```

Step 10 Wait until the standby appliance has suspended services.

Step 11 Change directory and run the **fostate.sh** command on the active appliance:

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

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

Step 12 Upgrade the active appliance as follows:

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

b. From the untarred upgrade directory created on the active appliance (for example **cca_upgrade-4.9.4**), run the upgrade script on the active appliance:

```
./UPGRADE.sh
```

c. For the CAM only, when prompted to update the Windows Agent, specify `y` or `n` to upgrade the Agent or retain the current Agent version.

```
Please choose whether to upgrade Windows Agent to 4.9.4.3 (It's highly recommended to
upgrade) (y/n)? [y]
Please choose whether to upgrade Mac Agent to 4.9.4.3 (It's highly recommended to
upgrade) (y/n)? [y]
```

Step 13 After the upgrade is completed, stop services on the active appliance by entering the following command via the console/SSH terminal:

```
service perfigo stop
```

Wait until the active appliance has suspended services.

Step 14 Restart services on the standby appliance by entering the following command via the console/SSH terminal:

```
service perfigo start
```

Step 15 Upgrade the standby appliance as follows:

a. Make sure the upgrade package is untarred in the **/store** directory on the standby appliance.

b. Change to the untarred upgrade directory created on the standby appliance:

```
cd cca_upgrade-4.9.4
```

c. Run the upgrade script on the standby appliance:

```
./UPGRADE.sh
```

d. For the CAM only, when prompted to update the Windows Agent, specify **y** or **n** to upgrade the Agent or retain the current Agent version.

```
Please choose whether to upgrade Windows Agent to 4.9.4.3 (It's highly recommended to
upgrade) (y/n)? [y]
Please choose whether to upgrade Mac Agent to 4.9.4.3 (It's highly recommended to
upgrade) (y/n)? [y]
```

Step 16 Verify whether or not the upgrade was successful by logging into the CLI of each CAM/CAS upgraded in the HA pair and entering the following commands:

```
cd /perfigo/common/bin/
./showstate.sh | grep INCORRECT
```

If you do not see any output from the "grep INCORRECT" portion of the command, then your appliance has been upgraded successfully.

If your system returns any "INCORRECT" statements from the upgrade process, enter **./showstate.sh** again to capture the entire upgrade process output (including all CORRECT and INCORRECT entries) and save it to an easily accessible location on your local machine along with your backup snapshot you created in Create CAM DB Backup Snapshot, page 61 to help debug any upgrade issues.

Step 17 After the upgrade is completed, stop services on the standby appliance by entering the following command via the console/SSH terminal:

```
service perfigo stop
```

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

```
reboot
```

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

Step 19 Reboot the standby appliance by entering the following command via the console/SSH terminal:

