Release Notes for Cisco NAC Profiler, Release 3.1.1

November 16, 2011, OL-23117-01

Contents

These release notes provide late-breaking and release information for Cisco NAC Profiler, Release 3.1.1. This document describes enhancements, limitations, and restrictions ("caveats"), upgrade instructions, and related information. These release notes supplement the Cisco NAC Profiler and Cisco NAC Appliance documentation that is included with the distribution. Read these release notes carefully and refer to the upgrade instructions prior to installing the software.

Cisco NAC Profiler Releases

Cisco NAC Profiler Version	Release Date
3.1.1-18	August 17, 2010

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

Note Cisco recommends that you deploy *early deployment* releases in a test network before you attempt top deploy this in a production network.

System Requirements

This section contains the following:

- Licensing
- Hardware Supported

Licensing

For general information on licensing for Cisco NAC Profiler Server and Cisco NAC Profiler Collector see *Cisco NAC Appliance Service Contract/Licensing Support*.

Hardware Supported

The supported Cisco NAC Profiler system consists of a Cisco NAC Profiler Server or Cisco NAC Profiler Lite Server, implemented as a standalone appliance or a high availability (HA) pair, and one or more NAC Profiler Collectors that run on Cisco NAC Server appliances. The NAC Profiler Collectors can also be deployed as HA pairs when run on Cisco NAC Server HA pairs. The Cisco NAC Profiler appliances leverage the Cisco NAC Appliance 3300-series hardware platforms.

Note Cisco NAC Appliance Release 4.7.(0) and Release 4.8 are the only tested FIPS 140-2 compliant releases. Cisco NAC Profiler and Cisco NAC Guest Server are not supported in FIPS-compliant deployments in Cisco NAC Appliance Releases 4.7.(0) or 4.8.

Cisco NAC Profiler Lite

The Cisco NAC Profiler Lite is a hardware platform that comes pre-installed with a default version of the Cisco NAC Profiler Lite software. Cisco NAC Profiler Lite requires a separate ISO file.

Note The Cisco NAC Profiler Server is only supported on the NAC-3355 hardware platform. If ordering a NAC Profiler Lite, you will actually receive a NAC-3355 based appliance with a NAC Profiler Lite License.

Cisco NAC Profiler Server

The Cisco NAC Profiler Server is based on the NAC-3350/3355 hardware platforms and is pre-installed with a default version of the Cisco NAC Profiler Server software (3.1.1-18).

Cisco NAC Profiler Collector (on Cisco NAC Servers)

A default version of the Cisco NAC Profiler Collector component is included as a service on Cisco NAC Server appliances beginning with the Cisco NAC Appliance 4.1.2.1 and later releases. The Cisco NAC Server operates on NAC-3310/NAC-3315 and/or NAC-3350/3355 Server appliance platforms only.

The Cisco NAC Profiler Collector is a distributed component that typically resides on the Cisco NAC Appliance Server - Clean Access Server (CAS) and communicates with the Cisco NAC Profiler Server. A default version of the Cisco NAC Profiler Collector is shipped with each CAS, and there is one Profiler Collector per CAS.

Note For proper operation, both the Cisco NAC Profiler Collector component on the Cisco NAC Server and Cisco NAC Profiler Server (Profiler Server or Profiler Lite) **must** run the same version of the Cisco NAC Profiler software. Refer to Cisco NAC Appliance/ Cisco NAC Profiler Compatibility Matrix, page 4 for details.

Note You need to upgrade the default version of the Profiler Collector shipped with the NAC Server software for compatibility with the latest Cisco NAC Profiler. For details refer to Cisco NAC Appliance/ Cisco NAC Profiler Compatibility Matrix, page 4.

Cisco NAC Profiler Collector (Standalone Version)

Note The Cisco NAC Profiler Collector standalone version is an option that is only valid for non-HA Collectors.

You can also deploy a standalone version of the Cisco NAC Profiler Collector component on appliances that are running only the Cisco NAC Profiler Collector service on Cisco NAC Servers that are running without the Cisco NAC Server services enabled.

For example, standalone Cisco NAC Profiler Collector components can be started and operated using the server connection type or the client connection type. For specific details, see the following sections in “Installing and Performing an Initial Configuration” in the *Cisco NAC Profiler Installation and Configuration Guide, Release 3.1.1* at: *http://www.cisco.com/en/US/products/ps8464/products_installation_and_configuration_guides_list.html*

- “Starting Up a Standalone NAC Profiler Collector using the Client Connection Type”
- “Starting Up a Standalone NAC Profiler Collector using the Server Connection Type”

While performing a **service collector config** command on a Cisco NAC Server appliance, you need to make sure to select the following options:

- Connection type (server/client) [client]:
- Connect to IP [127.0.0.1]: 10.30.30.5
- Port number [31416]:
- Encryption type (AES, Blowfish, none) [AES]: AES
- Shared secret []: cisco123 (this is an example only)

See Product Change Information, page 9 for details on the latest release 3.1.1 builds.

For ordering information, refer to the *Cisco NAC Profiler Ordering Guide*.

Software Compatibility

This section describes the following:

- Cisco NAC Appliance/ Cisco NAC Profiler Compatibility Matrix, page 4
- Cisco NAC Profiler Collector Support and NAC Server Deployment Modes, page 5
- Supported Web Browsers for Release 3.1.1, page 7
- Determining the Software Release Version, page 7

Note Cisco NAC Profiler Release 3.1.1 has been tested with Cisco Secure Access Control System (ACS) Release 5.1.

Cisco NAC Appliance/ Cisco NAC Profiler Compatibility Matrix

Table 1 shows Cisco NAC Appliance and Cisco NAC Profiler compatibility and software versions supported for each component of the Cisco NAC Profiler solution. For proper operation, both the Profiler Collector(s) and Profiler Server (Profiler Server or Profiler Lite) **must** run the same version of the Cisco NAC Profiler software.

Note Cisco NAC Profiler release 3.1.1 replaces and supersedes **all** previous releases of Cisco NAC Profiler.

Note Cisco NAC Appliance releases are shipped with a default version of the NAC Collector version. 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 NAC 4.7.2 and Profiler 3.1.1-18 and you upgrade to NAC 4.8.0, you need to manually re-install the NAC Collector release 3.1.1 and configure it following the NAC Server upgrade.

Note Cisco NAC Appliance Release 4.7.(0) and Release 4.8 are the only tested FIPS 140-2 compliant releases. Cisco NAC Profiler and Cisco NAC Guest Server are not supported in FIPS-compliant deployments in Cisco NAC Appliance Releases 4.7.(0) or 4.8.

Table 1 Cisco NAC Appliance / Cisco NAC Profiler Compatibility Matrix[1]

Cisco NAC Server Appliance Components[2]			Cisco NAC Profiler Appliance
Cisco NAC Appliance Version	Cisco NAC Profiler Collector Version Shipped with Cisco NAC Server	Upgrade Cisco NAC Profiler Collector Version to:[3]	Upgrade Cisco NAC Profiler Server to:
4.8.0	3.1.0-24	3.1.1-18	3.1.1-18[4]
4.7.2	2.1.8-39		
4.6.1	2.1.8-38		

[1] The Collector component and the Profiler Server **must** run the same version of the Cisco NAC Profiler software to inter-operate (for example, 3.1.1-18).

[2] Each version of the NAC Server software is shipped with a default version of the Profiler Collector component starting from Cisco NAC Appliance release 4.1.2.1 and later. The Profiler Collector can be upgraded independently of the NAC Server software for compatibility with a later Profiler Server/Profiler Lite Server release.

3. You must upgrade the Collector component on each NAC Server as described in Installing New/Upgrading Cisco NAC Profiler Collector Service on Cisco NAC Server, page 48.
4. You can only perform a new installation of NAC Profiler 3.1.1-18 or perform an upgrade from release 3.1.0 to 3.1.1-18. If you are running release 2.1.8-xx, you must first upgrade your system to release 3.1.0 before upgrading to release 3.1.1-18. See Upgrade Instructions for Release 3.1.1-18, page 42, for details.

Cisco NAC Profiler Collector Support and NAC Server Deployment Modes

The Cisco NAC Profiler system can be deployed in the following two primary modes:

1. Integrated with Cisco NAC Appliance. In this mode, the NAC Profiler Collectors run as:
   - An additional software service on Cisco NAC Servers.
   - The Cisco NAC Servers on which this service runs are part of an operational Cisco NAC Appliance solution.
   - The Cisco NAC Appliance solution is one in which Cisco NAC Manager and NAC Servers provide posture and remediation.
2. Not integrated with Cisco NAC Appliance. In this mode, the Profiler Collectors run:
   - On the Cisco NAC Servers, but the difference is that the Cisco NAC Manager is not present and the Cisco NAC Appliance system is not used for posture or remediation.
   - In this mode, the Cisco NAC Profiler system provides endpoint discovery, profiling, and identity monitoring.
   - The endpoint directory is enabled for LDAP access that allows other systems (for example, Cisco Secure ACS) to use the Cisco NAC Profiler as an external database for MAC Authentication/MAC Authentication Bypass (MAB).

The Collector service running on the NAC Server is composed of the NetMap, NetTrap, NetWatch, NetInquiry, and NetRelay component modules that collect endpoint data, and the Forwarder module that provides communication between the NAC Collector service running on a NAC Server and the Profiler Server. Depending upon deployment type, there are other considerations regarding Profiler Collector deployment that are outlined in the following sections.

Cisco NAC Profiler Integration with Cisco NAC Appliance Deployments

In this Cisco NAC Profiler deployment type, the NAC Server operating mode determines considerations for the Profiler Collector running on the NAC Server. Table 2 details the product features supported for each of the endpoint data collection modules based on NAC Server operating mode.

A *Yes* in the column for each of the operational modes in the following table indicates that the collection function is available and lists caveats with notes. *Selective* indicates that the collection function is available, but is subject to certain limitations as outlined in the notes.

Table 2 NAC Profiler Collector Modules and Cisco NAC Appliance Server Operating Mode

	Clean Access Server Operating Mode			
NAC Profiler Collector Module / Function	Real-IP Gateway	Virtual Gateway	Real-IP Gateway OOB	Virtual Gateway OOB
NetMap SNMP polling of switches and routers	Yes	Yes[1]	Yes	Yes [1]
NetTrap Receive SNMP traps from switches	Yes	Yes [1]	Yes	Yes [1]
NetWatch [2] • Observe traffic on eth2 (if not used for HA heartbeat) • Observe traffic on eth3 **Note** Interfaces eth0 and eth1 on CAS/Collector are not supported for Profiler Netwatch.	Yes [3] Yes	Yes [3] Yes	Yes [3] Yes	Yes [3] Yes
NetInquiry Active Profiling of endpoints	Yes	Yes[1]	Yes	Yes [4]
NetRelay Reception of NetFlow Export Data Records	Yes	Yes [1]	Yes	Yes [1]

1. The CAS/Collector in Virtual Gateway (bridged) mode can reliably contact endpoints/devices via the "untrusted" interface (eth1). However, a Virtual Gateway CAS/Collector cannot communicate with any Layer 2-adjacent device with the exception of its own default gateway via the "trusted" interface (eth0). This means the Virtual Gateway CAS cannot talk to, via its eth0 interface:
   -- any host connected to a trusted-side VLAN that is declared in the VLAN mapping table
   -- any host connected to a configured trusted-side CAS management VLAN
   -- any host connected to the trusted-side native VLAN (i.e. non-tagged traffic being bridged by the Virtual Gateway CAS)

   As long as the trusted-side target device is not Layer 2-adjacent, then the CAS can communicate with the device reliably via the eth0 interface. The target device must be separated from the CAS on trusted side by one or more Layer3 routing hops.

