Release Notes for Cisco NAC Profiler, Release 2.1.8

Revised: November 4, 2009, OL-15634-01

Contents

These release notes provide late-breaking and release information for Cisco NAC Profiler, release 2.1.8. This document describes new features, changes to existing features, limitations and restrictions ("caveats"), upgrade instructions, and related information. These release notes supplement the Cisco NAC Profiler and Cisco NAC Appliance documentation included with the distribution. Read these release notes carefully and refer to the upgrade instructions prior to installing the software.

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

Cisco NAC Profiler Releases

Cisco NAC Profiler Version	Release Date
2.1.8-39 ED	November 4, 2009
2.1.8-38 ED	December 22, 2008
2.1.8-37 ED	April 7, 2008
2.1.8-33 ED	March 4, 2008

System Requirements

This section contains the following:

Licensing

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

Note Refer to CSCsk25865, page 36 for additional details.

Hardware Supported

The Cisco NAC Profiler system consists of a Cisco NAC Profiler Server appliance or Cisco NAC Profiler Lite appliance, and one or more Cisco NAC Profiler Collectors that run on the Clean Access Server appliances (NAC-3310/3315 or NAC-3350/3355) deployed as part of the Cisco NAC Appliance system.

The Cisco NAC Profiler Server appliances leverage the Cisco NAC Appliance 3350 and 3310 hardware platforms only.

Cisco NAC Profiler Server

The Cisco NAC Profiler Server appliance is based on the NAC-3350 hardware platform and is pre-installed with a default version of the Cisco NAC Profiler Server software.

Cisco NAC Profiler Lite

The Cisco NAC Profiler Lite appliance is based on the NAC-3310 hardware platform and is also pre-installed with a default version of the Cisco NAC Profiler Server software. Profiler Lite is supported starting from release 2.1.8-37 only and requires a separate ISO file. Refer to New Installation of Release 2.1.8, page 47 for details.

Cisco NAC Profiler Collector (on CAS)

A default version of the Cisco NAC Profiler **Collector** component is included as an RPM service on the Clean Access Server (CAS) appliance starting from Cisco NAC Appliance release 4.1.2.1 and later. The Clean Access Server operates on NAC-3310/3315 and/or NAC-3350/3355 SERVER Appliance platforms only.

Note For proper operation, both the Cisco NAC Profiler Collector component on the CAS and Cisco NAC Profiler appliance (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 3 for details.

Note You will need to upgrade the default version of the Collector shipped with the CAS software for compatibility with the latest Cisco NAC Profiler release 2.1.8. For details refer to Cisco NAC Appliance/ Cisco NAC Profiler Compatibility Matrix, page 3.

See New and Changed Information, page 6 for details on the latest release 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

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

Note To upgrade to the latest Cisco NAC Profiler 2.1.8 release, refer to Upgrade Instructions for Release 2.1.8, page 48.

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

Cisco NAC Server Appliance Components[2]			Cisco NAC Profiler Appliance
CAS Version	Collector Version Shipped with CAS	Upgrade Collector Version to: [3]	Upgrade Profiler /Profiler Lite[4] Version to:
4.7	2.1.8-39	-	2.1.8-39 [5]
4.6(1)	2.1.8-37	2.1.8-39 [6]	2.1.8-39 [6]

Table 1 Cisco NAC Appliance / Cisco NAC Profiler Compatibility Matrix [1] (continued)

Cisco NAC Server Appliance Components[2]			Cisco NAC Profiler Appliance
CAS Version	**Collector Version Shipped with CAS**	**Upgrade Collector Version to: [3],**	**Upgrade Profiler /Profiler Lite[4] Version to:**
4.5	2.1.8-37	2.1.8-38	2.1.8.-38 [7]
4.1(6)			
4.1(3)	2.1.8-3		
4.1.2.1	2.1.7-4 [8]		

1. The Collector component and the Profiler appliance **must** run the same version of the Cisco NAC Profiler software to inter-operate (e.g. 2.1.8-38).
2. Each version of the Clean Access Server (CAS) software is shipped with a default version of the Cisco NAC Profiler Collector component starting from Cisco NAC Appliance release 4.1.2.1 and later. The Collector can be upgraded independently of the CAS software for compatibility with a later Cisco NAC Profiler release.
3. You must upgrade the Collector component on each CAS as described in Upgrading Collector Service on CAS, page 53. The same version must be run on both the Collector and the Profiler Server for compatibility (e.g. version 2.1.8-39).
4. The Profiler Lite appliance platform is supported starting from release 2.1.8-37 and later and requires a separate ISO file. Only the **nac_profilerlite_2.1.8-37-K9.iso** file (or later) can be installed on the Profiler Lite platform. See Hardware Supported, page 2 and New Installation of Release 2.1.8, page 47 for more information.
5. Version 2.1.8-39 is available as a software upgrade only for Profiler Server and Profiler Lite. There is no ISO file. See Upgrade Instructions for Release 2.1.8, page 48 for details.
6. You can upgrade to 2.1.8-39 from either 2.1.8-37 or 2.1.8-38.
7. Version 2.1.8-38 is available as a software upgrade only for Profiler Server and Profiler Lite. There is no ISO file.
8. Cisco NAC Profiler release 2.1.8 replaces and supersedes release 2.1.7. If running Cisco NAC Profiler release 2.1.7, upgrade your Cisco NAC Profiler appliance and Collector components to the latest available supported 2.1.8 release build.

Collector Support and CAS Deployment Modes

The Cisco NAC Profiler Collector application resides on each Clean Access Server. The Collector application is composed of the following modules: NetMap, NetTrap, NetWatch, NetInquiry, NetRelay. Table 2 details the features supported for each Collector module for each Clean Access Server deployment mode. A 'Y' in the column for each of the operational modes indicates that the collection function is available with any caveats indicated by the note(s). 'Selective' indicates that the collection function is available but subject to certain limitations that are outlined in the notes.

Table 2 Collector Modules and NAC Appliance Server Operating Mode

	Clean Access Server Operating Mode			
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	Yes [3] Yes	Yes [3] Yes	Yes [3] Yes	Yes [3] Yes

Table 2 Collector Modules and NAC Appliance Server Operating Mode

Collector Module / Function	Clean Access Server Operating Mode			
	Real-IP Gateway	Virtual Gateway	Real-IP Gateway OOB	Virtual Gateway OOB
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 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]). Refer to CAS/Collectors Running in Real IP Gateway Mode, page 13 for additional information.
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 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.

Determining the Software Version

You can determine the version of Cisco NAC Profiler components as follows:

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

Cisco NAC Profiler Server Version

- SSH or Telnet to the Profiler Server and type **`rpm -q Profiler`**.

  ```
  [root@profiler2 ~]# rpm -q Profiler
  Profiler-2.1.8-39
  ```

- Or, for additional status, SSH or Telnet to the Profiler Server and type **`service profiler status`**. You will need to provide the root user password. For example:

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

  Profiler Status
     Version: Profiler-2.1.8-39
  ```

```
   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 Version (on CAS)

SSH or Telnet to the Clean Access Server machine running the Collector service and type **`service collector status`**.