```
reboot
```

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

Known Issues for Cisco NAC Appliance

This section describes known issues when integrating Cisco NAC Appliance:

Known Issue with CAS-to-CAM Certificate Verification in Internet Explorer

When launching the CAM web console in Release 4.9 using Internet Explorer, you may see a “Choose a digital certificate” pop-up dialog with no options available in the selection window. This pop-up is a result of the way the CAM verifies CAS-to-CAM certificates for communication. If you click **OK** or **Cancel**, the dialog disappears and you can continue the web console session normally. If you want to ensure this pop-up does not appear in the future. you can apply the following custom security setting in Internet Explorer:

1. Go to **Tools > Internet Options**, click on the **Security** tab, and click **Custom Level**.
2. Scroll down and enable the **Don’t prompt for client certificate selection when no certificate or only one certificate exists** option.
3. Click **OK**.

Note This issue has not been observed when accessing the CAM with Mozilla Firefox or Google Chrome browsers.

Known Issue with Delayed IP Address Refresh for Windows 7/Vista Clients Running Cisco NAC Agent

The IP address release/renew process for Windows 7 and Windows Vista client machines running Cisco NAC Agent version 4.8.0.x that move from the authentication to access VLAN can take as long as 4 minutes to complete.

This situation can occur when the Network Connectivity Status Indicator, which is part of the Network Location Awareness in Windows, tries to reach the **msftncsi.com** web page while refreshing the client machines IP address. When the client machine cannot reach this page, Windows 7 and Windows Vista take longer to sense the machine's status, thus slowing down applications requiring internet access.

For reference, see:

- http://technet.microsoft.com/en-us/library/cc766017(WS.10).aspx
- http://technet.microsoft.com/en-us/library/ee126135(WS.10).aspx

To resolve this issue, open the following sites using host traffic policies in any user roles associated with the client login session (Unauthenticated/Quarantine, Temporary, and standard user login roles):

- **`ncsi.glbdns.microsoft.com equals Microsoft NCSI check`**
- **`.msftncsi.com ends Microsoft NCSI check`**

The administrator can also use a utility like Microsoft SMS to pass a registry update disabling this option in the Windows registry on client machines.

See CSCtg06599 for more information.

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 26.

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 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 4.9(x)*.

Client machines going across a GRE tunnel in the network are unable to authenticate and the agent doesn't popup.

Known Issue with IP Packet Fragmentation Leading to Disconnect Between CAS and Agent

TCP traffic between the Agent and CAS can break down if the overall network path MTU is smaller than the MTU needed for the CAS to send unfragmented packets and the packet coming from the CAS to the Agent has the "do not fragment" setting enabled.

Note This scenario has been observed with TCP SSL packets and generally only applies to authentication, posture, and discovery host traffic. This issue does not apply to traffic that is not directed specifically to the CAS/Discovery Host.

To address this issue, apply one of the following solutions to your network:

- Set the IP TCP adjust-mss for the GRE tunnel according to the guidelines at http://www.cisco.com/en/US/docs/ios/12_2t/12_2t4/feature/guide/ft_admss.html.
- Remove the "do not fragment" setting from the packet using a route map, as described in at http://www.cisco.com/en/US/tech/tk827/tk369/technologies_white_paper09186a00800d6979.shtml.

  Example configuration:

```
interface FastEthernet0/0
 ip address 10.32.32.101 255.255.255.0
 ip policy route-map removedontfrag
 duplex auto
 speed auto
!
access-list 101 permit tcp host 10.255.253.152 any
access-list 101 permit tcp host 10.255.252.152 any
access-list 101 permit tcp host 1.1.1.1 any
!
route-map removedontfrag permit 10