   The use of dedicated management VLANs for switches and routers (but not the same VLAN as the CAS management VLAN) is a general network engineering best practice that removes this concern for the purposes of both NetMap and NetRelay Collector component modules (and also NetInquiry, for Virtual Gateway In-Band only. For NetInquiry with Virtual Gateway OOB, see [4]).
2. The NetWatch Collector component module is used to observe endpoint behavior through targeted analysis of network traffic "sniffed" from various sources via any available network interface on the CAS/Collector. However NAC Profiler Collector functionality must coexist with CAS functionality. Therefore, not all of the CAS Ethernet interfaces can be used for general purpose monitoring (as detailed in the following notes). NetWatch is typically used:
   -- To sniff endpoint traffic via a switch-based port or VLAN monitoring mechanism ("SPAN" or similar), with network traffic directed to the eth3 interface (and/or eth2, for a standalone CAS - see [3]).
3. When the CAS is deployed as a high availability (HA) pair, eth2 is typically used for the UDP HA heartbeat connection. When eth2 is used for HA, eth2 is not available for NetWatch. For this reason, Cisco recommends using the eth3 interface of the CAS for general purpose traffic monitoring in most cases.
4. For Virtual Gateway OOB deployments, NetInquiry on the NAC Profiler Collector can actively profile endpoints while they are in the untrusted state. When an endpoint becomes OOB connected to an access VLAN, NetInquiry is NOT able to actively profile this endpoint while it remains in this state IF (and only if) the access VLAN is in the CAS VLAN Mapping Table (see [1]). If the endpoint becomes OOB connected via an access VLAN that is not in the VLAN Mapping Table (such that the endpoint is no longer Layer 2 adjacent to the CAS) then NetInquiry can continue actively profiling this endpoint.

Standalone Cisco NAC Profiler (not Integrated with Cisco NAC Appliance)

Even when the Cisco NAC appliance-specific Cisco NAC Server services are not enabled, the NAC Profiler Collector can operate in a standalone deployment mode and use the operating system and the underlying configuration of the NAC Server to continue performing endpoint data collection operations.

The Cisco NAC Profiler in either standalone or HA modes can function independently of how the Cisco NAC appliance in configured. The Cisco NAC Profiler can be integrated into either of these modes. The Cisco NAC Profiler standalone or HA modes are determined based upon how the Cisco NAC Profiler devices are configured.

To perform a minimum configuration of the NAC Server, see the following sections:

- Perform the Initial CAS Configuration; for a complete description, see the *Cisco NAC Appliance Hardware Installation Guide, Release 4.8* at: *http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/48/48hwinstal.html*
- Startup of NAC Profiler Collectors; for a complete description, see the *Cisco NAC Profiler Installation and Configuration Guide, Release 3.1.1* at: *http://www.cisco.com/en/US/products/ps8464/products_installation_and_configuration_guides_list.html*

Supported Web Browsers for Release 3.1.1

Release 3.1.1 of the Cisco NAC Profiler User Interface (UI) has been tested thoroughly with Windows® Internet Explorer® Versions 7 and 8, and Firefox® 3.0.x and later.

Note While efforts have been made to extend support back to Windows Internet Explorer Version 6.0.2900.2180.xpsp_sp2_qfe.080814-1242, it is recommended that you use Windows Internet Explorer Version 7, and Firefox Version 3.0.x for optimal UI performance.

Determining the Software Release Version

You can determine the release version for the following Cisco NAC Profiler components:

- Cisco NAC Profiler Server
- Cisco NAC Profiler Collector (on Cisco NAC Server)

Cisco NAC Profiler Server

Via the UI

- Navigate to the Home Tab (System Dashboard). The Cisco NAC Profiler Modules table of the System Status area of the dashboard indicates the Profiler Server version in parentheses following the Server link.

Via SSH

- SSH to the Profiler Server and type **service profiler status.** For example:

```
[root@profiler ~]# service profiler status
```

```
Profiler Status
   Version: Profiler-3.1.1-18

  o Server      Running
  o Forwarder   Not Installed
  o NetMap      Not Installed
  o NetTrap     Not Installed
  o NetWatch    Not Installed
  o NetInquiry  Not Installed
  o NetRelay    Not Installed
```

Cisco NAC Profiler Collector (on Cisco NAC Server)

- SSH to the NAC Server machine running the Collector service and type **`service collector status`**.

```
[root@bcas1 beacon]# service collector status

Profiler Status
   Version: Collector-3.1.1-18

  o Server      Not Installed
  o Forwarder   Running
  o NetMap      Running
  o NetTrap     Running
  o NetWatch    Running
  o NetInquiry  Running
  o NetRelay    Running
```

Product Change Information

This section describes enhancements made to this release of the Cisco NAC Profiler:

- Enhancements in Cisco NAC Profiler Release 3.1.1, page 9

Enhancements in Cisco NAC Profiler Release 3.1.1

Cisco NAC Profiler release 3.1.1 is a maintenance release that contains a number of bug fixes and minor enhancements to existing functionality. The Cisco NAC Profiler Release 3.1.1 is available as an **ISO** image for the Cisco NAC Profiler Server and Cisco NAC Profiler Lite or as an upgrade from release 3.1.0 to release 3.1.1.

The enhancements made in Release 3.1.1 of the Cisco NAC Profiler are detailed in the following sections:

- NAC Profiler Server Advanced Options, page 10
- Profiler Server based on NAC 3315, page 10
- Work Queue Size Option, page 10
- High Availability Pairs and Failover, page 10
- License File Sync, page 10
- LDAP Enhancements, page 11
- Factory Endpoint Profiles, page 11
- NetMap Polling of Network Devices and Active Directory Servers, page 11

Refer to the following sections for additional details regarding this release of the Cisco NAC Profiler:

- Caveats, page 11
- Open Caveats - Release 3.1.1-18, page 12
- Resolved Caveats - Release 3.1.1-18, page 32
- Upgrade Instructions for Release 3.1.1-18, page 42.

NAC Profiler Server Advanced Options

The NAC Profiler Server module now has relocated the configuration parameters to a new location on the Configure Server form labeled as Advanced Options:

- Work Queue Size
- Delay Collection
- Active Response Delay

For more details, see "Configuring the Cisco NAC Profiler Server" in the *Cisco NAC Profiler Installation and Configuration Guide, Release 3.1.1,* at: *http://www.cisco.com/en/US/products/ps8464/products_installation_and_configuration_guides_list.html)*

Profiler Server based on NAC 3315

NAC 3315 and 3355 Hardware platforms also supports NAC Profiler version 3.1.1-18 in FIPS 140-2 mode.

Work Queue Size Option

The NAC Profiler Server now provides a work queue size parameter in the Collector module that allows you to designate the size of messages that can be sent from the Collectors to the Cisco NAC Server module, in kilobytes.

For more details, see "Configuring Collector Modules" in the *Cisco NAC Profiler Installation and Configuration Guide, Release 3.1.1*, at: *http://www.cisco.com/en/US/products/ps8464/products_installation_and_configuration_guides_list.html)*

High Availability Pairs and Failover

The NAC Profiler now supports the capability to force a NAC Profiler Server HA pair to failover. This means that you can now manually initiate the transfer of primary node duties to the secondary to ensure that the failover capability of the pair is fully operational.

For example, this capability is desirable should you want the HA system to be tested, or at anytime you want to determine whether to shift the Primary duties to the other appliance in the HA pair.

For more details, see "Using the Cisco NAC Profiler Server Command Line" in the *Cisco NAC Profiler Installation and Configuration Guide, Release 3.1.1*, at: *http://www.cisco.com/en/US/products/ps8464/products_installation_and_configuration_guides_list.html)*

License File Sync

Starting from version 3.1.1-18 for a Cisco NAC Profiler running HA, a "FO Bundle" license with the eth0 MAC ID of the Primary as well as the secondary can be uploaded on the active node and the license will be replicated to the passive or secondary node. Replication of the license file is asynchronous, and will not occur if license files are deleted or are uploaded through SCP to either of the appliances in the failover pair.

LDAP Enhancements

Performance and scalability enhancements made to the NAC Profiler integration layer now improve routine LDAP directory operations. Group implementation changes have improved the performance of directory operations for LDAP-enabled endpoint profiles containing a large number of endpoints.

To supplement this change, optimizing available caching options was also implemented. These LDAP enhancement changes are not visible in the user interface nor do they affect the configuration of the LDAP integration layer. In effect, these enhancements are transparent to users of the endpoint data using LDAP (for example, RADIUS server users).

Factory Endpoint Profiles

Enhancements to the Endpoint Profiles included with the 3.1.1 release now make administration easier. The factory profiles that are loaded at the time of installation are now organized into Profile Groups that allow for Profiles of endpoints of the same type to be viewed collectively.

Note This enhancement is only supported in new installations of the Cisco NAC Profiler, Release 3.1.1. The act of upgrading an existing system to Release 3.1.1 will not be able to benefit from having additional factory profiles or default profile groups being added.

Release 3.1.1 also included a minor change to the Profile Group implementation. In previous releases, endpoint profiles that were not assigned to a specific group were placed in the “uncategorized” group by default. In this release, this has now been changed to “ungrouped.” If you want to remove an Uncategorized default group, you can delete it using the UI. Upon deletion, all profiles that were in the Uncategorized group are now moved to Ungrouped upon deletion of the old default Profile Group.

NetMap Polling of Network Devices and Active Directory Servers

This release supports a user-selectable polling interval in the Server configuration that allows you to control the frequency of polling for Active Directory servers system-wide (the default is 120 minutes). By setting this value to 0 minutes, this causes the system to cease polling for Active Directory Servers.

Caveats

This section describes the following caveats.

- Open Caveats - Release 3.1.1-18, page 12
- Open Caveats in Documentation - Release 3.1.1-18, page 25
- Resolved Caveats - Release 3.1.1-18, page 32

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

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

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

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

Open Caveats - Release 3.1.1-18

For Cisco NAC Appliance caveats that impact Cisco NAC Profiler, refer to the “Caveats” section of the applicable version of the *Release Notes for Cisco NAC Appliance (Clean Access)* at: *http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html*

Table 3 List of Open Caveats (Sheet 1 of 13)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCtr22225	No	cleanaccess.conf displays CAM credentials in plain text. Cisco NAC Appliance - Clean Access Manager (CAM) credentials are stored in plain-text in the NAC Profiler. **Conditions** NAC Profiler Deployed with NAC Appliance integration. **Workaround** **1.** Create a special account/password with privileges restricted to the API for the NAC Profiler to use when interacting with the Cisco NAC Manager. This blocks them from using the GUI and requires experience/knowledge of the NAC API interface with normal system operations. **2.** It is possible to remove the file after the NAC Profiler integration is established on 3.1.1 systems with Cisco NAC Manager (CAM). **Note** **Apply Changes -> Update Modules** re-generates the file, so remove the file upon each full restart of the system as a workaround.
CSCta83480	No	Default Collector status 4.7.0 should not be “Could not find install file.” When using system collector status on an uninstalled NAC Server 4.7.0 (CAS) collector, the system prompts “could not find install file.” This is before configuring and starting collector. [root@cas3-3350-rachnar beacon]# rpm -q Collector Collector-2.1.8-38 [root@cas3-3350-rachnar beacon]# service collector status Could not find installation file This message needs to be changed to make it more understandable. Such as a warning that collector needs to be configured/started. A more user friendly output would be: Collector is not installed, please install using system collector config **Conditions** Checking collector status. **Workaround** None.