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

Profiler Status
   Version: Collector-2.1.8-39

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

New and Changed Information

This section describes enhancements added to the following releases of Cisco NAC Profiler:

- Enhancements in Cisco NAC Profiler Release 2.1.8-39, page 6
- Enhancements in Cisco NAC Profiler Release 2.1.8-38, page 7
- Enhancements in Cisco NAC Profiler Release 2.1.8-37, page 9
- Enhancements in Cisco NAC Profiler Release 2.1.8-33, page 9

Enhancements in Cisco NAC Profiler Release 2.1.8-39

Build 39 of Cisco NAC Profiler release 2.1.8 added two new features addressing recent developments in the use of Web User Agents by applications. There are no bug fixes in the 2.1.8-39 release. Details on the features added to 2.1.8-39 are provided in the following sections:

- Endpoint Database Cleanup Utility, page 7
- NetWatch Filtering for Web User Agents, page 7

Refer to the following updated sections for additional details:

- Open Caveats - Release 2.1.8-39, page 21
- Open Caveats - Documentation, page 38
- Known Issues in Version 2.1.8, page 12
- CAS/Collectors Running in Real IP Gateway Mode, page 13
- Upgrade Instructions for Release 2.1.8, page 48.

Endpoint Database Cleanup Utility

Web User Agents and TCP Open Ports attributes of endpoint identity are collected for endpoints within the MyNetwork range cumulatively. Therefore a given endpoint may have multiple TCP Open Port and Web User Agent attributes collected for them and stored in the NAC Profiler endpoint database. In NAC Profiler systems that have been in operation for some time analyzing endpoint data flows via NetWatch, it may be desirable to purge collected web user agent and TCP Open Port data once the profile rules are well established to decrease database size and improve Modeler performance.

Version 2.1.8-39 adds a utility to purge unused TCP Open Port and Web User Agent endpoint data from the NAC Profiler endpoint database when executed by the administrator.

When the utility is run, it first determines the TCP Open Port and Web User Agents being used in enabled endpoint profiles. TCP Open Port and Web User Agent Data matching rules in enabled Endpoint Profiles are excluded from the purge so that no profile transitions occur as a result of using the database cleanup utility. Only data of this type that does not match a rule in any enabled profile is purged.

To run the database cleanup utility, follow the steps below:

Step 1 Navigate to the Utilities tab and select System Summary. The system summary page displays a Cleanup Database button, new to the 2.1.8-39 build.

Step 2 Click the Clean Up database button, which will display a warning dialog box confirming that the user wants to proceed with the deletion of Web User Agent and that TCP Open Port data not used in enabled Profiles will be permanently deleted from the database.

Step 3 Click OK to proceed with the cleanup. Successful execution of the cleanup is indicated by messages appearing in the UI confirming the cleanup of TCP Open Port and Web User Agent data.

NetWatch Filtering for Web User Agents

Version 2.1.8-39 adds a filtering capability specific to Web User Agent collection by NetWatch.

The NetWatch module configuration has a new parameter in the UI that allows the specification of a Regular Expression. Web User Agents collected by NetWatch that contain a matching string will **not** be forwarded to the Server for addition to the endpoint database. This feature provides a mechanism for excluding web user agent collection for some of the new streaming media players used by the network television websites for streaming of programming. These players can result in the collection of a very large number of Web User Agents for endpoints used to view streaming media from these sites which provides little value for profiling.

Entering a RegEx in the User-Filter Field of NetWatch modules collecting traffic will result in the discard of web user agents that match the RegEx.

Enhancements in Cisco NAC Profiler Release 2.1.8-38

Build 38 of Cisco NAC Profiler release 2.1.8 was a general and important bug fix release for the Cisco NAC Profiler that addresses the caveats described in Resolved Caveats - Release 2.1.8-38, page 29. Release 2.1.8-38 is available as a software upgrade only for the Profiler Server, Profiler Lite and Collector component on the CAS. No new features are added; however release 2.1.8-38 included the following enhancement:

- Endpoint and Directory Timeout Unified Into Endpoint Timeout, page 8

Refer to the following updated sections for additional details:

- Open Caveats - Release 2.1.8-39, page 21
- Open Caveats - Documentation, page 38
- Resolved Caveats - Release 2.1.8-38, page 29
- Known Issues in Version 2.1.8, page 12
- CAS/Collectors Running in Real IP Gateway Mode, page 13
- Upgrade Instructions for Release 2.1.8, page 48.

Endpoint and Directory Timeout Unified Into Endpoint Timeout

Changes were made to the timeout implementation which is configured via the Server module configuration. Endpoint Timeout and Directory Timeout have been unified into a single Endpoint Timeout parameter with units of days. The functionality of Endpoint Timeout is as follows:

- When this value is other than 0, Profiler will track the age of endpoint data for each endpoint in the database. Endpoints that have not had a refresh of endpoint data in greater than the number of days specified in the Endpoint Timeout will have the IP binding, location information (switch, port) disassociated from the MAC in the database and learned profiling data for the endpoint is purged. The endpoint MAC is maintained in the database in a “retired” state.
- At the time of the timeout, if an endpoint is in a Profile with the “Allow Timeout” option set to yes, the endpoint will be removed from the Profile and the Endpoint Directory. If that Profile matched a NAC Event, the removal from the Endpoint Directory would result in a removeMAC operation on the CAM. In the case of LDAP integration, if the Profile was enabled for LDAP, the endpoint would be removed from the LDAP directory upon expiration of the Endpoint Timeout on the next LDAP sync. This is the behavior of the Directory Timeout in version 2.1.8 build-37 and earlier.
- In the Endpoints by Profile view, Profiles with the “Allow Timeout” option set to yes will no longer display endpoints that have not had a refresh of data within the Endpoint Timeout value and are in a retired state in the database. This change will correct an issue with deleted/disabled Profiles remaining in this view, if they contained endpoints that were timed-out while in the profile prior to it being disabled or deleted.
- Endpoints in the “unknown” (un-profiled) state upon expiration of the Endpoint Timeout will not be shown in the Endpoint Directory or when viewing endpoints by Profile as Unknown has “allow timeout” enabled implicitly. Unknown endpoints that are marked as retired will not be displayed in any Endpoint Console views.
- If an endpoint that has been timed-out in the Profiler database is reconnected to the network, the discovery and profiling process for that endpoint is the same as that for a new endpoint joining the network for the first time. The identity attributes of the endpoint must be observed by the Profiler and the endpoint profiled accordingly—profiling data for the endpoint collected by the Profiler previous to the timeout is not available for the profiling decision as it is cleared from the database when the endpoint is retired.
- Upon upgrade to the build-38 maintenance release, if the system had an Endpoint Timeout set (value in hours in previous builds) this value is ignored during the upgrade. If the Directory Timeout was enabled in the configuration prior to upgrade, this value will be carried forward and set as the new unified Endpoint Timeout value for the system.
- On systems with a Directory Timeout set to other than the default (0 = no timeout), any endpoint in the database that had not had a refresh of endpoint data within the number of days specified by the timeout was already marked as 'retired' in the database. Upon upgrade to 2.1.8-38, all endpoints that had been subjected to the Directory Timeout and placed in the retired state previous to the upgrade

will be treated as described above: they will be removed from the Endpoint Directory and view endpoints by Profile views of the Endpoint Console, and searching on the MAC address of the endpoint will return no results.

Refer to CSCsv55509, page 33 for further information.

Enhancements in Cisco NAC Profiler Release 2.1.8-37

Build 37 of Cisco NAC Profiler release 2.1.8 is a general and important bug fix release for the Cisco NAC Profiler that addresses the caveats described in Resolved Caveats - Release 2.1.8-37, page 35.