 match ip address 101
 set ip df 0


NOTE: 10.255.253.152 is the trusted IP Address of the CAS
NOTE: 10.255.252.152 is the trusted IP Address of the CAS
NOTE: 1.1.1.1 is the discovery host resolved IP Address.
```

Known Issues with Switches

For complete details, see *Cisco NAC Appliance Switch and Wireless LAN Controller Support*.

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 *Cisco NAC Appliance Switch and Wireless LAN Controller Support* 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 4.9(x)*.

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 20.

Known Issue for Integrating NAC with ISE Profiler

When the admin users are assigned to the group "Help Desk" and "Read-only", and added to ISE, the endpoints created in ISE are getting added to the CAM Filter list. The Help Desk and Read-only users added in ISE under NAC Managers are able to update the endpoints.

Only the Admin users under "Full Control Admin" should be able to add, edit, or delete the endpoints in CAM.

See also CSCts37221, page 47.

Known Issue with CDL Timer

The change of VLAN configuration on CDL timer expiry is not supported for wireless users.

Known Issue While Upgrading to Mac OS X Agent

When you try to upgrade Mac OS X Agent versions 4.9.0.638 or 4.8.2.594 to the latest Mac OS X 4.9.1.684, there may be issues.

You can try the following workarounds:

- Manually remove **CCAAgent.pkg** from **/var/folders/<temporary directory>**. This temporary directory may differ for the client machines. You can find the exact path as follows:
  - Run Terminal
  - Enter the following command

    ```
    set | grep TMPDIR
    ```

- Reboot the client machine.
- Connect to the web login page and install the Agent from there, if available.

Known Issue While Downloading NAC Agent and Web Agent

While downloading the NAC Agent 4.9.2.8 and Web Agent 4.9.2.6 on Windows XP clients, you may not be able to download the Agents properly. The browser might show the status as “Undefined” and might fail to launch the ActiveX or Java Applet.

The issue happens due to Windows XP root certificate. You can download the **rootsupd.exe** file and run it on the client machine. This updates the XP root certificate and allows you to install ActiveX controls.

You can download **rootsupd.exe** from the following website:

http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/rootsupd.exe

Troubleshooting

This section provides troubleshooting information for the following topics:

- Recovering Root Password for CAM/CAS
- Filtering Logs by CAS and/or Agent IP
- Troubleshooting CAM/CAS Certificate Issues
- Troubleshooting CAM Database During Upgrade
- Troubleshooting Switch Support Issues
- Other Troubleshooting Information

Note For additional troubleshooting information, see also New Installation of Release 4.9(4), page 53.

Obtaining Configuration Details of CAM and CAS

In Cisco NAC Appliance Release 4.9 and later, you can use the **showrun** command to get the configuration details of the CAM and CAS. This command reads the file system and database from the CAM and CAS without impacting services, and provides the output as an .xml file.

The Administrator can send this .xml file to the Cisco TAC support team for troubleshooting purposes. This file provides the details of the features configured in the CAM and CAS.

In CAM, you can run the following commands in the **/perfigo/diag** folder.

./showrun.sh or **./showrun.sh** *-config config.xml* — Use this command to get the general configuration details.

./showrun.sh *-verifydb* — Use this command to check the database consistency.

./showrun.sh *-verifyha <peerip>* — Use this command to validate the HA configuration.

You can run the following command to validate the HA configuration in both CAM and CAS. Run the command in the **/perfigo/common/bin/havalidator** folder in CAM and/or CAS.

./havalidator.pl *<peerip>*

For the general configuration details, the **config.xml** file should be available in the **/perfigo/diag** folder. In this file, you can specify the options for which you need the configuration details.

Example config.xml file:

```
<?xml version="1.0" encoding="UTF-8"?>
<nac:Configuration xmlns:nac="http://nac.cisco.com/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://nac.cisco.com/X
MLSchema Config.xsd ">
  <nac:Output>
    <nac:XML>true</nac:XML>
  </nac:Output>
  <nac:NACM>
    <nac:basic>true</nac:basic>
    <nac:filter>true</nac:filter>
    <nac:policy>false</nac:policy>
    <nac:auth>true</nac:auth>
    <nac:role>true</nac:role>
    <nac:oob>true</nac:oob>
  </nac:NACM>
  <nac:NACS>
    <nac:nacsConfig>
      <nac:basic>true</nac:basic>
      <nac:advanced>true</nac:advanced>
```

```
      <nac:dhcp>true</nac:dhcp>
      <nac:filter>true</nac:filter>
      <nac:policy>true</nac:policy>
      <nac:auth>true</nac:auth>
    </nac:nacsConfig>
    <nac:nacsInfo>
      <nac:ip>10.201.5.65</nac:ip>
      <nac:nacsConfig>
        <nac:basic>true</nac:basic>
        <nac:advanced>true</nac:advanced>
        <nac:dhcp>true</nac:dhcp>
        <nac:filter>true</nac:filter>
        <nac:policy>true</nac:policy>
        <nac:auth>true</nac:auth>
      </nac:nacsConfig>
    </nac:nacsInfo>
  </nac:NACS>
</nac:Configuration>
```

The **showrun** command gets configuration details for the fields that are set to "true" in the **config.xml** file.

The above example generates output files as follows:

NACMBasic.xml file:

This is a basic information xml file that contains build information like name, version, and date. The file includes details like interface, DNS, time zone, update information like agent version, role list, etc.

The following example shows a sample output file containing basic information.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>
 <nac:camBaseInfo xmlns:nac="http://nac.cisco.com/XMLSchema"
xmlns:ns2="http://nac.cisco.com/OobInfo" xmlns:ns4="http://nac.cisco.com/CasAdvancedInfo"
xmlns:ns5="http://www.example.org/VlanProfile"
xmlns:ns6="http://www.example.org/OSDetection">
  <nac:build>
  <nac:name>Clean Access Manager</nac:name>
  <nac:version>4.9.0</nac:version>
  <nac:date>2011-05-22</nac:date>
  </nac:build>
  <nac:MasterSecret>HWVwHfdThzT5kV8o1WmNe8tJptU=</nac:MasterSecret>
  <nac:network>
  <nac:eth0>
  <nac:ip>9.9.10.5</nac:ip>
  <nac:netmask>255.255.255.0</nac:netmask>
  <nac:gateway>9.9.10.1</nac:gateway>
  </nac:eth0>
  <nac:dns>
  <nac:hostname>CAM-NAG</nac:hostname>
  <nac:dnsServer>171.70.168.183</nac:dnsServer>
  </nac:dns>
  <nac:time>
  <nac:timeZone>Asia/Kolkata</nac:timeZone>
  <nac:ntpServer>time.nist.gov</nac:ntpServer>
  </nac:time>
  </nac:network>
  <nac:updates>
  <nac:versions>
  <nac:updateVersion>
  <nac:CiscoChecksRules>0</nac:CiscoChecksRules>
  <nac:AVASWindows>0</nac:AVASWindows>
  <nac:AVASMacintosh>0</nac:AVASMacintosh>
  <nac:HostPolicies>0</nac:HostPolicies>
```

```
<nac:L2Policies>0</nac:L2Policies>
<nac:OsDetection>0</nac:OsDetection>
<nac:OOBSwitchOIDs>0</nac:OOBSwitchOIDs>
</nac:updateVersion>
<nac:agentVersion>
<nac:WindowsCleanAccessAgent>4.9.0.28</nac:WindowsCleanAccessAgent>
<nac:MacintoshCleanAccessAgent>4.9.0.638</nac:MacintoshCleanAccessAgent>
<nac:CiscoNacWebAgent>4.9.0.14</nac:CiscoNacWebAgent>
<nac:CiscoNacAgentActiveX>4.9.0.3</nac:CiscoNacAgentActiveX>
<nac:CiscoNacAgentApplet>4.9.0.5</nac:CiscoNacAgentApplet>
<nac:L3MacAddressDetectionActiveX>2.9.0.0</nac:L3MacAddressDetectionActiveX>
<nac:L3MacAddressDetectionApplet>3.3.0.0</nac:L3MacAddressDetectionApplet>
</nac:agentVersion>
</nac:versions>
<nac:updateSettings>
<nac:autoUpdate>
<nac:enabled>false</nac:enabled>
<nac:updateTime>01:00:00</nac:updateTime>
</nac:autoUpdate>
<nac:updateWindowsAgent>false</nac:updateWindowsAgent>
<nac:updateMacAgent>false</nac:updateMacAgent>
<nac:updateWebAgent>false</nac:updateWebAgent>
<nac:updateL3Agent>false</nac:updateL3Agent>
</nac:updateSettings>
<nac:httpSettings>
<nac:useProxy>false</nac:useProxy>
</nac:httpSettings>
</nac:updates>
<nac:ha Mode="STANDALONE" />
<nac:caslist />
<nac:rolelist>
<nac:RoleName>Unauthenticated Role</nac:RoleName>
<nac:RoleName>Temporary Role</nac:RoleName>
<nac:RoleName>Quarantine Role</nac:RoleName>
</nac:rolelist>
<nac:policySyn>
<nac:enable>false</nac:enable>
</nac:policySyn>
</nac:camBaseInfo>
```

Apart from the above file, the following output files are generated.

- **NACMFilter xml:** This file contains information about all the device filters.
- **NACMAuth.xml:** This file contains information about the Auth Servers.
- **NACMRoleInfo.xml:** This file contains details of role-entry list.

The output files for the CAM are available at **`/perfigo/diag/output/cam`**. For the CAS, the output files are stored at **`/perfigo/diag/output/cas/`** with subdirectories for each CAS connected to the CAM.

Note The configuration details are obtained only for the CASs connected to the CAM.

Each time you run the **showrun** command, it overwrites the output files in the above directories.

Troubleshooting Click Logs

In Cisco NAC Appliance Release 4.9 and later, you can use the Click Logging script to monitor the traffic that passes from the client to the Clean Access Server. When the traffic is passed through certain perfigo elements, the actions are recorded in a log file. This helps the administrator to analyze the cause when a packet is dropped by the CAS.