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

DDTS Number	Software Release- Cisco NAC Profiler Version 3.1.1-18	
	Corrected	**Caveat**
CSCsy84379	No	SNMP informs needed for Cat 6500 Profiler compatibility. NAC Profiler does not process SNMP informs in release 2.1.8 **Conditions** Access switch SNMP configuration. **Workaround** Access switch SNMP configuration should use traps not informs to send mac-notiification mib.
CSCsy37162	No	Debug trace needs detail levels. Debugging on collector or server gives little or no useful information for troubleshooting purposes. This is not a scalable approach for support in the field. The application needs to provide more detail in the form of standard log levels. 0--7 are standard, for example syslog: <0-7> Logging severity level 7-debug; debugging. Debugging messages (severity=7) 6-inform; informational. Informational messages (severity=6) 5-notif; notifications. Normal but significant conditions (severity=5) 4-warn; warnings. Warning conditions (severity=4) 3-err; errors. Error conditions (severity=3) 2-crit; critical. Critical conditions (severity=2) 1-alert; alerts. Immediate action needed (severity=1) 0-emerg; emergencies. System is unusable (severity=0) **Conditions** Observed in version 002.001(008.037) **Workaround** The collector does not offer field debug capabilities.
CSCsx42320	No	Profiler and Collector unable to communicate through NAT device. NAC Profiler and Collector can not communicate with each other between a NAT device. **Conditions** When a Profiler and Collector are connected between a NAT device, communication is not established. **Workaround** NAT breaks the communication and should be moved to a Non-Nat setup between Collector and Profiler.

Table 3 List of Open Caveats (Sheet 3 of 13)

DDTS Number	Software Release- Cisco NAC Profiler Version 3.1.1-18	
	Corrected	**Caveat**
CSCsv91750	No	NacProfiler - xml configuration file protected by a signature. The configuration file is not secure and susceptible to get changed manually. The goal is to have a protection mechanism on the file, as only the software can change it. It ensures the integrity of the file. Having a Digest+Signature at the end of each XML file increases product security by avoiding manual and unauthorized change in the config file. **Conditions** Observed in version 002.001(008.037) **Workaround** None.
CSCsy40430	No	Breadcrumbs do not match the actual category name sometimes. **Conditions** Observed in version 003.000(000.000). Click > Configuration > Accounts: Configuration > NAC Profiler Users is displayed for breadcrumbs. **Workaround** None. Cosmetic.
CSCsy37696	No	Mac osx Firefox and Safari clear endpoint message unclean formatting. When clearing endpoint the system prompts, "Are you sure you want to clear this Endpoint? All current information about this endpoint in the endpoint database will be removed. History information will be retained should the endpoint be rediscovered. Click OK to permanently remove this endpoint." **Conditions** Using OS X Firefox 3.0.7 & Safari. **Workaround** Use Windows IE6 or Firefox 3.0.7 if you want to see it right, operationally it does not matter.
CSCsz73384	No	Service collector status lists profiler status. Lists collector status as profiler status. **Conditions** Observed in version 003.000(000.000). On CAS collector - service collector status. **Workaround** None, cosmetic issue.

Table 3 List of Open Caveats (Sheet 4 of 13)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCta97229	No	Collector Modules show "Stopping" instead of "Stopped" in Profiler UI. When the collector is stopped manually, the Profiler UI "Table of Collectors" shows status of "All modules Stopped". However, the collector services (such as NetMap, NetTrap, NetWatch) always remain in Stopping state. They never change to reflect "Stopped" state even upon waiting or clicking Refresh. **Conditions** Profiler/Collector 2.1.8.39. Stopping collector manually. **Workaround** The services are actually stopped (can do a service collector status on the CAS).
CSCsw30875	No	NAC Profiler license is not included in the CCA evaluation bundle. The Clean Access evaluation license does not include the NAC Profiler and Collector licenses. **Conditions** Request for NAC evaluation license in order to evaluate NAC Profiler and Collector. **Workaround** The current workaround is to provide the customer with manually generated licenses, after asking the customer for the appliance MAC address (the other NAC evaluation licenses are not bound to a specific MAC).
CSCtn27257	No	Profiler GUI shows CSV Import success for devices even if import fails. Profiler GUI reports successful import of network devices even if import fails due to format or other issues. **Conditions** Observed in version 003.001(001.000). Data import from CSV file in improper format. **Workaround** dberrlog log to show an insert error stating syntax is wrong.
CSCti25311	No	When doing "Clear Endpoint" page should navigate back to Table of Profile" NAC Profiler GUI should navigate back to "Table of Profile Name" or the Clear Endpoint should be disabled, but navigation still remains same and Clear Endpoint is enabled. **Conditions** GUI does not refresh back or move away in version 3.1.x. **Workaround** None. Need to navigate manually.

Table 3 List of Open Caveats (Sheet 5 of 13)

DDTS Number	Software Release- Cisco NAC Profiler Version 3.1.1-18	
	Corrected	**Caveat**
CSCti16784	No	NAC Profiler not able to profile netflow traffic. The NAC Profiler ignores Netflow summary packets when the IP address is not known for the end-point. **Conditions** Netflow summary packets are forwarded to the NAC collector to be used as a network layer profiling method for the endpoint. The Netflow summary packets contain network and transport layer information of the endpoint, which includes the source/destination IP address and port number. However, since the IP to MAC mapping is not know to the Profiler, the Netflow summary packets are being dropped and not profiled. This occurs when Netflow is the only network layer profiling method. **Workaround** None.
CSCsl59431	No	Devices in L3 IB NAC deployments cannot be added/removed from filterlist. Devices in L2 can be added to the filter list, removed from the filter list--based on their profile information; as the profiler can call addmac or removemac API calls towards CAM. But, if these devices are at L3 and IB is the mode of CASs, then Profiler has to use addip/removeip type of APIs to add IP addresses to the IP filter list. This is not currently done for L3 IB devices. IP address is missing from the CAM when populated via addMac from the profiler: CAM GUI - device management - filters - list. This is because the profiler call to the CAM is not using the parameter for the device IP address. If the IP address is available, you should try to populate the listing as an added feature to the customer. Tested with 4.5 and 4.1.3.1 CAMs using 2.1.8-37 profiler. **Conditions** L3 inband removal of devices via IP address. **Workaround** None. This is not a supported feature.

Table 3 List of Open Caveats (Sheet 6 of 13)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCtn17418	No	Profiler can not see 2950 VLANs via SNMP When using device provisioning on the NAC Profiler, the Profiler can not obtain the VLAN information from a Cisco 2950 switch. The switch is configured for basic SNMPv1 communities. Configuration -->Network Devices --> Add Infrastructure Device. Once the 2950 is contacted, if you then go to Display Endpoints by Network Infrastructure Device Ports and then manage the 2950, the VLAN information is not available. **Conditions** NAC Profiler 3.1.1 or earlier. Cisco 2950 switch which runs 12.1(22)EA14 or earlier **Workaround** Remove the network device from the group and set the individual switch settings accordingly.
CSCtg62414	No	RNE from CDETs_On Primary Profiler appliance under /backup folder .dump files increase drastically in size when HA subsystem on Profiler is non functional. **Conditions** In Cisco NAC Profiler version 2.1.8-x or even with latest 3.1 Profiler code, it is a known behavior for Profiler to output .dump files in /backup folder which is ideally to be used as backup and also for DB sync between Primary and Secondary Profilers. In particular situation of HA subsystem of Profiler, when synchronizing DB from primary to secondary it is observed that .dump files in /backup directory of "Primary Profiler" increase in size with days of HA subsystem being non functional. Ideal size of .dump files is ~60-100MB, but anything higher ~800MB is a direct indication that DB is not being synchronized on HA pairs. **Workaround** To check if HA subsystem is working fine: 1. One of the best ways to detect issues on the heartbeat network that will be the precursor to DB sync failure is monitoring the /usr/beacon/logging/HAPing.out. This is an error log that logs failures of HAPing. Nothing in HAPing out is an indication that all is well on the heartbeat network. 2. more /var/log/messages | grep heartbeat Heartbeat messages can be monitored for error conditions using that technique. Any issue with HA should be resolved by removing and then re-adding HA configuration as mentioned in document very elaborately. Issue with HA has to be resolved at the earliest as .dump file size might consume all of hard disk space on Primary Profiler causing it to be non responsive to SSH, Profiling.

Table 3 List of Open Caveats (Sheet 7 of 13)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCtg62424	No	RNE from CDETs_psql: FATAL: sorry, too many clients already. **Conditions** Error observed in 2.1.8-x version of NAC Profiler appliances in Server.out logs. This essentially suggests that there are too many open connections to Beacon DB and they have to be closed. One possible issue could be that HA subsystem on Profiler pair is non functional and/or some of the scripts have opened connections to DB and have not closed. **Workaround** None.
CSCsr58170	No	The CAS service collector status should not list the server module status as “not installed”. **Conditions** The CAS Collector does not include a server module, only the NAC Profiler includes this module. **Workaround** None. This should not be listed on the CAS Collector status output. **Note** This does not affect the function of the NAC Collector.

CSCsr91618	No	The Profiler service status lists the services not supported on the NAC Profiler server. The NAC Profiler status shows all the modules for the NAC Collector that will never be running or be installed.
		Conditions Forwarder, NetMap, NetTrap, NetWatch, NetInquiry, or NetRelay will never be installed or supported on the NAC Profiler server so they should not be listed in its status:
		`[root@profiler1 ~]# service profiler status`
		`Profiler Status`
		`   Version: Profiler-2.1.8-37`
		`  o Server      Running`
		`  o Forwarder   Not Installed`
		`  o NetMap      Not Installed`
		`  o NetTrap     Not Installed`
		`  o NetWatch    Not Installed`
		`  o NetInquiry  Not Installed`
		`  o NetRelay    Not Installed`
		Workaround None.
		Note This does not affect the function of the NAC Profiler Server.

Table 3 List of Open Caveats (Sheet 8 of 13)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCti28260	No	The NAC Profiler restarts its services every minute. **Conditions** This issue can be seen if the directory containing the licenses for the NAC Profiler includes an extra entry or the directory is one that the NAC Profiler is not able to parse (for example, `/usr/home/beacon/.lmlic`). It is also possible that this issue may occur in the `/usr/beacon/working/flexlm` directory. **Workaround** Remove all non-license entries from the license subdirectory of the NAC Profiler.
CSCsu46348	No	The NAC Profiler UI NAC roles should use an API call to populate the listing. NAC roles should be populated using a query instead of manually typing them in the NAC Profiler server config—this reduces the chance of error with user input and increases the ease of use for customers. **Conditions** This occurs during the entry of NAC roles. **Workaround** Carefully performing a manual entry of roles.
CSCsy37604	No	The NAC Profiler does not verify that the Collector and Profiler versions running are the same. **Conditions** The Collector version should be running the same version as the NAC Profiler. **Workaround** Verify that the version of Collector software matches the version running on the NAC Profiler. You can use the NAC Profiler UI to view the versions of the Collector service running on each Collector and the version running on the NAC Profiler.
CSCth26878	No	An issue with invalid characters in the NAC Profiler profile name can cause the Cisco NAC Profiler database to not start up properly. **Conditions** This has been caused by invalid non-alphanumeric characters used in profile names. **Workaround** Rename the profiles using supported alphanumeric characters.

Table 3 List of Open Caveats (Sheet 9 of 13)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCth94818	No	The NAC Profiler displays wrong endpoint VLAN identifier when the VLAN is changed by access switch (Authenticator) via dynamic VLAN assignment. Using Profiler UI > Endpoint Console > View/Manage Endpoints > Display Endpoints by Profile does not display correct VLAN information when the endpoint is enabled with 802.1X/MAB authentication. **Conditions** VLAN assignment is used for dynamically assigning an access switch port to a policy-controlled VLAN for each authenticated supplicant. When the supplicant is authenticated, the switch-port VLAN is changed from the port-assigned VLAN to the dynamically-assigned VLAN defined on the RADIUS server. When the access port is updated with the dynamically-assigned VLAN, the NAC Profiler does not update the endpoint VLAN identifier. The VLAN displays the default port-assigned VLAN or a zero. **Workaround** None.
CSCth96702	No	Active Response port disable, bounce, and re-authentication will not be working properly in NAC Profiler if the location information (switch IP address and port information) is not present. The location information is a mandatory requirement for NAC Profiler because this is needed to handle race conditions in profile creation to trigger the appropriate events. **Conditions** Normally, during the Cisco NAC Profiler event delivery methods (**Configuration > NAC Profiler Events > Edit Event**), as soon as NAC Profiler learns endpoint details, it should fire off the following events: • Active Response • Disable Port • Bounce Port • Re-authenticate (Cisco switches) The error is with the re-authentication process. The NAC Profiler needs to be configured such that re-authentication is triggered only when the endpoint is moved from one to another NAC Profiler. **Workaround** There is no current workaround.