This release also includes the following enhancements:

- LDAP Enhancement, page 9
- Advanced Rule Editor, page 9

Refer to Known Issues in Version 2.1.8, page 12 for additional details.

For upgrade instructions, refer to Upgrade Instructions for Release 2.1.8, page 48

LDAP Enhancement

Enhancements were made to the LDAP Synchronization code to further improve performance.

Advanced Rule Editor

User Interface was modified to increase the size of the window used for entering/editing Advanced XML rules. This provides additional space for creating and editing Advanced rules that extend to multiple lines. Refer to CSCso50683, page 35.

Enhancements in Cisco NAC Profiler Release 2.1.8-33

This section describes enhancements added for release 2.1.8, build 33 of the Cisco NAC Profiler software for the Cisco NAC Profiler Server and Cisco NAC Profiler Collector (on the CAS).

- Enhancements for HA CAS/Collectors and HA Profiler Servers, page 10
- Enhancements for “service collector” Commands, page 10
- LDAP Integration, page 10
- Bounce Port by MAC, page 10
- Profiler Server GUI Enhancements, page 11
- HA Usability Enhancements, page 11
- Database Restore Enhancements, page 11
- NetMap Module Enhancements, page 12
- Clear Endpoint Enhancements, page 12
- MAC Vendor Database Updates, page 12
- FlexLM License Enhancements, page 12
- Restore Factory Defaults, page 12

Enhancements for HA CAS/Collectors and HA Profiler Servers

Release 2.1.8-33 of Cisco NAC Profiler adds required functionality to support high availability (HA) CAS/Collectors deployed with the Cisco NAC Profiler Server in standalone and HA modes using the 'Server' connection type. Collector configuration allows for the selection of a name for the HA-CAS pair (both appliances), and the ability to specify one or more addresses of the Profiler Server using the 'service collector config' command to allow the Collector service to accept connections from standalone and HA Profiler Servers.

Refer to Configuration of Collectors on HA-CAS Pairs for Cisco NAC Profiler Release 2.1.8, page 17 for specific instructions to configure HA CAS/Collectors deployed with standalone and HA Profiler Servers.

Enhancements for "service collector" Commands

service collector verify

The 'service collector' command set has a new option 'service collector verify' that shows current configuration of a Collector for verification of current settings without entering configuration mode.

service collector config

The 'service collector config' command has been modified so that the value shown in brackets after each configuration parameter is either the current value of that parameter, or the default if not configured previously. In previous versions, only the default value was shown, not the current value of the parameter.

LDAP Integration

Cisco NAC Profiler release 2.1.8-33 substantially improves implementation of LDAP (Lightweight Directory Access Protocol), which allows the system to be queried by external systems such as RADIUS authentication servers. With this release, the Profiler Server includes an onboard LDAP directory which automatically synchronizes with LDAP-enabled Profiles in the Profiler endpoint database. Refer to the *Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8* for an overview of enhancements and LDAP system configuration.

Bounce Port by MAC

Cisco NAC Profiler integration with Cisco NAC Appliance now features the ability to force endpoints as they are Profiled into a Profile that matches a NAC Event to be re-provisioned by Cisco NAC Appliance immediately upon being Profiled. This allows endpoints previously undiscovered by the Profiler Server (e.g., new printer added to the network) to be discovered, profiled, and re-provisioned by Cisco NAC Appliance such that they get the proper network access with no manual intervention.

Refer to Use of "Custom API" Feature, page 15 for details on the use/configuration of this option.

Profiler Server GUI Enhancements

Release 2.1.8-33 includes several enhancements to the Profiler Server web administration interface.

Utilities Tab > System Summary

- Clicking the 'Display Server Log' button displays the Server.out file with last entry at top, and log entries are now date/time stamped.
- Clicking new button 'Download DB dump' creates a database (configuration and endpoint data) backup and copies it to a specified off-appliance location in a single operation.
- Clicking new button 'Collect Technical Logs' collects all technical log files in a single compressed archive and copies them to a specified off-appliance location in a single operation.
- The Edit Collector form adds a Refresh button which when clicked refreshes the status of Collector Component Modules without leaving the page.
- Network Device Import from CSV now supports bulk import of network devices running SNMPv3. For details, refer to the "Adding Network Devices to the NAC Profiler Configuration" chapter of the *Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8*.

HA Usability Enhancements

Release 2.1.8-33 includes several enhancements to the usability of the High Availability (HA) option for the Cisco NAC Profiler Server. Several automation scripts are added that enhance the following Profiler Server HA operations:

- Adding HA to an operational standalone Profiler Server
- Temporarily disabling HA on an operational HA Profiler Server
- Permanently removing an HA Profiler Server configuration
- Automated reconfiguration of HA on a Profiler Server pair after permanent removal (e.g., resetting the HA configuration on a pair)
- Added automated replication of UI user accounts and passwords between HA systems.
- The Cisco NAC Profiler Server software upgrade script detects when it is being used to upgrade members of an HA pair and guides the user through the proper steps necessary for HA upgrade. This includes: upgrade the Secondary, perform automated failover of the system, then prompt for the upgrade of the former Primary appliance.

Database Restore Enhancements

Release 2.1.8-33 adds Profiler Server database restore scripts that can be used to restore the Profiler Server database of a Cisco NAC Profiler system from a database backup. The script is run from the command line and accepts the filename of the desired backup file (.gz format). You can run these scripts to automate the restore of the system configuration and endpoint database to standalone and HA systems from a backup. Running the script and specifying a backup file drops all contents of the Profiler Server database recreate and restore using the data in the backup file. In previous versions this operation had to be performed in multiple steps via the command line.

NetMap Module Enhancements

Release 2.1.8-33 implements automated checking of Network Devices in the Profiler system configuration for devices that have not been polled by the NetMap Collector component module in greater than 3 days. The new script can be run from the command line on the system hosting the Profiler Server and database to output a list of stale network devices to the console. The script checks the database for Network Devices (switches, routers) that have not been contacted by the designated NetMap module of the Profiler system in over three days.

Clear Endpoint Enhancements

The Clear Endpoint functionality has been changed to age-out all Profiling data about an endpoint when selected from the Summary Information page for a selected MAC or IP Address. Selecting Clear Endpoint for a given endpoint will result in the removal of all information about the device from the Profiler database requiring the endpoint to be re-learned in order for information about it to be presented by the GUI.

MAC Vendor Database Updates

The OUI (MAC Vendor) database for the Profiler Server has been updated.

FlexLM License Enhancements

FlexLM license upload has been modified on the Profiler Server to accept MAC addresses regardless of case. This addresses caveat CSCsk25865, page 36.

Restore Factory Defaults

A script has been added to the system to enable restore of the Profiler Server to factory defaults. Additional command line operations are outlined in the “NAC Profiler Server Command Line Reference” chapter of the *Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8*.

Known Issues in Version 2.1.8

This section describes the following:

Refer also to Open Caveats - Release 2.1.8-39, page 21 for additional important information.

Inference-Based Profiles

The “inference-based” Profiles, enabled by specifying Print Servers or Voice Gateways in the MyNetworks config, creates the Generic Printer and Generic IP Phone Profiles. The NAC Event logic does not match these Profiles, even if the regex matches the Profile name (e.g., /phone/i, /printer/i).