Command syntax for the Click Logging script:

click-logging enable-by-ip <ip> [brief | detail] | enable-by-mac <mac> [detail] | disable

Note It is recommended to try this command with the help of Cisco TAC.

The following are some of the perfigo elements through which the traffic passes from the client to the CAS:

- Device Filters
- Subnet Filters
- Roles
- Traffic Policies
- DNS
- ARP

The script **click-logging.sh** can be run by providing either the IP Address or the MAC Address of the client as input.

To enable the logging script:

Step 1 Login to CAS CLI and go to **/perfigo/access/bin/**

Step 2 Run the command as follows:

```
./click-logging enable-by-ip <ip> [brief|detail] | enable-by-mac <mac> [detail]
```

where **ip** is the IP Address and **mac** is the MAC Address of the client. The **brief** option provides information without the packet contents. The parameter **detail** provides details of the packet contents along with the other information in the log files.

Note The parameter **brief** or **detail** is optional. If you do not include this parameter in the command, the log files provide **brief** information by default.

The logs are constantly recorded as the traffic passes through the elements in the click. You can troubleshoot by referring to the output logs that are available at `/var/log/messages`.

After troubleshooting, remember to disable the script by running the command `click-logging disable`.

Note When the click logging script is enabled, the performance of the CAS may be slow.

Disabling Administrator Prompt for Certificate on IE 8 and 9

If no certificates or only one certificate is installed in the personal store in Windows then there is an administrator prompt for certificate in IE9. The prompt can be disabled by setting the option on Internet Explorer.

To disable the prompt:

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

Step 2 Click the S**ecurity** tab. Select a zone to view or change security settings (that the NAC Manager URL falls under).

Step 3 Click **Custom level** under Security level for this zone.

Step 4 **Enable** Don't prompt for client certificate selection when no certificates or only one certificate exists.

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 10, IE 8, and IE 7Certificate Revocation List

Note In Internet Explorer versions 10, 8, and 7, 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 4.9(x)*.

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.

Troubleshooting SSKEY Mismatch Error

SSKEY is an identifier used by CAM to identify a CAS. This key is a combination of the MAC addresses (eth0 + eth1) of the CAS. In an HA environment, it is the combination of the MAC addresses(eth0 + eth1) of the Primary CAS. Each CAS or CAS pair has a unique SSKEY stored in the CAM database.

SSKEY mismatch would happen when the primary CAS is replaced. When SSKEY mismatch happens, CAM-CAS communication fails. See CSCtq74462, page 49.

Perform the following to modify the SSKEY in the CAM database:

Step 1 Run **`service perfigo stop`**

Step 2 Run **`/perfigo/control/bin/replace_sskey.sh`** *`[CAS IP] [SSKEY]`*

[SSKEY] is the MAC addresses(eth0 + eth1) of the new primary CAS.

Step 3 Run **`service perfigo start`**

Step 4 Run the following command to check whether SSKEY has been updated properly.

```
psql -U postgres -h localhost controlsmartdb -c "SELECT * from securesmart_info"
```

In an HA environment, ensure that the SSKEY of secondary CAS is also updated.

Step 1 In the secondary CAS, go to **Administration > Network Settings > Failover**.

Step 2 Update **[Primary] Peer Serial No**. with the combination of the MAC addresses (eth0 + eth1) of new primary CAS along with **[Primary] Peer MAC Address** for both trusted-side and untrusted-side interfaces.

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 , page 12).
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 82.
9. If necessary, provide CAM support logs as described in Creating CAM/CAS Support Logs, page 84.

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 4.9(x)*.

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 4.9(x)* or *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Recovering Root Password for CAM/CAS

Refer to the "Password Recovery" chapter of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.9(x)*.

Filtering Logs by CAS and/or Agent IP

Refer to the "Filtering logs by CAS and/or agent IP" section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x)* and *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Troubleshooting CAM/CAS Certificate Issues

Refer to the "Troubleshooting Certificate Issues" sections of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x)* or *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*.

Troubleshooting CAM Database During Upgrade

Starting from Cisco NAC 4.9, there is a mechanism to check CAM's database consistency during upgrade. When the database of a CAM is inconsistent, upgrading the CAM creates problems. Database of the CAM becomes erroneous due to some missing constraints like primary key, foreign key, or unique key. It also becomes erroneous due to bad data or records present in the database or a combination of missing constraints and bad records.