Table 3 List of Open Caveats (Sheet 10 of 13)

DDTS Number	Software Release- Cisco NAC Profiler Version 3.1.1-18	
	Corrected	**Caveat**
CSCth97458	No	When a profile matches more than one NAC event, this cause NAC synchronization to behave erratically. While this is happening, devices that are profiled and should be added to the CAM filter list may not be added to the CAM as a result. **Conditions** For example, if you have a profile name of "Cisco IP Phone" and two NAC events with filter strings of "/IP Phone/i" and "/Cisco IP Phone/i", the profile will match both of these events. In the Server.out log, you will see a NAC sync start, but there will be be no NAC sync end. Something similar to the following error will occur: NAC_SYNC: CCA Event Rule Configuration Conflict: profile 'Cisco IP Phone' is matched by more than one CCA Event Rule. At a minimum, the following CCA Event Rules are involved: • IP Phone • Cisco IP Phone **Workaround** You need to modify the filter so that only one profile can match any one NAC event. For instance, using this example, change the first regex string to "/^IP Phone/i" so that it will match only those profiles that start with "IP Phone". Cisco NAC event names are wild card entries, which should match specific wild card event names.
CSCth84633	No	The Admin UI in NAC Profiler allows a NAC Collector name to exceed the 24-character limit. **Conditions** The NAC Profiler UI should validate the NAC Collector name and limit or truncate any name that exceeds 24 characters in length. **Workaround** There is no current workaround.

Table 3 List of Open Caveats (Sheet 11 of 13)

DDTS Number	Software Release- Cisco NAC Profiler Version 3.1.1-18	
	Corrected	**Caveat**
CSCtg22772	No	The endpoint is correctly modeled and the Active Response event is triggered. However, NAC Profiler 3.1.0 release was unable to bounce, disable, or re-authenticate the switch port. Under the even summary, the switch IP and port information is shown as 0.0.0.0/0. **Conditions** Related conditions can include the following: • Under some conditions (network/switch behavior), the NAC Profiler 3.1.0 release receives the NetWatch information on DHCP a few milliseconds (MS) before the TrapReport information for SNMP. • As a result of this timing issue, this causes new endpoints to be profiled and events to be triggered before getting the switch IP and port information via TrapReport. So, this means it is without the data it needs to perform an Active Response event (bounce, disable, or re-authenticate) on the witch ports. • The switch learns the MAC on the port, adds it to its FDB which will in turn generates a MAC Notification trap (this is done via the “slow path”, which requires switch CPU interaction). • As the DHCP discover is forwarded by the switch (“fast path”) it is seen by NetWatch. The DHCP discover reported to the server by NetWatch results in the Profiler discovering the endpoint and profiling it simultaneously (because the DHCP VCI rule is the one used in the endpoint profile). This also cause the New Endpoint event to trigger. • As the endpoint is discovered by NAC Profiler, it is also being modeled into the endpoint profile, which triggers the event immediately upon the modeler action initiated upon receipt of the DHCP information from NetWatch. • This results in the DHCP discover triggering the endpoint profile and the event even before the NAC Profiler is able to get the switch IP and port info via SNMP. **Workaround** None.

Table 3 List of Open Caveats (Sheet 12 of 13)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCti29950	No	The secondary high availability (HA) configuration is failing with the following error: ERROR: invalid input syntax for type timestamp: "Tue Aug 10 09:05:06.603466 2010 IDT". **Conditions** The Cisco NAC Profiler HA setup configured with NTP of Asia, Israel (IDT) rounds. **Workaround** Perform the following: 1. Remove the HA (/root/.resetProfiler removeHA). 2. Change the time zone to be for example, US or CSET on each member (service profiler setupntp). 3. Attempt to join the HA (service profiler setupha).
CSCti13583	No	When looking at the licensing page of the Cisco NAC Profiler in an HA setup, a green check is displayed for the local Profiler but a red x is displayed for the remote Profiler and Collector, even when valid licenses are uploaded. These are display characteristics only and do not affect Cisco NAC Profiler operations. **Conditions** Cisco NAC Profiler in an HA setup mode. **Workaround** This is only a display characteristic. No action required.
CSCti13604	No	If a NAC Profiler is connected to a HA set of NAC Collectors and they experience a failover, there is a minimal delay period before reconnection is made between the NAC Collector and the NAC Profiler. This is caused because the CAS is in a secondary mode and its eth0 is shutdown so no traffic is passed through until it resumes its active state. When this resumes, the NAC collector again shows its status as running. **Conditions** Can occur when NAC Collectors are running in an HA mode. **Workaround** This is a minimal recovery period (one minute or less).

Table 3 List of Open Caveats (Sheet 13 of 13)

DDTS Number	Software Release- Cisco NAC Profiler Version 3.1.1-18	
	Corrected	**Caveat**
CSCti03181	No	NAC Profiler does not seem to emulate the condition that previously known devices have not been heard from. **Conditions** This issue can occur because the NAC Profiler has a 'certainty' mechanism that reduces confidence that a device matches against any previously matched profile over a period of time. This is intended to handle devices that have not responded for some length of time. By adjusting the date on a NAC Profiler server, you can emulate the condition that previously known devices have not responded for a period of time (for example, a week, a month, etc.). This could be a previously profiled endpoint (such as an HP Printer) that has been disconnected for a number of days. **Workaround** There is no current workaround.
CSCts98131	No	NAC Profiler HA does not work with all timezones as their NTP sources. After configuring HA on NAC Profiler, if WIT or some of the other timezone formats are used, HA on profiler is known to have issues during replication to secondary node. **Workaround** Use only GMT or UTC as NTP timezone on the NAC Profiler for the NTP and HA to work properly. Use the command `service profiler setupntp` to make changes to the NTP setttings on an HA Profiler installation.
CSCtu16631	No	NAC Profiler MAC Address Rule Allows Unlimited Characters. NAC Profiler DB has a limit of 24 characters. While adding a rule, the number of characters added in the MAC Address are not automatically limited. Anyway, the string is truncated to 24 characters when saved.

Open Caveats in Documentation - Release 3.1.1-18

Table 4 List of Open Caveats - Documentation

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCtl66972	No	Profiler 3.1.1 guide does not document OUI update feature. Profiler 3.1.1.18 introduced a feature to update the vendor OUIs from the internet with a script. This needs to be documented. **Workaround** [beacon@BeaconHA1 ~]$ cd /usr/beacon/scripts/maint [beacon@BeaconHA1 /usr/beacon/scripts/maint]$ ls altBuild.php bundle convertLog.pl restoreDB-HA.pl rmNetDev.pl beacondb.gz check.sh ouiUpdate.pl restoreDB.pl setHTPass.php [beacon@BeaconHA1 /usr/beacon/scripts/maint]$ ./ouiUpdate.pl Downloading the OUI file... Please Wait... Validating OUI file... Please Wait... Found a total of 14165 entries. Please type 'list' to see the new entries or 'replace' to replace your current OUI table with the new one: replace Updating the Profiler's Database... Please Wait... The update is complete. [beacon@BeaconHA1 /usr/beacon/scripts/maint]$ New feature in 3.1.1, does not have any dependency on 3.1.1--you could copy the script from a 3.1.1 system to a 3.1.0 system.

Table 4 List of Open Caveats - Documentation (continued)

DDTS Number	Software Release- Cisco NAC Profiler Version 3.1.1-18	
	Corrected	**Caveat**
CSCtk99552	No	NAC profiler certificate type and conversion. OpenSSL on NAC Profiler appliance can convert different encoding types to PEM. Though this is not Profiler specific feature, including this information in the configuration guide helps customers (and Cisco as well) to easily convert certificates to PEM in order to get the profiler up and running. In chapter "Configuring Cisco NAC Profiler for the Target Environment" under section "Importing a Digitally Signed SSL Certificate onto the Cisco NAC Profiler System" add: **Note** The certificates must be encoded in PEM. If the profiler and/or CA chain certificates are in different formats, they must be converted. This can be done from the Profiler server CLI, by logging in as root: openssl <current encoding> -print_certs -in <current certificate name> -out <output name> To verify that the profiler certificate is valid and signed by a CA somewhere in the chain certificate bundle: openssl verify -CAfile <chain certificate> <profiler certificate>" **Workaround** Convert the certificates to PEM. This can be done from the Profiler server CLI, by logging in as root: openssl <current encoding> -print_certs -in <current certificate name> -out <output name>

Table 4 List of Open Caveats - Documentation (continued)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCte93969	No	NAC profiler does not update the complete MAC address list on the CAM. Full synchronization between the NAC profiler and CAM does not happen properly. Individual MAC address entries make it through to the CAM filer list. The following sync error is seen: NAC_SYNC: unexpected error -- timeout on stderr at /usr/lib/perl5/site_perl/5.8.8/IPC/Session.pm line 93. **Conditions** Keyless ssh works but the ssh config file has referenced a banner file that has no trailing EOL **Workaround** RNE suggests that when configuring Banner is on CAM, when you want interoperability with the profiler, you need to make sure the EOL is at every line and the end of the doc. The trailing EOL can be introduced by opening the banner file with VI editor and saving it. Other Linux editors might allow a file to be saved without an EOL **Workaround** It can be easily corrected on the customer's system with the following steps (on both NAC Manager nodes): 1. Log in as root 2. Open in 'vi' editor -- vi banner.pre 3. Save file by typing ":wq" 4. (renable banner) Edit /etc/ssh/sshd_config and un-comment last line ("Banner ...")-- write changes 5. Restart ssh service -- service sshd restart
CSCta06865	No	Profiler Documentation does not cover configuring Failover NAC Managers. The Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8 section "Integration with Cisco NAC Appliance" does not cover how to add failover NAC managers to the NAC Profiler. RNE from CDETs suggests the need to add the DNS/IP of the CAM VIP and secondary (comma separated) in the Profiler server config Address field. **Conditions** NAC Profiler 2.1.8 **Workaround** Add the Manager Service IP/DNS Name followed by the Secondary Manager IP/DNS Name and separate them by a comma.

Table 4 List of Open Caveats - Documentation (continued)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCtj15872	No	RNE from CDETs_Password recovery procedure for 2.1.8-x and 3.1.x versions of Profiler. Procedure to set a new password for root for 2.1.x NAC Appliance. **1.** Press any key during the GRUB Loading message **2.** Select appropriate kernel (mostly there is only one) and press e: **3.** Select the kernel boot line (typically the second line) and press e: **4.** Add capital S at the end of the line **5.** Press Enter and verify your edit **6.** Press b to boot into Single User mode **7.** Use passwd to set a new root password at the prompt **8.** Once the password is set, use shutdown -r now to reboot **9.** Type "passwd beacon" from root and press Enter **10.** Enter the Beacon user password and press Enter **Note** Ignore messages that password is short or a dictionary word **11.** Retype password when prompted press Enter Procedure to set a new password for root on a 3.x and above NAC Appliance. **1.** Boot the appliance and press 4 at the boot option menu **2.** Enter the path to the shell you wish to use for single user mode session or press Enter for default (bourne shell) **3.** Use mount -u / followed by mount -a to mount the root file system (this must be done for the password to take) **4.** Use passwd to set the root password, at the command line prompt **5.** Use the sync command (issued as sync;sync) to make sure the new password is written to disk **6.** Use reboot OR shutdown -r now to reboot the system
CSCtd37697	No	NAC Collector 3.1 on a Cisco NAC 4.6.1 gets downgraded when the Cisco NAC is upgraded to 4.7.1. When a user upgrades the Cisco NAC Profiler including the Profiler Collector to 3.1 in Cisco NAC 4.6.1, followed by upgrading the NAC 4.6.1 to 4.7.1, it overwrites the Collector 3.1 with Collector 2.1.8.39. **Workaround** After upgrading NAC 4.6.1 to 4.7.1, you must manually upgrade the Profiler Collector 2.1.8.39 to 3.1, because Cisco NAC Profiler Collector 2.1.8.39 comes bundled in NAC 4.7.1.