Workaround

Add Profiles named Generic Printer and/or Generic IP Phone Profile to the configuration (Create Profiles), then endpoints in these automatically created Profiles will be included in the synchronization.

CAS/Collectors Running in Real IP Gateway Mode

Real-IP Gateway and Collector modules enabled on a CAS with eth0 and/or eth1 configured for NetWatch are subject to an issue where HSRP duplicate frames are sent by the CAS in Real-IP Gateway mode with Collector NetWatch enabled on eth0. This causes HSRP issues and the default gateway to go down.

Eth0/NetWatch Workaround

The workaround is as follows:

- Use of eth0 and NetWatch concurrently is not supported.
- Configure eth2 or eth3 with an IP address to receive the IP helper packets and remove NetWatch/SPAN monitor for eth0 of the CAS Collector, as described in the following steps.

Step 1 Configure an unused interface (eth2 or eth3) of the NAC Server (CAS) collector via the CLI. For example:

a. cd to /etc/sysconfig/network-scripts

b. copy file ifcfg-eth0 to ifcfg-eth3 and edit (using VI)

c. cp ifcfg-eth0 ifcfpg-eth3

d. vi ifcfg-eth3

Note The IP Address configured for this interface needs to be a separate network from the eth0/eth1 interfaces on the NAC Server. If this is being set up for HA NAC Server Collectors, then you must also configure this interface via the CLI on the other NAC Server in the HA pair.

```
IPADDR=172.16.14.18
NETMASK=255.255.255.248
BOOTPROTO=static
ONBOOT=yes
PERFIGO_VLANPASS=
GATEWAY=
BROADCAST=
DEVICE=eth3
NETWORK=
```

Network routing needs to exist for this new network. The interface is not configured with a default gateway (so that the NAC Server routing is not confused/disrupted as a precaution). Since IP helper is sent UDP, a response is not needed. The client subnet is simply informing the Collector interface

(running NetWatch) about the new DHCP requests and the Profiler is able to use this to get Client OS (DHCP Vendor) information used in profiling. You will not be able to ping this interface from the network since there is no default gateway. To troubleshoot and verify if the packets are being seen on the interface you can use `tcpdump -i eth3`.

Step 2 IP helper addresses configured on routed interfaces (SVIs) will need to point to the IP(s) of this interface (HA will have 2 separate IPs) for profiling of DHCP requests.

Step 3 Set up Collector NetWatch for this interface via the Profiler GUI:

a. Go to **Configuration > NAC Profiler Modules > List NAC Profiler Modules** and click on the appropriate Collector.

b. Under **NetWatch Configuration**, click **Add Interface**.

c. Type in the new interface name and choose the network(s) to match.

d. Click **Add Interface**, **Save Collector**, then **Apply Changes** and **Update Modules**.

See also CSCsm20254, page 29 and Collector Support and CAS Deployment Modes, page 4.

Server.out Log

The Server.out log viewable from the GUI does not collect all Cisco NAC Appliance synchronization messages, only a subset of these messages.

Follow the procedures specified in the *Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8* for viewing the NAC integration logs.

Device Filter List on the CAM

When Cisco NAC Profiler is integrated with Cisco NAC Appliance release 4.1(3), entries in the Device Filter List on the Clean Access Manager (CAM) made by the Profiler Server cannot be edited normally. Attempting to edit a Device Filter List entry made by the Profiler Server via synchronization will return a database error on the CAM.

Workaround

Add Profiles named Generic Printer and/or Generic IP Phone Profile to the configuration (Create Profiles), then endpoints in these automatically created Profiles will be included in the synchronization.If a Profiler-created Device Filter List entry on the CAM needs to be edited, the following procedure can be used:

1. On the CAM, navigate to Device Management > Filters > Devices > List, and click the Edit button for the Profiler-generated Device Filter entry.
2. In the Edit screen for the entry, select all the current text in the Description field and delete the description (click in the existing description text, CTRL-A, DEL).
3. Make any desired edits to the Device Filter entry, e.g.:

- Change Access Type (ALLOW, DENY, ROLE, CHECK, IGNORE)
- Add custom description, if desired, per normal guidelines as outlined in the *Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8*.

4. Click “Save” to apply change

The next time the Profiler-NAC synchronization process runs, the description field will return to its normal form, unless the "*" prefix has been used. Refer to chapter "Integration with Cisco NAC Appliance" in the *Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8* for details.

Refer to CSCsm58145, page 29 for additional details.

Use of "Custom API" Feature

The Custom API option of the Server module NAC configuration (Configuration -> Profiler Modules -> Server -> NAC Configuration) should only be implemented in specific situations as described in this documentation, or as directed by the Cisco TAC. Whenever upgrading Cisco NAC Profiler or Cisco NAC Appliance software, carefully consult the release notes to determine if it is appropriate for the Custom API to be enabled.

The Custom API functionality was implemented to provide extensions to the Cisco NAC Appliance API for three specific scenarios:

Scenario A: Cisco NAC Appliance 4.0, Access Types CHECK and IGNORE

The API for Cisco NAC Appliance release 4.0 does not support Device Filter List access types CHECK and IGNORE. If either of these access types is to be used with NAC-Event-Rules, then the Custom API must be enabled, using patch file **cca4_api_addmac.diff**.

Scenario B: Cisco NAC Appliance 4.1.0, 4.1.1, 4.1.2, Out Of Band Deployments

For Out Of Band (OOB) deployments, switch port VLAN provisioning typically immediately enforces updates to the Device Filter List as soon as they are made. In other words, the assigned VLAN on a port should immediately be updated if a Device Filter List entry, which specifies the MAC address for an endpoint connected to the given port, is added, removed, or changed. For OOB deployments with Cisco NAC Appliance releases 4.1.0, 4.1.1, 4.1.2, the immediate enforcement of network access policy via Device Filter List changes does not occur. For example, if a printer is already connected to the network and a Device Filter List entry for the printer's MAC address is added, the printer is not immediately granted network access (nor is access immediately revoked if the Filter List entry is removed).

If this behavior is desired when running Cisco NAC Appliance 4.1.0, 4.1.1, 4.1.2, the Custom API must be enabled, using patch file **cca41x_api_bounceport.diff**.

Note This mode of Custom API use has been tested and approved for use with the following Cisco NAC Appliance releases:

- Cisco NAC Appliance 4.1.0, 4.1.1, 4.1.2
- If using release 4.1.0 or 4.1.1, patching of ssl.conf is required as described in Implementation Instructions, page 16, and Important Caveat, page 17.

Scenario C: Cisco NAC Appliance 4.1.3, Out Of Band Deployments

This scenario is similar to Scenario B: Cisco NAC Appliance 4.1.0, 4.1.1, 4.1.2, Out Of Band Deployments, page 15, but affect Cisco NAC Appliance 4.1(3).

For this scenario no patch file is utilized. For implementation, simply enable the Custom API checkbox in the Profiler Server Configuration as described in Step #2 in the implementation instructions below.

Note This mode of Custom API use has been tested and approved for use with the following Cisco NAC Appliance release:

- Cisco NAC Appliance 4.1.3

Implementation Instructions

For the following instructions:

- PATCH_FILE is the selected patch file named in the corresponding section
- CAM is the IP or DNS address of the Clean Access Manager system (VIP/service address for HA CAM pairs).

Perform the following steps to enable the Custom API.