In a database table, if the problem that exists is missing primary key, foreign key, or unique key, upgrade process takes care of auto-correction of the missing key constraints. These missing key constraints are enabled again. When both the problems of missing constraints and bad records are present in the database table, upgrade process is aborted and the user needs to manually correct the data before trying to upgrade again.

Note Starting from Cisco NAC 4.9, CAM upgrade is aborted due to the presence of bad records. This requires CAM to be upgraded first before CAS. Else, a situation may come wherein the NAC setup has the CAS upgraded to 4.9 and CAM is still on lower version causing CAM-CAS communication failure and network down.

This following example shows the DB correction mechanism during CAM upgrade. You should be careful while manipulating the database. If you do not have a good understanding of database and SQL, contact Cisco TAC for help.

```
[root@nacmanager cca_upgrade-4.9.0]# ./UPGRADE.sh
Stopping the perfigo service...
Verifying the CAM db schema...
CAM db schema is invalid. Proceeding to rectify ...

-------------------------------------------------
Running DB restorer script ...
Going to start modifying the db
Temporary verification database No temporary database present. Proceeding...
Creating temporary database...
Temporary database creation succeeded.
Populating temporary database with schema succeeded.
Extracted temporary database schema successfully.
Dumping data from controlsmartdb...
Temporary verification database Dropping temporary database...
Dropping tempdb database succeeded.
Temporary database creation succeeded.
Populating temporary database with schema succeeded.
pg restore of archive file to tempdb succeeded.
ERROR: Adding constraints to temporary database failed. Transaction changes were rolled
back.
FATAL: Database restoration aborted
-------------------------------------------------

ERROR: Data in CAM's db inconsistent. Correct the data first or contact TAC!
FATAL: CAM upgrade aborted!
```

Now, CAM upgrade is aborted due to erroneous database. Check the file **`/perfigo/control/data/constr.log`** and observe the first point of error.

For example, if you get a message as follows:

```
NOTICE:  ALTER TABLE / ADD PRIMARY KEY will create implicit index "switch_profile_pkey"
for table "switch_profile"
NOTICE:  ALTER TABLE / ADD UNIQUE will create implicit index "uploaded_file_file_type_key"
for table "uploaded_file"
ERROR:  could not create unique index
DETAIL:  Table contains duplicated values.
```

The above error means that the unique key constraints on the **uploaded_file table** are not added as they have duplicate values with respect to the unique key. The unique key for uploaded_file table is (**file_type, file_name**). Go to the **`controlsmadb`** database CLI on the CAM to check the following:

```
[root@nacmanager cca_upgrade-4.9.0]# su - postgres
bash-3.2$ psql -h 127.0.0.1 controlsmartdb
controlsmartdb=# select * from uploaded_file;

file_id | file_type | file_name  | file_data | file_size |          file_timestamp          |
file_flag |   file_desc    |   ss_key
```

```
---------+-----------+------------+-----------+-----------+---------------------------------+-----
------+---------------+-------------
      2 | Test      | Mcafee.txt |           |      3024 | 2011-09-16 09:23:31.333309+05:30 | true
| test file only | G.L.O.B.A.L
      2 | Test      | norton.txt |           |      2024 | 2011-09-16 09:22:48.341087+05:30 | true
| test file only | G.L.O.B.A.L
      1 | Test      | Mcafee.txt |           |      1024 | 2011-09-16 09:22:20.004592+05:30 | true
| test file only | G.L.O.B.A.L
```