Table 4 List of Open Caveats - Documentation (continued)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCtg65296	No	NAC Profiler 3.1.0 and later releases do not retrieve VLAN information for Cisco 4500 switches that are configured for NAC out-of-band (OOB). **Conditions** The following conditions need to be met: • Profiler needs to query the OID .1.3.6.1.4.1.9.5 so it can retrieve the VLAN information from the Cisco 4500 switches. • The MIB CISCO-SMI containing this OID .1.3.6.1.4.1.9.5 is supported only on certain images of the Cisco 4500 switches. See the following: *http://tools.cisco.com/ITDIT/MIBS/AdvancedSearch?ReleaseSel=0&PlatformSel=94&fsSel=0&mibIdArr=4623&totalPages=14226&totalNoOfImages=-1&pgSelect=1* • IOS 12.2(23) is the latest code version that supports the CISCO-SMI MIB, and in turn, the OID .1.3.6.1.4.1.9.5. • However, Cisco 4500 switches are supported in NAC out-of-band (OOB) starting from 12.2(31)SGA02. See the following for details: *http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/switch_spt.html#wp40017* **Workaround** None.
CSCti30635	Yes	NAC Profiler licensing guide recommends using upper case MAC addresses when generating a license. **Conditions** The Cisco NAC Appliance Service Contract/Licensing Support documentation incorrectly states that “When entering the MAC address to generate the license, you must enter all upper case hexadecimal characters.” Because the licenses are case-sensitive, licenses for the Cisco NAC Profiler and Collector must be generated with lower case MAC(s). When entering the MAC address to generate the license, you must enter all lower-case hexadecimal characters. **Workaround** None.

Table 4 List of Open Caveats - Documentation (continued)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCsw97514	No	Unable to delete a NAC Collector from the Cisco NAC Profiler. An error displays that indicates that the NAC Collector does not exist in the database. **Conditions** If you enter a Collector name when initially configuring the service that exceeds 24 characters in length, the name is truncated when added to the database. This results in a mismatch between what is displayed in the UI and what is stored in the database, which prevents the NAC Collection from being deleted. **Workaround** Manually delete the Collector from the Profiler database. 1. SSH to the Profiler Server as user 'beacon'. 2. Enter the following command at the prompt: echo “delete from beacon_component where name LIKE '<*collector name as it appears in the UI*>’;” | psql

Table 4 List of Open Caveats - Documentation (continued)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCtg57780	No	Events are triggered even without any switch IP and port information. **Conditions** Profiler can correctly bounce, disable, or re-authenticate a port through an Active Response only when receiving switch IP and port information before an event is triggered. This is done only when SNMP data is received before DHCP data by the Profiler. However, if DHCP information is received before the SNMP data, it could cause the following scenarios to occur: • When the switch learns the MAC on the port, adds it to its FDB, this in turn, generates a MAC Notification trap (done using the "slow path" that requires CPU interaction). As DHCP discover is forwarded by the switch ("fast path") and seen by NetWatch. DHCP discover is reported to the server by NetWatch which results in the Profiler discovering and profiling the endpoint simultaneously (due to the use of DHCP VCI rule for endpoint profiles). This also triggers a New Endpoint event. • When the endpoint is discovered by the Profiler it is also being modeled into an endpoint profile that triggers an event immediately upon the modeler action initiated on receipt of DHCP information from NetWatch. The DHCP discover triggers an endpoint profile and an event even before the Profiler is able to get the switch IP and port information via SNMP. • As a result, an Active Response event could be fired without any switch IP and port information. Thus, not allowing the Profiler to bounce, disable, or re-authenticate the switch port. The order of receipt of the data by the Server is important here. If the NetWatch/DHCP data used for discovery, profiling, and event triggering precedes the NetTrap location information, the system does not have a valid location (switch and port) at the instant the endpoint is profiled. Hence, it cannot fire the event. However, by the time the NAC Profiler UI is checked, the location information has already been received and stored in the database, so that it falsely appears that the location information was known. This means that the switch IP and port information in the event summary may not appear because at the time the event was triggered, that information had not yet been received via SNMP. This may cause a condition for example, when a non-PoE device (PC, printer, etc.) plugged into a switch interface is (re)booted. The switch will first forward first the DHCP traffic, and next the SNMP traps. Because only after an IP is tied to the MAC address does the switch send out SNMP notification. Consequently, the NAC Profiler cannot support Active Response events with devices that are (re)booting. **Workaround** None.

Resolved Caveats - Release 3.1.1-18

Table 5 List of Resolved Caveats (Sheet 1 of 9)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCsw70560	Yes	NAC Profiler configuration guide page 9-4 LDAP AAA list incorrect **Workaround** Replace Cisco ACS or Juniper with Cisco Secure ACS or comparable AAA server.
CSCtl94426	Yes	Document needs to clarify what MAC addresses should be in the Profiler/Collector licenses. **Conditions** If it is Profiler HA, the Collector license needs to contain 2 MAC addresses (no matter if it is Collector HA or Stand alone): One of the eth0 of the Primary Profiler; the other is eth0 of the Secondary Profiler. **Workaround** License File Sync -Starting from version 3.1.1-18 for a Cisco NAC Profiler running HA, a "FO Bundle" license with the eth0 MAC ID of the Primary as well as the secondary can be uploaded on the active node and the license is replicated to the passive or secondary node. Replication of the license file is asynchronous, and does not occur if license files are deleted or are uploaded through SCP to either of the appliances in the failover pair."
CSCtl51096	Yes	Profiler document needs to document that eth0/eth1 are not Supported for NetWatch. **Conditions** This may be related to issues running NetWatch on eth0/eth1 interface. Still an open issue-run NetWatch on eth2/3 interface. **Workaround** Document that eth0 and eth1 are not supported for Profiler NetWatch. Since this is applicable to all current Profiler versions, update the equivalent documents for all releases.
CSCtc34810	Yes	Endpoint location data is not displayed when trunk port info is received. **Conditions** If Profiler receives data that indicates the endpoint (a single mac address) is seen on two ports, such as a physical port and a trunk port, no information is displayed for the endpoint. **Workaround** There is a patch released for this and same will be the workaround.

Table 5 List of Resolved Caveats (Sheet 2 of 9)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCtd69946	Yes	In the CAM Device Filter list (integrated to Cisco NAC Profiler), upon clicking on the Profiler link in the Description field, the user cannot login to the profiler to view the summary information for the endpoint. **Conditions** No display of the endpoint summary in CAM Device Filter List if browsing through Internet Explorer. **Workaround** Right click on the profiler link and chose **Open link in new window** or **Open link in new tab** to view the Profiler summary information.You can also use Mozilla Firefox browser for this purpose.
CSCte41353	Yes	SNMP Session Reauthentication is not working. **Conditions** When the re-authentication event is triggered, the NAC Profiler has insufficient information about the authentication session on the switch to carry out the operation via an SNMP set. This issue is specific to Cisco NAC Profiler Release 3.1. **Workaround** Download **Patch-CSCte41353-K9.zip** from *http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438162*, and apply this patch on NAC Profiler/Collector 3.1.0 version.
CSCte93435	Yes	The Profiler MAC Address OU database is outdated for HP MAC address. **Conditions** New HP Printer MAC addresses are not being recognized by Profiler because the OU database does not have the entries. **Workaround** None.

Table 5 List of Resolved Caveats (Sheet 3 of 9)

DDTS Number	Software Release- Cisco NAC Profiler Version 3.1.1-18	
	Corrected	**Caveat**
CSCsy03646	Yes	There was an issue with the Cisco NAC Profiler HA license requirements. Based on CCO documentation it is not clear which License files are required for Profiler HA/Collector HA setup. See the following: *http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/license.html#wp39197* • For Cisco NAC Profiler or Cisco NAC Profiler Failover (HA) licenses, submit the eth0 MAC address of the Primary Profiler Server. • For Cisco NAC Profiler Failover (HA) license only, submit the eth0 MAC address of the secondary Profiler Server. *http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/license.html#wp39086* • A Profiler Server license—installed on the Profiler Server • A Profiler Collector license for each CAS Collector— installed on the Profiler Server. • Failover Profiler Server (based on NAC-3350) - for HA pair. **Conditions** Profiler HA / Collector HA setup. **Workaround** One Profiler HA LIC file with MAC address primary Profiler eth0 and secondary Profiler eth0.
CSCtb17189	Yes	Profiler incorrectly sets switch ports connecting endpoints other than IP Phones using CDP as trunk ports in the Cisco NAC Profiler UI. Cannot view endpoints on trunk ports in UI. **Conditions** In 2.1.8 version, automatic trunk detection was excluded only on ports that registered CDP Platform Type containing the string 'phone.' Endpoints using CDP Platform Type not containing phone would be marked as trunk ports in the UI. **Workaround** None. **Note** 3.1.0 version requires administrator configuration of CDP Trunk Exclusion parameter of Profiler Server module to exclude CDP Platform Types in addition to the default of 'phone.'.
CSCsl20917	Yes	The installed licenses are not displayed. **Conditions** When displaying the Admin UI - Upload Licenses, the installed licenses are not displayed. **Workaround** Check the file via the CLI at the following location: /usr/beacon/working/flexlm

Table 5 List of Resolved Caveats (Sheet 4 of 9)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCsl21160	Yes	Profiler Admin session should Logout after timed interval. The Cisco NAC Profiler GUI Admin logged in never is logged out. **Workaround** None.
CSCte60976	Yes	Trap Handling for v2c traps are INOP for version 4.7.1 of the CAS/Collector Only. Older versions of SNMP Research in the CentOS build used for Cisco NAC Appliance Release 4.7.1 result in NetTrap being unable to determine the IP address of the trapping agent. **Conditions** This issue is specific to Cisco NAC Profiler Release 3.1 when integrated with Cisco NAC Appliance Release 4.7.1. **Workaround** Download **Patch-CSCte60976-K9.gz** from *http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438162*, and apply this patch on the Cisco NAC Profiler/Collector 3.1 version.
CSCsm72012	Yes	Need SSL import/export certificate GUI tab for the Profiler. Profiler needs to have an import/export utility for SSL certificates on the Profiler GUI. **Workaround** None.
CSCsq34147	Yes	The primary NAC Profiler shows database errors on Endpoint Console. The standby NAC Profiler displays Unknown DB Error on the Endpoint Console page. **Conditions** Cisco NAC Profiler running 2.1.8-37 in a failover pair. This will only show up on the standby Profiler. **Workaround** Nothing specific, this is a display issue. **Further Problem Description** The Active Profiler has the secondary database locked. When the secondary endpoint console page is brought up it tries to write to the database, but is denied. This error will not affect the operation of the Profilers.