Prerequisite

Configure Cisco NAC Profiler integration with Cisco NAC Appliance as described in the *Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8* before enabling the Custom API.

1. For Scenarios A and B ONLY: Patch API file

Log on to the Profiler Server via SSH as user beacon and perform the following commands.

Note Be especially careful with the last command.

```
1. profiler# cd /usr/beacon/etc
2. profiler# scp root@CAM:/perfigo/control/tomcat/normal-webapps/admin/cisco_api.jsp
cisco_api.jsp
3. profiler# patch -b < cca_api/PATCH_FILE
4. profiler# scp cisco_api.jsp
root@CAM:/perfigo/control/tomcat/normal-webapps/admin/cisco_api_alt.jsp
```

2. For ALL Scenarios: Tun on Feature in Profiler Server UI

In the Cisco NAC Profiler Server web interface, do the following:

Step 1 Browse to Server module configuration screen by navigating to Configuration-> NAC Profiler Modules->List NAC Profiler Modules->"Server"

Step 2 In the "NAC Configuration" section, enable the checkbox labeled Custom API

Step 3 Click Update Server

Step 4 Restart the Server module: Configuration->Apply Changes->Re-Model

3. Scenarios B and C on Cisco NAC Appliance 4.1.0, 4.1.1: Patch ssl.conf

Note This step is required for Scenario B: Cisco NAC Appliance 4.1.0, 4.1.1, 4.1.2, Out Of Band Deployments, page 15 andScenario C: Cisco NAC Appliance 4.1.3, Out Of Band Deployments, page 16 when the Cisco NAC appliance release is 4.1.0 or 4.1.1 only. This step is not required for release 4.0 or 4.1.2 and later.

Log on to the Profiler Server system via SSH as user beacon and perform the following commands:

```
1.      profiler# cd /usr/beacon/etc
2.      profiler# scp root@CAM:/perfigo/control/apache/conf/ssl.conf ssl.conf
3.      profiler# patch -b < cca_api/cca41x_ssl_conf.diff
4.      profiler# scp ssl.conf root@CAM:/perfigo/control/apache/conf/ssl.conf
5.      profiler# scp ssl.conf root@CAM:/perfigo/control/apache/conf/ssl_alt.conf
6.      On CAM, execute these commands:
7.      cam# /perfigo/control/bin/stopapache
8.      cam# /perfigo/control/bin/startapache
```

Important Caveat

This setup will stop being operational if either the CAM is rebooted or command 'server perfigo restart' is executed on the CAM. If this happens, the following commands must be executed to restore the custom API to operational status.

```
cam# cd /perfigo/control/apache/conf/ssl_alt.conf
cam# cp ssl.conf.patched ssl.conf ssl.conf
cam# /perfigo/control/bin/stopapache
cam# /perfigo/control/bin/startapache
```

Note Upgrading to Cisco NAC Appliance release 4.1(2) or later removes the need for this CAM ssl.conf file workaround.

Configuration of Collectors on HA-CAS Pairs for Cisco NAC Profiler Release 2.1.8

Release 2.1.8 of Cisco NAC Profiler includes changes to the procedure for the configuration of CAS/Collector HA pairs deployed with standalone and HA Profiler Server pairs. Use the following procedure when deploying CAS/Collector HA pairs in a Cisco NAC Profiler system:

Step 1 Configure CASs for HA mode operation and verify that the HA protocol is operational. This step is critical to complete first to ensure that the HA protocol between the CASs is operating normally and the VIP is available for the Collector service configuration on both appliances in the CAS pair.

Step 2 Determine a name for the Collector service to run on the CAS pair. The name must be no greater than 24 characters, and a name that associates the Collector service on **both** members of the CAS pair is recommended such as "Building-26-CAS" for example. This name will be used in the Profiler Server configuration to identify the Collector service on the HA CAS Pair so that it can be managed via the GUI as a **single** Collector.

Step 3 Configure the Collector service on the primary CAS first by using the 'service collector config' command.

a. Select yes when asked if you would like to enable the NAC Collector

b. Select yes when asked if you would like to configure the NAC Collector

c. Enter the name for the Collector service on the pair which was determined in Step 2.

Note An identical name for the Collector service must be used in the configuration on both CASs in the HA pair. Normally, the hostname of the CAS appliance is chosen by default when configuring a Collector. For release 2.1.8-33 and later, there is an option to specify a name for the Collector when using the 'service collector config' command. When configuring CAS/Collector HA pairs, a name for the Collector service must be chosen and used on **both** appliances in the pair identically (e.g., case sensitive, spaces, etc.).

d. The Connection type for the Collector configuration **must** be set to 'Server'. For CAS/Collector HA Pairs, the Profiler Server will have to initiate the connection to the Collector service running on the pair. This is accomplished by selecting the Server connection type for the CAS/Collector.

e. Listen on IP - the Collector should be configured to listen on the VIP/Service IP address assigned to the CAS HA pair during CAS HA configuration.

f. Enter the IP address(es) of the Profiler Server that will connect to the CAS/Collector:

1. For a standalone Profiler Server, this should be the IP address of the eth0 (management interface) of the Profiler Server. Enter the IP address of the eth0 interface, then type 'done' when prompted for another address.
2. If the Profiler Server is deployed as an HA pair, the eth0 interface IP addresses of **each** Profiler appliance needs to be entered in this step along with the VIP/Service IP of the HA Profiler Server pair. Enter the IP address of the eth0 interface of the first Profiler Server appliance, press enter; enter the IP address of the eth0 interface of the other Profiler Server appliance in the HA pair, press enter, enter the VIP/Service IP address of the HA Profiler Server pair, then enter 'done' to progress the script to the next step.

g. Enter the port number for the TCP connection between the Profiler Server and Collector—the default of 31416 is acceptable in almost all cases. The port number specified for the Collector must match that of the Network Connection specified for the Server module in Step 5.f.

h. Select the Encryption type for the connection between the Collector and the Profiler Server. Select 'none' if no encryption is desired. The encryption type on the Collector must match that of the Network Connection specified for the Server module in Step 5.g.

i. Specify a shared secret if encryption was selected. If no encryption was selected, do not enter a shared secret. The shared secret for encryption on the Collector must match that of the Network Connection specified for the Server module in step 5.h below.

Step 4 Complete the steps outlined in Step 3 on the secondary CAS in the pair, ensuring that the parameters are entered identically for the second appliance as they were for the first member of the CAS HA pair.

Step 5 Create a Network Connection of type Client in the Server module configuration which will result in the Profiler Server initiating a connection to the VIP/Service IP address of the Collector service running on the HA CAS pair

a. Using the GUI, open the Configure Server form by navigating to the Configuration tab and selecting NAC Profiler Modules -> List NAC Profiler Modules. From the Server table, click on the Server link to display the Configure Server form and display the current Profiler Server configuration.

b. Scroll down to the Network Connections section of the form, near the bottom

c. Select the 'Add connection' button to add a new network connection

d. For Connection Type: select the 'client' radio button

Note When the Client radio button is selected, the add network connection form changes. Note that the Allow Connections From section is shown at the bottom of the form. For standalone appliances, this should be populated with the loopback address (127.0.0.1) and the IP address of the eth0 interface of the Profiler Server. For HA Profiler Server pairs, the loopback and the eth0 interface addresses of both appliances should be displayed.

e. Enter the IP address of the VIP of the CAS HA pair hosting the Collector service in the IP Address field.

f. Enter the TCP port number for the connection between Profiler Server and Collector. This must match what is configured on the Collector services running on both members of the HA pair (Step 3.g. and Step 4.g.)

g. Select the desired encryption type from the drop down. This must match what is configured on the Collector services running on both members of the HA pair (Step 3.h. and Step 4.h.)

h. Enter the shared secret for the encryption type selected—leave blank if no encryption was selected. The shared secret must match what is configured on the Collector services running on both members of the HA pair (Step 3.i. and Step 4.i.) if applicable)

i. Click on Add connection button to save new connection

j. Verify that the newly added connection now appears in the list of network connections for the Server module (Edit Server form), then click on Update Server to save the configuration.