You can view two records if you have the same **(file_type, file_name)** tuple. Retain the right one and delete the rest. This is an example of duplicate records. Exit from the db prompt and run the upgrade again.

```
controlsmartdb=# delete from uploaded_file where file_id = 2 and file_size = 3024;
controlsmartdb=# \q
-bash-3.2$ exit
logout
[root@nacmanager cca_upgrade-4.9.0]# ./UPGRADE.sh
Stopping the perfigo service...
Verifying the CAM db schema...
CAM db schema is invalid. Proceeding to rectify ...

--------------------------------------------------
Running DB restorer script ...
Going to start modifying the db
Temporary verification database Dropping temporary database...
Dropping tempdb database succeeded.
Creating temporary database...
Temporary database creation succeeded.
Populating temporary database with schema succeeded.
Extracted temporary database schema successfully.
Dumping data from controlsmartdb...
Temporary verification database Dropping temporary database...
Dropping tempdb database succeeded.
Temporary database creation succeeded.
Populating temporary database with schema succeeded.
pg restore of archive file to tempdb succeeded.
ERROR: Adding constraints to temporary database failed. Transaction changes were rolled
back.
FATAL: Database restoration aborted
--------------------------------------------------

ERROR: Data in CAM's db inconsistent. Correct the data first or contact TAC!
FATAL: CAM upgrade aborted!
```

The upgrade is aborted again. Look at the file **`/perfigo/control/data/constr.log`** for errors. For example:

```
ERROR:  insert or update on table "user_account_prop" violates foreign key constraint
"user_account_prop_user_id_fkey"
DETAIL:  Key (user_id)=(2) is not present in table "user_account".
```

The above is an example of bad records caused by violation of foreign key constraints. The table **user_account_prop** has some records **(user_id = 2)** that do not correspond to records in the parent table **user_account**.

```
controlsmartdb=# select * from user_account;
 user_id | user_name | user_password        | role_id | user_enable | user_desc
---------+-----------+----------------------+---------+-------------+----------
       0 | guest     | ba53bd3282     |       0 |           1 | guest user
       1 | alex      | password1      |       1 |           1 | test user

controlsmartdb=# select * from user_account_prop;
```

```
 user_id | prop_name   | prop_value
---------+-------------+------------
       1 | RadiusUser  | true
       2 | RadiusUser  | false
```

In the above example, **user_account_prop** table shows a record **user_id = 2**, which does not have a corresponding entry in the **user_account** table. To fix this, either add an user with **user_id = 2** in the **user_account** table or delete the record with user_id = 2 from the **user_account_prop** table.

In the following example, after deleting the record from **user_account_prop** table, the upgrade is run again:

```
controlsmartdb=# delete from user_account_prop where user_id = 2;

[root@nacmanager cca_upgrade-4.9.0]# ./UPGRADE.sh
Stopping the perfigo service...
Verifying the CAM db schema...
CAM db schema is invalid. Proceeding to rectify ...

-----------------------------------------------------
Running DB restorer script ...
Going to start modifying the db
Temporary verification database Dropping temporary database...
Dropping tempdb database succeeded.
Creating temporary database...
Temporary database creation succeeded.
Populating temporary database with schema succeeded.
Extracted temporary database schema successfully.
Dumping data from controlsmartdb...
Temporary verification database Dropping temporary database...
Dropping tempdb database succeeded.
Temporary database creation succeeded.
Populating temporary database with schema succeeded.
pg restore of archive file to tempdb succeeded.
Adding constraints to temporary database succeeded.

Renaming controlsmartdb database to controlsmartdb_orig succeeded.
Renaming tempdb to controlsmartdb  succeeded.
Running showstate.sh to check database remediation...
Showstate.sh completed successfully.
Dropping controlsmartdb_orig database succeeded.
Database remediation was successful.
-----------------------------------------------------

CAM db schema corrected!
Upgrade to proceed normally!
<Rest of the text deleted here>
```

The above example shows that the database issues are corrected and the upgrade is successful.

Troubleshooting Switch Support Issues

To troubleshoot switch issues, see *Cisco NAC Appliance Switch and Wireless LAN Controller Support.*

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 8 Updates to Release Notes for Cisco NAC Appliance, Release 4.9(4)

Date	Description
02/10/2014	Release 4.9(4)

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 4.9(x)*
- *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.9(x)*
- *Cisco NAC Appliance - Clean Access Server Configuration Guide, Release 4.9(x)*
- *Getting Started with Cisco NAC Network Modules in Cisco Access Routers*
- *Cisco NAC Appliance FIPS Card Field-Replaceable Unit Installation Guide*
- *Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later*
- *Cisco NAC Appliance Switch and Wireless LAN Controller Support*
- *Cisco NAC Appliance Service Contract / Licensing Support*

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