Table 5 List of Resolved Caveats (Sheet 5 of 9)

DDTS Number	Software Release- Cisco NAC Profiler Version 3.1.1-18	
	Corrected	**Caveat**

CSCsq42942	Yes	Cisco NAC Profiler: secondary NAC Profiler shows License Error.
		The secondary Profiler in a failover pair will display a license error for the Collector licenses installed on the server since they were generated with the primary Profiler's MAC address.
		Conditions Cisco NAC Profilers running in a failover pair. This is only seen on the secondary Profiler. This was observed in 2.1.8-37.
		Workaround None, this is a display issue and will not affect the operation of the Profilers.
		Further Problem Description
		Example error:
		`INFO: [2008-05-02 15:48:44 (fcapGetHWAddr:91)] Retrieving`
		`HWAddr for eth0 ERROR: (FlexLM): Unknown MAC ->XXXXXXXXXXXX`
		`ERROR: (FlexLM): No match found in ->`
		`[<Count>2</Count><PrimaryMAC>YYYYYYYYYYYY</PrimaryMAC>]`

CSCsu29905	Yes	Cisco NAC Profiler SNMP trap receive does not check community string. Cisco NAC Profiler NetMap Collector solution is unable to verify network device (switch) snmp trap community string. Operationally the solution is processing endpoints and correctly profiling. **Conditions** Any SNMP (v1, v2c) trap sent community string. **Workaround** None.
CSCsu46247	Yes	Cisco NAC Profiler GUI allows duplication of Collector entry. A Collector with the same name and IP address can be created as a duplicate in the Cisco NAC Profiler GUI. **Conditions** When a Collector of the same info already exists. **Workaround** None.
CSCsu46273	Yes	Cisco NAC Profiler GUI needs the ability to set time and NTP information. Currently, there is no way to set the time using the GUI. **Workaround** The time must be set through the Linux CLI and there is a procedure for how to setup NTP (requires HA setup to be uninstalled when doing this). This document is out of the scope of the defect. The current system time is now shown on the Home tab and when viewing the system log from the Utilities tab.

Table 5 List of Resolved Caveats (Sheet 6 of 9)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCsu46311	Yes	Cisco NAC Profiler GUI does not display IP or name of active Profiler. When you click on the Config - Cisco NAC Profiler modules - List Config - Server server it displays Server Name: Server. The CLI name shows machines profiler1 and profiler2, but this is not shown nor the actual IP config on the boxes using the GUI. **Workaround** None.
CSCsv66296	Yes	Changes of Collector NetWatch config corrupt network block formatting. The formatting of the network block is corrupted and saving the config gives an error (example 172.16.17.0/24172.16.18.0/24 is not a IP v4 Address). **Conditions** Removing/adding/editing the NetWatch interface under the Collector configuration and then saving the Collector. **Workaround** Fix the blocks before saving the configuration or return to the configuration and correct it.
CSCsu46247	Yes	A NAC Collector with the same name and IP can be created as a duplicate in the Cisco NAC Profiler UI without warning the user. **Conditions** Adding Collectors to the Cisco NAC Profiler configuration, no validation that the Collector Name already exists. **Workaround** None.
CSCtg99187	Yes	During the process of querying, Profiler 3.1.1 now adds cn=user to the Active Directory (AD) user. **Conditions** A patch was released to address this issue for customers with NAC Profiler 3.1.0-24. Release 3.1.1 of the Cisco NAC Profiler has resolved this issue. **Workaround** None.
CSCth25337	Yes	In Profiler 3.1.0 and earlier releases, high availability (HA) setups can encounter database corruption if the active database is rapidly “flipped” back and forth between servers. **Conditions** Reboot or shutdown of the NAC Profiler is not consistent in NAC Profiler 3.1.0 and earlier releases as these release encountered issues withe the database sync and the NAC Profiler service not starting up properly. A patch was released patch for NAC Profiler 3.1.0, and this was and resolved in NAC Profiler 3.1.1. **Workaround** The same “graceful” HA commands added to the NAC Profiler service CLI in 3.1.1 are also available in the 3.1.0 patch.

Table 5 List of Resolved Caveats (Sheet 7 of 9)

DDTS Number	Software Release- Cisco NAC Profiler Version 3.1.1-18	
	Corrected	**Caveat**
CSCth43163	Yes	When using the DNS Zone Transfer feature in NAC Profiler 3.1.0 release code, retrieving an IPv6 DNS entry could cause the NAC Collector to be unable to send the DNS entries to the NAC Profiler. **Conditions** When any IPv6 entries were found in a reverse DNS lookup, this would cause the NAC Profiler to stall. **Workaround** This issue was resolved in release 3.1.1. However, in the 3.1.0 release, IPv6 entries need to be removed manually.
CSCth43091	Yes	NAC Profiler release 3.1.0 encounters an issue with large DNS tables in which the collector correctly polls the DNS table, but is unable to send the table to the profiler. There is a hard-coded limit at 1 megabyte (MB). **Conditions** For better performance in release 3.1.0, on CAS the limit for DNS tables was set to 1 MB only. The limit is on work queue size for communication between the NAC Collector and the NAC Profiler via TCP port 31416. **Conditions** Starting with release 3.1.1, the number of endpoints that NAC Profiler can now support has been increased, and there is a configurable work queue size on the NAC Profiler UI under collector configuration (Configuration--> click on collector name--> Forwarder- “Work Queue Size”).
CSCtc84603	Yes	The Profiler does not purge old entries from the database, even after the timers have expired and regardless of timer settings used. **Conditions** This has been observed and reported on NAC Profiler, release 2.1.8-38. **Workaround** None.
CSCsx97856	Yes	The software version in the Profiler and Collector CLI and GUI views should reflect the same version (for example, both should show as r_6). The problem reflects the Profiler GUI version in 3.0 displaying one version (3.0.0r.6), while the CLI version for the NAC Profiler and Collector displays another version (3.0.0r_6). **Conditions** There was a mismatch in the versions displayed in the GUI and the version showing up using CLI commands. ny workarounds. **Workaround** None. This issue has been resolved in release 3.1.1.

Table 5 List of Resolved Caveats (Sheet 8 of 9)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCtd02716	Yes	An industry-wide vulnerability exists in the Transport Layer Security (TLS) protocol that could impact any Cisco product that uses any version of TLS and SSL. The vulnerability exists in how the protocol handles session renegotiation and exposes users to a potential man-in-the-middle attack. **Conditions** An advisory is posted at the following location: *http://www.cisco.com/warp/public/707/cisco-sa-20091109-tls.shtml* Consult the advisory.
CSCtg50546	Yes	CDP-based profiling for IP phones may not work as expected, due to some known issues. **Conditions** The issues were with NAC Profiler release 3.1.0-24. **Workaround** It is recommended that you change to DHCP-based profiling for the IP phones until NAC Profiler release 3.1.1 is available.
CSCsy37604	Yes	The NAC Profiler does not verify whether the NAC Collector version is different from the version it is running. **Conditions** This can occur when the NAC Profiler and NAC Collector are running different versions of the supported software. **Workaround** Ensure that all NAC Collectors are running the same version of the software running on the NAC Profiler.
CSCth45393	Yes	Some devices may fail to be profiled despite the correct information about these devices having been received by the NAC Profiler. **Conditions** In NAC Profiler release 3.1.0, profiling was based only on the MAC notification trap. **Workaround** It is recommended that you uncheck the Trust Cisco MAC Notification Trap option on the server module of the NAC Profiler UI, and perform an Apply Changes.
CSCsx62489	Yes	An issue exists with the 2.1.8.x and 3.0.0 versions of the Cisco NAC Profiler and Collector. When setting up a collector using the service collector configuration, set the default encryption type to 'none', which should default to AES for security and match the server config defaults. Check the NAC Profiler UI that the server defaults to AES (Configuration > NAC Profiler Modules > List Modules > Server > Add Network Connection). **Conditions** When configuring the NAC Collector, use service collector config. **Workaround** Enter the type in which you want to match.

Table 5 List of Resolved Caveats (Sheet 9 of 9)

	Software Release- Cisco NAC Profiler Version 3.1.1-18	
DDTS Number	**Corrected**	**Caveat**
CSCth39950	Yes	A condition existed where the first installed NAC 3355 appliance in an earlier release was installed and it detected the ports as: port 1 as eth0 and port 2 as eth1. A subsequent installation using the NAC Profiler ISO image detected these port interfaces in the reverse order. This caused network issues when the NAC Profiler did not correctly recognize the order of the interfaces. **Conditions** This condition has been resolved. **Workaround** None.
CSCsw97514	Yes	An error occurred because of an inability to delete a NAC Collector from the NAC Profiler. This error indicates that the NAC Collector does not exist in the database. **Conditions** The NAC Controller version is 2.1.8-37 and the NAC Collector name exceeded the 24-character length limit. **Workaround** A manual workaround exists for deleting the NAC Collector from the NAC Profiler database. To do this, perform the following: • SSH to the NAC Profiler server as user ‘beacon’. • Enter the following command at the prompt: ‘<*collector name as it appears in the UI*>%;’ | psql **Note** The database field for the NAC Collector name is limited to 24 characters in length. The NAC Profiler UI currently does not check the length of the user input for this value. If a name exceeds the 24-character limit, it is truncated to that length when entered into the database.
CSCth58694	Yes	An issue occurred when attempting to grab Active Directory (AD) data for a large number of AD users that exceeded the 1MB limit, which caused data to be discarded on the NAC Collector without alerting user. **Conditions** Active Directory data collected exceeded the 1 MB limit. **Workaround** None.

New Installation of Cisco NAC Profiler Release 3.1.1-18

The following section describes the process for performing a new installation of the Cisco NAC Profiler software (3.1.1-18) required for the Cisco NAC Profiler and Profiler Lite appliances. The files required for installing Cisco NAC Profiler Release 3.1.1-18 are available from Cisco Secure Software at:

- *http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438162*

The software installation files for performing a new installation of Cisco NAC Profiler and Profiler Lite appliances are:

- **Profiler-3.1.1-18-iso-md5sum.txt**–This is a 128-bit MD5 hash checksum file (defined in RFC 1321) that verifies the file's digital fingerprint and integrity as having not changed as a result of file transfer or disk error.
- **nac-collector-3.1.1-18-K9.rpm**–This is the NAC Collector RPM that is loaded onto the NAC Server (CAS) to upgrade the NAC Collector component.
- **nac-profiler-3.1.1-18-K9-iso**–This is the ISO installation file for the Cisco NAC Profiler appliance.
- **nac-profilerlite-3.1.1-18-K9.iso**–This is the ISO installation file for the Cisco NAC Profiler Lite appliance.

You must log in using your Cisco.com registration user name and password to download these files.

Cisco NAC Profiler Server and Cisco NAC Profiler Lite Server

If performing a new CD installation/upgrade of the Cisco NAC Profiler software on the Cisco NAC Profiler Server or Cisco NAC Profiler Lite Server or HA pair that has yet to be configured/deployed, use the steps described below.

For upgrade of an operational Cisco NAC Profiler system running version 2.1.8, refer to the instructions in Upgrade Instructions for Release 3.1.1-18, page 42 in order to retain all system configuration and data.

Note The Profiler Lite appliance platform is supported starting from release 2.1.8-37 and requires a separate ISO file. Only the **nac-profilerlite-3.1.1-18-K9.iso** file can be installed on the Profiler Lite platform. See Hardware Supported, page 2 and Software Compatibility, page 3 for details.

Step 1 Follow the instructions on your welcome letter to obtain a license file for your installation. See *Cisco NAC Appliance Service Contract/Licensing Support* for details. (If you are evaluating Cisco NAC Profiler, visit *http://www.cisco.com/go/license/public* to obtain an evaluation license.)

- Log into the Security Software download site for Cisco NAC Appliance and download the latest Cisco NAC Profiler version 3.1.1 ISO image from: *http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438162*
- For the standard NAC Profiler Server, download the latest **nac-profiler-3.1.1-18-K9.iso**.
- For the NAC Profiler Lite, download the latest **nac-profilerlite-3.1.1-18-K9.iso**.

Step 2 Burn the ISO as a bootable disk to a CD-R.

Step 3 Insert the CD into the CD-ROM drive of the appliance that the NAC Profiler Server/Profiler Lite Server is to be installed on, and reboot the appliance to start the ISO process.

Step 4 Follow the on-screen instructions to complete a "standard" (for example, no custom keyword) ISO of the NAC Profiler Server or Profiler Lite Server appliance, or appliances in the case of high availability (HA) configuration of Profiler Server appliances. Once the ISO installation completes, the appliance ejects the ISO CD and boots to the root prompt. It is now in the same state as a new NAC Profiler Server or Profiler Lite Server would be shipped from the factory with version 3.1.1-18 installed.