Step 6 Add the Collector for the CAS pair into the Profiler Server Configuration via the GUI.

a. Click on Add Collector to open the Add Collector form

b. Enter the Collector Name in the field. The Collector name must match the name determined and configured for the Collector service running on both members of the CAS pair in Step 2. This ensures that Collector failover will occur automatically upon failover of the CAS service from one to the other member of the pair.

c. In the Forwarder Configuration section of the form, enter the following information to complete the configuration:

   a. IP Address: enter the VIP/Service IP address of the CAS pair hosting this Collector service

   b. From the Connection drop-down, select Listen for: Server (port: 31416 (or selected port number))

d. Select Add Collector to save the new Collector to the Profiler Server configuration

e. Select Apply Changes -> Update modules to restart the system.

After 3-5 minutes, the Server should establish the connection to the Collector service running on the active member of the CAS pair. Upon failover of the CAS, the Collector service will move with the CAS service to the active member of the pair along with the connection to the Profiler Server.

Caveats

This section describes the following caveats.

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

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

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

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

Open Caveats - Release 2.1.8-39

Note 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 8)

	Software Release- Cisco NAC Profiler Version 2.1.8-39	
DDTS Number	**Corrected**	**Caveat**
CSCsl20917	No	Upload Licenses page should display the licenses already present **Conditions** While looking at the Admin GUI - Upload Licenses, installed licenses aren't displayed. **Workaround** Check in the file via the CLI /usr/beacon/working/flexlm.
CSCsl21160	No	Profiler Admin session should Logout after timed interval NAC Profiler GUI Admin logged in never gets logged out. **Workaround** None

Table 3 List of Open Caveats (Sheet 2 of 8)

DDTS Number	Software Release- Cisco NAC Profiler Version 2.1.8-39	
	Corrected	**Caveat**
CSCsl59431	No	Devices in L3 IB NAC deployments cannot be added/removed from CAM filter list Devices in L2 can be added/removed to/from the filter list based on their profile information as the Profiler can call addmac or removemac API calls towards the CAM. But if these devices are at L3 and IB is the mode of the CASs, then the Profiler has to use the addip/removeip type of APIs to add IP addresses to the IP filter list. **Conditions** L3 inband removal of devices via IP address. **Workaround** None. This is not a supported feature.
CSCsq34147	No	Profiler: Standby Profiler shows database errors on Endpoint Console Standby NAC Profiler displays Unknown DB Error on the Endpoint Console Page. **Conditions** NAC Profiler running 2.1.8-37 in a failover pair. This will only show up on the Standby Profiler. **Workaround** None but this is a cosmetic 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.
CSCsq42942	No	NAC Profiler: Secondary 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** 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 cosmetic 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>]`

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

DDTS Number	Software Release- Cisco NAC Profiler Version 2.1.8-39	
	Corrected	**Caveat**
CSCsr58170	No	CAS service collector status should not list Server module status CAS service collector status lists Server status as “not installed” **Conditions** CAS Collector does not include a Server module, only the Profiler does. **Workaround** None. This should not be listed on the CAS Collector status output **Note** This does not affect the function of the Collector.
CSCsr84407	No	IP address missing in CAM device filter list added from Profiler via API CAM GUI: Device Management > Filters > List | Endpoint device listed lists IP address as 0.0.0.0 **Conditions** Profiler addition of device into CAM device filter list **Workaround** Currently Profiler does not use the IP address in the device filter list so this is just a cosmetic issue.

CSCsr91618	No	service profiler status lists services not supported on Profiler server
		The Profiler status shows all the modules for the Collector that it will never be running or have installed.
		
		Conditions Forwarder, NetMap, NetTrap, NetWatch, NetInquiry, NetRelay will never be installed or supported on the 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

Table 3 List of Open Caveats (Sheet 4 of 8)

DDTS Number	Software Release- Cisco NAC Profiler Version 2.1.8-39	
	Corrected	Caveat
CSCsu29905	No	NAC Profiler SNMP trap receive does not check community string 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	No	NAC Profiler GUI allows duplication of Collector entry A Collector with the same name and IP can be created as a duplicate in the NAC Profiler GUI. **Conditions** When a Collector of the same info already exists. **Workaround** None.
CSCsu46273	No	NAC Profiler GUI needs the ability to set time and NTP information Currently there is no way to set the time via 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.
CSCsu46311	No	NAC Profiler GUI does not display IP or name of active Profiler When you click on the Config - NAC Profiler modules - List Config - Server server it displays Server Name: Server. The CLI name shows machines profiler1 & 2 but this is not shown nor the actual IP config on the boxes via the GUI. **Workaround** None
CSCsu46325	No	NAC Profiler GUI software version should match CLI version output The software version for NAC Profiler/Collector shown on the admin GUI does not match the version shown via CLI. **Workaround** View the Profiler and Collector version via the CLI with commands: • CAS Collector: service collector status • NAC Profiler Server: service profiler status

Table 3 List of Open Caveats (Sheet 5 of 8)

	Software Release- Cisco NAC Profiler Version 2.1.8-39	
DDTS Number	**Corrected**	**Caveat**
CSCsu46348	No	NAC Profiler GUI NAC roles should use API call to populate listing NAC Roles need to be populated with a query instead of typing them in manually in the Profiler server config—too much chance of error for user input and will increase customer ease of use. **Conditions** Entry of NAC roles **Workaround** Manual entry of role
CSCsv66296	No	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.
CSCsw30875	No	NAC Profiler license is not included in the CCA evaluation bundle. **Symptom** The Clean Access evaluation license doesn't include the NAC Profiler and Collector licenses despite the information included in the following page: http://www.cisco.com/en/US/customer/docs/security/nac/appliance/support_guide/license.html#wp39250 **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).

Table 3 List of Open Caveats (Sheet 6 of 8)

DDTS Number	Software Release- Cisco NAC Profiler Version 2.1.8-39	
	Corrected	**Caveat**
CSCsw97514	No	Profiler: Admin UI allows Collector name greater than 24 characters **Symptom** Inability to delete a Collector with a name greater than 24 characters from the NAC Profiler Server. An error pops up that Collector does not exist in the database. **Conditions** NAC Profiler running 2.1.8-37. The Collector name has to be greater than 24 characters. **Workaround** Manually delete the Collector from the Profiler database. 1. SSH to the NAC 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 GUI>%';" | psql` **Further Problem Description** The Database field for the Collector name is limited to 24 characters. The GUI currently does not check the length of the user input. If a name greater than 24 characters is entered it is truncated when placed in the database.
CSCsx03749	No	Profiler: Does not produce error message when no slash (“/”) used in event match **Symptom** Profiler does not produce an error message when no forward slash (“/”) is used in event, and the Profile will never be matched **Conditions** When adding a NAC event and matching the Profiler names. **Workaround** None

Table 3 List of Open Caveats (Sheet 7 of 8)

DDTS Number	Software Release- Cisco NAC Profiler Version 2.1.8-39	
	Corrected	Caveat
CSCsx42320	No	Profiler and Collector unable to communicate through NAT device **Symptom** NAC Profiler and Collector cannot communicate with each other with a NAT device between them. **Conditions** When a Profiler and Collector are connected between a NAT device, communication will not be established. Profiler reconfigures the Collector's configuration during normal operation. Collector will not communicate properly in the client or server setup. **Workaround** Collector and Profiler should be configured and connected on an internal trusted network. NAT breaks the communication and should be moved to a Non-NAT setup between Collector and Profiler.
CSCsy84379	No	SNMP informs needed for Cat 6500 Profiler compatibility **Symptom** 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-notification mib
CSCta25695	No	Profiler incorrectly handles traps and polling with SNMPv3 **Symptom** Edge switches running SNMPv3 are not polled correctly by the Collector after sending a link up or MAC notification trap. Discovery of endpoints connecting to ports on switches running SNMPv3 is delayed until the next regular poll of the switch by NetMap. **Conditions** NetTrap receives a link up/MAC notification trap for switch running SNMPv3, subsequent poll triggered by trap fails and endpoint location is not collected/displayed by the system until the next scheduled poll. **Workaround** A patched Server module binary must be installed on the NAC Profiler Server version 2.1.8-39.

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

	Software Release- Cisco NAC Profiler Version 2.1.8-39	
DDTS Number	**Corrected**	**Caveat**
CSCtb02389	No	Profiler: Cisco MAC address shows up as unknown **Symptom** MAC Vendor Code 00:24:c4 is being displayed as an unknown vendor in the NAC Profiler. This is a Cisco vendor code and should be displayed as such. **Conditions** NAC Profiler 2.1.8-38 **Workaround** None
CSCtb17189	No	Profiler incorrectly shows ports as trunks **Symptom** In NAC Profiler, endpoint ports may show up as trunk ports. **Conditions** This happens in Profiler 2.1.8 code. This has been observed on a switch port with a Cisco VG224 attached to the port. **Workaround** None.

Resolved Caveats - Release 2.1.8-38

Table 4 List of Resolved Caveats (Sheet 1 of 7)

	Software Release- Cisco NAC Profiler Version 2.1.8-38	
DDTS Number	**Corrected**	**Caveat**
CSCsm20254	Yes	CAS Collector: Overwrites HSRP packets with CAS MAC address HSRP duplicate frames are sent by CAS in Real-IP Gateway with Collector NetWatch enabled on eth0. This causes HSRP issues and the default gateway to go down. **Conditions** Real-IP Gateway and Collector modules enabled on a CAS with ETH0 and or ETH1 configured for NetWatch. **Workaround** • Use of eth0 and NetWatch concurrently is not supported. • Configure eth2 or eth3 with an IP address to receive the IP helper packets and remove NetWatch/SPAN monitor for eth0 of the CAS Collector. Refer to CAS/Collectors Running in Real IP Gateway Mode, page 13 for detailed steps.
CSCsm55679	Yes	Clean Access Manager: CSRF tags get added to GLOBAL MacFilterList description field upon edit **Symptom** CSRF tag gets added to a GLOBAL MAC device filter's description when edited **Conditions** If the description of a GLOBAL MAC filter contains a single quote (') and is edited from the CAM GUI then the CSRF tag gets appended to the description. It will be added every time you edit and save the filter from the web GUI. **Workaround** None
CSCsm58145	Yes	CAM: Database error when editing a description to CAM filter list If an entry placed by the Profiler Server on the CAM Device Filter List is **edited** in the CAM UI, a database error occurs due to the length of the description field. **Workaround** Refer to the workaround listed in Device Filter List on the CAM, page 14.

Table 4 List of Resolved Caveats (Sheet 2 of 7)

DDTS Number	Software Release- Cisco NAC Profiler Version 2.1.8-38	
	Corrected	**Caveat**
CSCsm71798	Yes	Collector modules show stalled at various times during the day Description: Netflow agent module on the CAS collector shows stalled at various times of the day. Receive the following errors in the Netrelay logs: ERROR:[2008-02-13 14:25:35 (WriteBytes:405)] Write error [Broken pipe] INFO: [2008-02-13 14:25:35 (writePendingData:262)] Write indicated closing connection **Symptom** Collector modules show stalled at various times during the day **Conditions** Usually under heavy load from SPAN or Netflow **Workaround** Lower the number of traffic rules configured. • Make sure you are not looking at an everything wildcard like 0.0.0.0 for IP addresses. • Make sure you narrow the source and or destination ports in the traffic rules. • Be specific on the networks you are SPANNING traffic for or passing Netflow to the clean access server. Do not supernet your subnets like 10.0.0.0/8 if you are not using the whole class C. • The Modules should recover once they have finished completing their task.
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** The process for importing a certificate is available on Cisco.com at: http://www.cisco.com/en/US/partner/products/ps6128/products_configuration_example09186a00809f0e60.shtml See defect CSCsm83238, page 44 for additional details.

Table 4 List of Resolved Caveats (Sheet 3 of 7)

	Software Release- Cisco NAC Profiler Version 2.1.8-38	
DDTS Number	**Corrected**	**Caveat**
CSCsq86847	Yes	Collector: NetTrap not handling SNMPv2c traps correctly. SNMP v2c Link-up and down traps are not being handled properly by the CAS Collector. You will not see new devices right away in the endpoint console. **Conditions** Switches configured for SNMP version 2c **Workaround** Use SNMP version 1 or contact support for a patch to use v2c.
CSCsr51748	Yes	Collector: NetInquiry Ping Sweep not completing NetInquiry Ping Sweep function is not completing sweep of specified InternalAddressBlock. **Conditions** When doing a ping sweep of a /16 or /8 network. Class A or B size. **Workaround** Limit ping sweep to a class C. **Further Description** In the NetInquiry module configuration, the "Enable Ping Sweep" checkbox was removed in this maintenance release. The ping sweep functionality is not required for NetInquiry functionality and Active Profiling; hence it was removed as a configuration option. Upon upgrade of a NAC Profiler system to the 2.1.8-38 maintenance release, any NetInquiry module with the ping sweep enabled in the system configuration will be reconfigured automatically to disable the ping sweep. Turning this function off has no effect on the normal operation of the NetInquiry module and Active Profiling in general.
CSCsr52954	Yes	Configuration of NetInquiry Module can cause Collector to go down When configuring a large IP scope for NetInquiry and activating Ping Sweep and/or DNS Collection, the CAS running the Collector can crash, respectively running out of CPU and Memory resources. It could be fixed by checking the configuration validity or by running the NetInquiry module in a safer way. **Workaround** Configure smaller IP scopes.
CSCsr64573	Yes	Need to update the Profiler MAC list with the new range of Apple MACs Apple has a new range of vendor specific addresses which are not properly detected by the Profiler. **Conditions** Users with hardware which use a new Apple vendor specific OUI **Workaround** Update oui.txt on the Profiler

Table 4 List of Resolved Caveats (Sheet 4 of 7)