Step 5 Upgrade the Profiler Collector component on each Clean Access Server to the appropriate version as described in Installing New/Upgrading Cisco NAC Profiler Collector Service on Cisco NAC Server, page 48.

Step 6 See "Installing and Performing an Initial Configuration" in the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1.1 for complete installation and configuration instructions for installing new Cisco NAC Profiler systems.

Upgrade Instructions for Release 3.1.1-18

This section provides instructions to upgrade operational Cisco NAC Profiler systems that are running the earlier supported release (3.1.0-24) to this release, 3.1.1-18.

- **nac-profiler_upgrade-3.1.1-18-K9-iso–**This is the ISO upgrade file required for upgrading to this release of the Cisco NAC Profiler software.

Note Only a new installation of NAC Profiler release 3.1.1-18 software or an upgrade from release 3.1.0 to 3.1.1-18 is supported. If you are running an earlier release (for example, 2.1.8-xx), you must first upgrade your system to release 3.1.0 before upgrading to release 3.1.1-18.

Note To support Cisco NAC Profiler release 3.1.1-18, the NAC Server(s) must already be configured and running the latest supported Cisco NAC Appliance release as described in Software Compatibility, page 3. The Profiler Collector component must also be upgraded on the NAC Server to the corresponding version as described in Software Compatibility, page 3 and Installing New/Upgrading Cisco NAC Profiler Collector Service on Cisco NAC Server, page 48.

Note The Profiler Lite appliance platform is supported starting from release 2.1.8-37 and requires a separate ISO file. Only the **nac-profilerlite-3.1.1-18-K9.iso** file can be installed on the Profiler Lite platform. See Hardware Supported, page 2 and Software Compatibility, page 3 for details.

The upgrade instructions for the Profiler Server include both standalone and HA-pair configurations, and the following sections provide these instructions:

- Upgrading 2.1.8 Cisco NAC Profiler Server and Cisco NAC Profiler Lite Server Standalone Systems to 3.1.0-24, page 43
- Upgrading Cisco NAC Profiler Systems from 3.1.0 to 3.1.1, page 43
- Installing New/Upgrading Cisco NAC Profiler Collector Service on Cisco NAC Server, page 48

Caution Cisco strongly recommends performing a database backup and moving the backup file off-appliance before you begin the upgrade process.

Note You must complete the upgrade for all Profiler Servers and Profiler Collectors in the system to bring all components up to the most current version.

Upgrading 2.1.8 Cisco NAC Profiler Server and Cisco NAC Profiler Lite Server Standalone Systems to 3.1.0-24

Two conditions require that early releases (2.1.8) of the Cisco NAC Profiler and Profiler Lite Server systems be upgraded to release 3.1.0-24 before these systems can be upgraded to Release 3.1.1-18:

1. The operating system of the Cisco NAC Profiler Server system changed in version 3.1.0, requiring systems running 2.1.8 to undergo a complete reinstallation of the NAC Profiler Server software to successfully upgrade to release 3.1.0.
2. There are only two supported methods for installing Cisco NAC Profiler and Profiler Lite release 3.1.1-18 system software on Cisco NAC Server appliances:
   - A new installation of the release 3.1.1-18 software.
   - An upgrade of earlier releases to release 3.1.0-24, and then an upgrade to release 3.1.1-18. This requires migrating the 2.1.8 database forward to release 3.1.0 compatibility.

For information about database migration and upgrading the Cisco NAC Profiler and Profiler Lite Servers release 2.1.8 to release 3.1.0-24, see "Upgrading 2.1.8 Cisco NAC Profiler Server and Cisco NAC Profiler Lite Server Standalone Systems to 3.1.0" in the *Release Notes for Cisco NAC Profiler, Release 3.1.0* at:*http://www.cisco.com/en/US/docs/security/nac/profiler/release_notes/310/310rn.html*.

Upgrading Cisco NAC Profiler Systems from 3.1.0 to 3.1.1

Warning **The 3.1.1 upgrade package requires the Cisco NAC Profiler system to be upgraded and running release 3.1.0 before proceeding with this upgrade to release 3.1.1. The release 3.1.1 upgrade will check the current version of the Cisco NAC Profiler running on the system and will terminate without completing the upgrade if the running version is other than release 3.1.0.**

Tip If the system to be upgraded is not running release 3.1.0, refer to Upgrading 2.1.8 Cisco NAC Profiler Server and Cisco NAC Profiler Lite Server Standalone Systems to 3.1.0-24, page 43.

Upgrading existing Cisco NAC Profiler systems running release 3.1.0 can be performed so that most existing configuration and system data is seamlessly migrated forward as the system is upgraded to release 3.1.1 using the provided upgrade package and without requiring any ISO re-imaging of the appliances.

Note The only configuration of the release 3.1.0 Cisco NAC Profiler system that is not migrated forward automatically by the upgrade is that required for RADIUS authentication of Cisco NAC Profiler UI users. If the release 3.1.0 system is currently authenticating UI users via RADIUS, the parameters in the Cisco NAC Profiler configuration (RADIUS server DNS/IP address and shared secret) will have to be re-entered by the Administrator and saved to the configuration post completion of the upgrade to release 3.1.1.

For distributed Cisco NAC Profiler systems (for example, one or more NAC Collector appliance(s), upgrade the Cisco NAC Profiler Server appliance hosting the server module for the Cisco NAC Profiler system first before upgrading the NAC Collector appliance(s). The upgrade procedure for Cisco NAC Profiler appliances is dependent upon the operating mode: standalone or HA-pair. The procedures for upgrading systems in both operating modes are provided in the following sections.

Upgrading Standalone Cisco NAC Profiler Systems (Release 3.1.0 to 3.1.1-18)

Upgrading the Cisco NAC Profiler software on standalone release 3.1.0 systems to release 3.1.1-18 is a process that uses an upgrade script that determines the operating mode of the system and upgrades all installed components automatically as needed.

This upgrade requires a reboot of the appliance following the upgrade of installed components that occurs near the midpoint of the upgrade process. Following the reboot, the upgrade script is called again to complete the process. Perform the following steps to upgrade standalone Cisco NAC Profiler systems.

Warning **The reboot occurs before the upgrade is completed. Following the reboot, the upgrade must be continued as described in the following procedure.**

Note Upgrading all-in-one or server only HA-pairs requires an HA-specific procedure, if you are upgrading an HA system proceed to Upgrading NAC Profiler Server HA Pairs (3.1.0 to 3.1.1-18), page 46.

Step 1 Back up the current database via the **Utilities-> System Summary-> Backup Database** button.

Step 2 Download the latest **nac-profiler_upgrade-3.1.1-18-K9.zip** upgrade package from the Cisco Secure Software website.

Tip After downloading this file from the Cisco Secure Software website, you can rename the file as desired. This procedure uses the release file name (**nac-profiler_upgrade-3.1.1-18-K9.zip**).

Step 1 SCP the **nac-profiler_upgrade-3.1.1-18-K9.zip** to the /home/beacon directory of the appliance to be upgraded.

Step 2 SSH to the system being upgraded, and elevate to root user using the command:

```
su -
```

Step 3 Change directory (**cd**) to /home/beacon.

```
cd /home/beacon
```

Step 4 Verify that the MD5 checksum of the upgrade package matches the checksum specified for the file on the Cisco Secure Software website. Use the following command to generate the checksum of the file on the target system, for example:

```
md5 nac-profiler_upgrade-3.1.1-18-K9.zip
```

This command calculates and displays the checksum of the file to the terminal on the appliance so it can be checked against the one displayed on the Cisco Secure Software website.

Step 5 Unzip the upgrade package, for example:

```
unzip nac-profiler_upgrade-3.1.1-18-K9.zip
```

This uncompresses the files required for upgrade, and creates a new subdirectory for /home/beacon (for example, named nac-profiler_upgrade-3.1.1-18).

Step 6 Change directory to the nac-profiler_upgrade-3.1.1-18 directory created when the upgrade package was unzipped, for example:

```
cd nac-profiler_upgrade-3.1.1-18
```

The directory should include a script named install.sh. Execute the upgrade script by entering the following command:

```
./install.sh
```

During the upgrade process, several messages may be sent to the terminal indicating progress of the upgrade as installed components are upgraded. When the update script completes the upgrading of the appliance OS, the appliance must be rebooted to restart the system utilizing the upgraded components. The following messages are displayed:

```
An intermediate reboot is required

Upon reboot, login in as the root user and re-run this upgrade script

Hit ENTER to reboot the appliance
```

Step 7 Press **Enter** to reboot the appliance. Wait for the reboot to complete then re-login to the appliance, and elevate to root access.

Step 8 Resume the upgrade scripts by calling the script in /home/beacon/nac-profiler_upgrade-3.1.1-18 again:

```
./install.sh
```

Step 9 The script will continue the upgrade process. At the completion of the upgrade script, verify the Cisco NAC Profiler software version of the appliance by observing the output of the command:

```
service profiler status
```

The output will include the full version of the Cisco NAC Profiler system including the build number (for example, Profiler-3.1.1_18), and should indicate the running status for the installed module(s) on the system.

Repeat steps 2 – 8 above on the other standalone Cisco NAC appliances in the system being upgraded to the selected 3.1.1 release.

Note When upgrading Cisco NAC Profiler Server systems integrated with Cisco NAC Appliance, the key-less SSH connection with the Cisco NAC Manager must be re-established after the upgrade to release 3.1.1.

Use the following command to re-establish the key-less SSH:

```
service profiler setupccakey
```

Failure to perform this step will result in the failure of NAC synchronization.

Upgrading NAC Profiler Server HA Pairs (3.1.0 to 3.1.1-18)

The procedure for upgrading the software on a HA-pair is performed on the **secondary node in the pair first**, and then on the primary. In the process of the upgrade, the system that was the secondary node prior to the upgrade will take over the functions of the primary node, similar to what would occur in the event of the failure of the primary.

Warning **Upgrading the Cisco NAC Profiler software on a HA pair must be completed on both members of the pair sequentially in a single operation. Do not leave the pair with the first appliance upgraded and delay the upgrade of the other member of the pair as the Cisco NAC Profiler system will not be functional in this state.**

Tip If it is desirable to return the HA pair back to its state previous to the upgrade, failover of the pair will be necessary to force the appliance that was primary node prior to the upgrade back to that state.

You can find the proper procedure for forcing an HA-pair to failover in the *Cisco NAC Profiler Installation and Configuration Guide, Release 3.1.1*, at: *http://www.cisco.com/en/US/products/ps8464/products_installation_and_configuration_guides_list.html*

Complete the following procedures to upgrade the Cisco NAC Profiler software on a HA pair.

Step 1 Back up the current database via the **Utilities-> System Summary-> Backup Database** button on the primary appliance.

Step 2 Download the latest **nac-profiler_upgrade-3.1.1-18-K9.zip** upgrade package from the Cisco Secure Software site.

Tip After downloading this file from the Cisco Secure Software website, you can rename the file as desired. This procedure uses the release file name (**nac-profiler_upgrade-3.1.1-18-K9.zip**) .

Tip SCP the upgrade package file to the /home/beacon directory of both members of the HA-pair.

Tip Use the eth0 interface IP addresses of both appliances in the pair, not the VIP when copying the upgrade package to the appliances, and when performing the upgrade.

Step 3 Determine which appliance is currently the secondary appliance in the pair using the procedure outlined in the *Cisco NAC Profiler Installation and Configuration Guide, Release 3.1.1*.

Step 4 SSH to the IP address of the eth0 interface on the secondary node in the pair, and change to the root user access using the `su -` command.

Step 5 Change directory to /home/beacon (`cd /home/beacon`), and verify the MD5 checksum of the upgrade package against the checksum specified for the file on the Cisco Secure Software website. Use the following command to generate the checksum of the file on the target system, for example:

```
md5 nac-profiler_upgrade-3.1.1-18-K9.zip
```

This command calculates and displays the checksum of the file to the terminal on the appliance so it can be checked against the one supplied with the file.

Step 6 Unzip the upgrade package (**nac-profiler_upgrade-3.1.1-18-K9.zip**), which uncompresses the files required for upgrade, and creates a new subdirectory (for example, named nac-profiler_upgrade-3.1.1-18) in the beacon/home directory.

Step 7 Change directory to the `nac-profiler_upgrade-3.1.1-18` directory created when the upgrade package was unzipped.

The new directory will include a script named install.sh. Execute the upgrade script by entering the following command:

```
./install.sh
```

During the upgrade process, several messages may be sent to the terminal indicating the progress of the upgrade as installed components are upgraded. When the update script completes the upgrade of the appliance OS, the appliance must be rebooted to restart the system utilizing upgraded components. The following messages are displayed:

```
An intermediate reboot is required

Upon reboot, login in as the root user and re-run this upgrade script

Hit ENTER to reboot the appliance
```

Step 8 Press **Enter** to reboot the appliance. Wait for the reboot to complete, then re-login to the appliance, and change to the root user.

Step 9 Resume the upgrade scripts by calling the script in /home/beacon/nac-profiler_upgrade-3.1.1-18 again:

```
/install.sh
```

Step 10 The script continues the upgrade process to completion. At the completion of the upgrade script, verify the Cisco NAC Profiler software version of the secondary node by observing the output of the following command:

```
service profiler status
```

The output includes the full version of the Cisco NAC Profiler system including the build number (for example., Profiler-3.1.1_18), and should indicate the running status for the installed module(s) on the system. This completes the upgrade of the software on the original secondary appliance.

Step 11 Proceed with performing the upgrade process on the appliance that was primary node at the beginning of the upgrade procedure by repeating steps #5-10 (substituting primary for secondary).

The original primary node will become the secondary node during this process, initiated by running the upgrade script on that appliance. The secondary node at the beginning of the upgrade that was upgraded to release 3.1.1 in the previous step now becomes the primary node for the pair maintaining availability of the system.

Step 12 Verify the successful upgrade of the system by entering the **`service profiler status`** command. The output will include the current version of the Cisco NAC Profiler system, and should indicate the status of the installed module(s) on the system which is now the secondary node.

Once the second appliance has been successfully upgraded, both members of the HA-pair are now at the 3.1.1-18 release state.

Note When upgrading Cisco NAC Profiler Server systems integrated with Cisco NAC appliance, the key-less SSH connection with the Cisco NAC Manager must be re-established after the upgrade to 3.1.1. Use the command `service profiler setupccakey` to re-establish key-less SSH. Failure to perform this step will result in the failure of NAC synchronization.

Installing New/Upgrading Cisco NAC Profiler Collector Service on Cisco NAC Server

New installations or upgrades of the NAC Profiler Collector service on a Cisco NAC Server to version 3.1.1 is accomplished via a single RPM file (**nac-collector-3.1.1-18-K9.rpm**). This RPM file for the NAC Collector gets loaded onto the Cisco NAC Server (CAS) for upgrading the Collector component.

The Profiler Collector RPM is a complete package that can be used to upgrade an existing NAC Collector service on a Cisco NAC Server to version 3.1.1. This RPM can also be used for a new installation on a Cisco NAC Server that does not have the NAC Collector service running on it. Use the following steps to upgrade or install the NAC Collector service on a Cisco NAC Server.

Note When upgrading the Collector service only on a NAC Server via this process, the existing configuration of the Profiler Collector remains intact. For new installations, the Collector service must be provided an initial configuration via the NAC Server CLI, using the **service collector config** command. See "Installing and Performing an Initial Configuration" in the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1.1 for complete instructions on starting up NAC Profiler Collectors.

Note Cisco NAC Appliance releases are shipped with a default version of the NAC Collector version. When upgrading the NAC Server to a newer appliance release, the current version of the NAC Collector is replaced with the default version of the NAC Collector shipped with the Cisco NAC Appliance release. For example, if you are running NAC 4.7.2 and Profiler 3.1.1-18 and you upgrade to NAC 4.8.0, you need to manually re-install the NAC Collector release 3.1.1 and configure it following the NAC Server upgrade.

Step 1 Download the latest Profiler Collector RPM file (that is **nac-collector-3.1.1-18-K9.rpm)** from the Cisco NAC Profiler Version 3.1.1 location on Cisco Secure Software website.

Note Prior to downloading, take note of the MD5 value in the Details table of the Software Download screens.

Step 2 SCP the file to the /home/beacon directory of the NAC Server(s) to be upgraded.

Note If the NAC Server/Collector is implemented as an HA pair, copy the upgrade file to both NAC Server appliances in the pair using the eth0 IP address for each NAC Server. Do not use the Service IP address of the HA-NAC Server pair.

Step 3 Initiate an SSH session to the NAC Server being upgraded and login as the root user using the root password.

Step 4 Run the following command to verify the MD5 checksum of the upgrade file against the one provided on the Cisco Software Download site:

```
md5sum nac-collector-3.1.1-18-K9.rpm
```

Step 5 Run the RPM file by issuing the following command to install or upgrade the NAC Collector service on the appliance. For NAC Server HA pairs, execute this command on both NAC Servers in the pair:

```
rpm -Uhv nac-collector-3.1.1-18-K9.rpm
```

Step 6 The RPM completes and the command prompt returns when it has completed successfully.

Step 7 For newly installed NAC Profiler Collectors, see “Installing and Performing an Initial Configuration” in the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1.1 for complete instructions on starting up NAC Profiler Collectors at:

http://www.cisco.com/en/US/products/ps8464/products_installation_and_configuration_guides_list.html

When upgrading operational NAC Profiler Collectors, complete the remaining steps in this section to restart the NAC Collector services on the new software version using the existing configuration.

Step 8 Issue the following command to restart the Collector service on the NAC Server.

```
service collector start
```

Step 9 Issue the ‘service collector status’ command to verify the version and check the status of the NAC Profiler Collector components which should indicate a status of “Running”, with the exception of the Server which indicates “Not Installed”.

```
[root@bcas1 beacon]# service collector status

Profiler Status
   Version: Collector-3.1.1-18

  o Server      Not Installed
  o Forwarder   Running
  o NetMap      Running
  o NetTrap     Running
  o NetWatch    Running
  o NetInquiry  Running
  o NetRelay    Running

[root@bcas1 beacon]#
```

For NAC Profiler Collectors running in HA mode on HA NAC Server pairs, Step 8 and Step 9 should be performed on both NAC Server appliances in the pair.

Step 10 Using the Cisco NAC Profiler UI, verify the upgraded Profiler Collectors show a status of “All Modules Running” in the System Status table of the **Configuration** tab.

Documentation Updates

Table 6 Updates to Release Notes for Cisco NAC Profiler, Release 3.1.1

Date	Description
November 16, 2011	• Added caveat CSCtu16631 to Open Caveats - Release 3.1.1-18, page 12. For details, see CSCtu16631, page 24
October 14, 2011	• Added caveat CSCts98131 to Open Caveats - Release 3.1.1-18, page 12. For details, see CSCts98131, page 24
March 24, 2011	• Added a note under Cisco NAC Profiler Lite section. • Added new caveats (see Open Caveats - Release 3.1.1-18, page 12). – CSCsl59431 (for details, see CSCsl59431, page -16). – CSCtn17418 (for details, see CSCtn17418, page -17). – CSCti16784 (for details, see CSCti16784, page 16). – CSCti25311 (for details, see CSCti25311, page 15). – CSCtn27257 (for details, see CSCtn27257, page 15). – CSCsw30875 (for details, see CSCsw30875, page 15). – CSCta97229 (for details, see CSCta97229, page 15). – CSCsz73384 (for details, see CSCsz73384, page 14). – CSCsy37696 (for details, see CSCsy37696, page 14). – CSCsy40430 (for details, see CSCsy40430, page 14). – CSCsv91750 (for details, see CSCsv91750, page 14). – CSCsx42320 (for details, see CSCsx42320, page 13). – CSCsy37162 (for details, see CSCsy37162, page 13). – CSCsy84379 (for details, see CSCsy84379, page 13). – CSCta83480 (for details, see CSCta83480, page 12). • Added new caveats (see Open Caveats in Documentation - Release 3.1.1-18, page -25). – CSCtl66972 (for details, see CSCtl66972, page -25). – CSCtk99552 (for details, see CSCtk99552, page -26). – CSCte93969 (for details, see CSCte93969, page -27). – CSCta06865 (for details, see CSCta06865, page -27). • Added new caveats (see Resolved Caveats - Release 3.1.1-18, page -32). – CSCsw70560 (for details, see CSCsw70560, page -32). – CSCtl94426 (for details, see CSCtl94426, page -32). – CSCtl51096 (for details, see CSCtl51096, page -32).

Table 6 Updates to Release Notes for Cisco NAC Profiler, Release 3.1.1

Date	Description
February 11, 2011	• Added new caveat (see Open Caveats - Release 3.1.1-18, page 12). – CSCtn17418 (for details, see CSCtn17418, page 17). • Updated Product Change Information (see Product Change Information, page -9) • Added new caveat (see Open Caveats - Release 3.1.1-18, page 12) – CSCtn17418 (for details, see CSCtn17418, page -17)
November 26, 2010	• Added new caveats (see Open Caveats - Release 3.1.1-18, page 12). – CSCtg62414 (for details, see CSCtg62414, page 17). – CSCtg62424 (for details, see CSCtg62424, page 18).
September 23, 2010	Cisco NAC Profiler Release 3.1.1-18 • Renamed section "New Features and Enhancements" to "Enhancements" (see Enhancements in Cisco NAC Profiler Release 3.1.1, page 9). • Changed caveat status to resolved for the following caveats (see Resolved Caveats - Release 3.1.1-18, page 32): – CSCsy37604 (for details, see CSCsy37604, page 39). – CSCsw97514 (for details, see CSCsw97514, page 40). • Added new caveat (see Open Caveats - Release 3.1.1-18, page 12). – CSCti28260 (for details, see CSCti28260, page 19).
August 17, 2010	Cisco NAC Profiler Release 3.1.1-18

Related Documentation

For the latest updates to Cisco NAC Profiler and Cisco NAC Appliance documentation on Cisco.com see: http://www.cisco.com/en/US/products/ps8464/tsd_products_support_series_home.html, or simply http://www.cisco.com/go/nac/appliance:

- Cisco NAC Profiler Installation and Configuration Guide, Release 3.1.1 *(http://www.cisco.com/en/US/docs/security/nac/profiler/configuration_guide/311/Profiler311I-C.html)*
- Release Notes for Cisco NAC Profiler, Release 3.1.1 *(http://www.cisco.com/en/US/docs/security/nac/profiler/release_notes/311/311rn.html)*
- License and Documentation Guide for Cisco NAC Profiler, Release 3.1.1 *(http://www.cisco.com/en/US/docs/security/nac/profiler/doc_roadmap/78-19566-01.html)*
- Release Notes for Cisco NAC Appliance *(http://www.cisco.com/en/US/docs/security/nac/appliance/release_notes/48/48rn.html)*
- Cisco NAC Appliance Hardware Installation Guide *(http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/48/48hwinstal.html)*
- Cisco NAC Appliance - Clean Access Server Configuration Guide *(http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/48/cas/48cas-book.html)*

- Cisco NAC Appliance - Clean Access Manager Configuration Guide *(http://www.cisco.com/en/US/docs/security/nac/appliance/configuration_guide/48/cam/48cam-book.html)*
- Cisco NAC Appliance Service Contract / Licensing Support *(http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/license.html)*
- Regulatory Compliance and Safety Information for Cisco 1121 Secure Access Control System, Cisco NAC Appliance, Cisco NAC Guest Server, and Cisco NAC Profiler *(http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_system/5.1/regulatory/compliance/csacsrcsi.html)*

Obtaining Documentation and Submitting a Service Request

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

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

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

This document is to be used in conjunction with the documents listed in the Related Documentation, page 51 section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2010 Cisco Systems, Inc. All rights reserved.