	Software Release- Cisco NAC Profiler Version 2.1.8-38	
DDTS Number	**Corrected**	**Caveat**
CSCsu30089	Yes	Profiled device is assigned a DENY role with Check in NAC event filter. Profiled device is assigned a DENY role when the NAC event filter is defined for Check. Allow and Ignore roles do not have this problem. **Conditions** Profiler and Collector are running version 2.1.8-37. **Workaround** Assign the role in NAC Profiler event.
CSCsu37693	Yes	NAC Event not triggered with multiple rules in a profile NAC Event is not triggered by matching a higher Certainty value within a Profile. **Workaround** Create one rule in the Profile to match, or create separate Profiles and match on the Profile you want to add to the NAC Manager filter list. The rule that results in the higher CF should be standalone in a Profile that the NAC Event is defined to match—so that when endpoints are profiled into that higher-certainty Profile, the NAC event is fired and the endpoint is placed on the CAM Filter List as desired.
CSCsv52414	Yes	NetWatch DHCP handling enhanced DHCP messages processed by NetWatch and the Profiler sometimes changed the profile for the endpoint which would result in a network access change. The endpoint profile which was sourced from DHCP packets was not persistent. **Conditions** With DHCP messages beside Discovery, Request, and Inform. Profiles which were sourced by DHCP packets of other types for purposes other than address and network parameter discovery/assignment. **Workaround** None

Table 4 List of Resolved Caveats (Sheet 5 of 7)

DDTS Number	Software Release- Cisco NAC Profiler Version 2.1.8-38	
	Corrected	Caveat
CSCsv54925	Yes	NetInquiry process improvement of /16 & /24 networks (DNS, TCP, banners) NetInquiry of /16 and /24 networks are not completely finishing and populating the Profiler. **Conditions** An issue with NetInquiry collection across /16 and /24 network blocks was corrected so that DNS name collection, TCP Open Port and Web/SNMP server banner collection across an entire class network or subnetted class network (e.g., 10.1.0.0/16) is completed correctly by the NetInquiry module. **Workaround** Limit the size/scope of the inquiry.
CSCsv55509	Yes	Endpoint summary timestamps for network stack info display inconsistency In the Endpoint Summary, the timestamp for the Network Stack Info (View Profile Data, Table of Other Data) was displayed differently than other parameters in the Endpoint Console views. **Workaround** None Refer to Endpoint and Directory Timeout Unified Into Endpoint Timeout, page 8 for further details.
CSCsv55569	Yes	Endpoint & Directory Timeout have been unified into Endpoint Timeout Changes were made to the timeout implementation which is configured via the Server module configuration. Endpoint Timeout and Directory Timeout have been unified into a single Endpoint Timeout parameter with units of days.
CSCsv55719	Yes	Profiler handling of unknown vendor MAC addresses The table of MAC and IPs would be empty despite the fact that the system had one or more endpoints with MACs with unknown vendors. **Conditions** When using Utilities -> Profile Data -> Endpoint data summary -> MAC Vendors, if there were endpoints in the database with MAC Address OUIs that did not resolve to a vendor in the Profiler OUI database, displaying the MAC/IP Addresses of those endpoints by clicking on the 'Show MAC/IP' button from the table of MAC vendors for the Unknown row did not function. **Workaround** None

Table 4 List of Resolved Caveats (Sheet 6 of 7)

	Software Release- Cisco NAC Profiler Version 2.1.8-38	
DDTS Number	**Corrected**	**Caveat**
CSCsv55800	Yes	Endpoint search by MAC not returning result without IP-to-MAC binding **Conditions** If an IP-to-MAC binding for the endpoint was not in the database. **Workaround** None
CSCsv56013	Yes	Multiple traps received close together cause NetMap to poll too soon An issue with the trap handling mechanism in cases where multiple traps received in rapid succession would cause the NetMap module to poll the device before the MAC Address was added to the switch source address table (CAM) **Conditions** The poll resulting from a link transition with more than just a single link down, link up trap would not gather location information for the endpoint joining the network. **Workaround** None.
CSCsv56037	Yes	Log file rotation for Collector and Profiler Beacon logs are not rotating on the Profiler or Collector **Conditions** /usr/beacon/logging directory with an extension of .log or .out **Workaround** None

Table 4 List of Resolved Caveats (Sheet 7 of 7)

DDTS Number	Software Release- Cisco NAC Profiler Version 2.1.8-38	
	Corrected	Caveat
CSCsv56096	Yes	service collector config incorrectly reports the name always as hostname The 'service collector config' command run on the CAS/Collector would incorrectly report the current Collector name if a name other than the CAS hostname was selected for the Collector. **Conditions** The output of the 'service collector config' command would report the Collector name as the appliance hostname always, regardless of current configuration. **Workaround** None
CSCsw70085	Yes	NAC Profiler configuration guide table 2-7 wording for operating mode #3 **Symptom** Documentation explanation of operating mode #3 is inaccurate. **Conditions** The mode or state of the clients does not determine what traffic can be seen by the Collector NetWatch. If NetWatch is running on eth2/3 then it will only see what traffic the span/monitor session is sending to it. It is probably good practice not to span the authenticated VLAN for regular users. It would be good to span the auth VLAN plus the printer VLAN (and any other special purpose networks) in case a machine masquerading as a simple device suddenly exhibits PC behavior and is then profiled to be put in the auth VLAN. **Note** Section "Collector Support and CAS Deployment Modes" section on page 4 is corrected in the 2.1.8 guide and release notes.

Resolved Caveats - Release 2.1.8-37

Table 5 List of Resolved Caveats (Sheet 1 of 2)

DDTS Number	Software Release- Cisco NAC Profiler Version 2.1.8-37	
	Corrected	Caveat
CSCsm71830	Yes	CAS Collector intermittently loses connection to the Profiler.
CSCso50683	Yes	Increase the size of window used for entering/editing Advanced XML rules
CSCsm71994	Yes	Profiler: NAC Event Minimum Profile Certainty Ignored for Devices
CSCso50710	Yes	While adding/editing Network Devices, have enabled entries {} and []

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

	Software Release- Cisco NAC Profiler Version 2.1.8-37	
DDTS Number	**Corrected**	**Caveat**
CSCso50837	Yes	Issue with the use of 32-bit masks in MyNetwork configuration
CSCso50865	Yes	Re-enable the “Allow only additions to CAM Filter List”
CSCso50915	Yes	Parameters like L2/L3 Net. device mapping int. change required restart.

Resolved Caveats - Release 2.1.8-33

Table 6 List of Resolved Caveats (Sheet 1 of 2)

	Software Release- Cisco NAC Profiler Version 2.1.8-33	
DDTS Number	**Corrected**	**Caveat**
CSCsk25865	Yes	MAC Address needs to be in Upper Case with no Colons for License Generation When generating licenses on the Cisco registration page for Cisco NAC Profiler Server/Collector, note that the MAC address field is case-sensitive. The eth0 MAC address entered for the Profiler Server must be in upper case (i.e. hexadecimal letters must be capitalized). should not have any colons in between. If necessary, simply edit the format of the MAC address to correct this issue. **Note** With 2.1.8, the Profiler UI/License Check code in the Profiler Server will accept a license with the MAC address in upper case or lower case.
CSCsk25881	Yes	Changing the NAC Profiler Database Password When the NAC Profiler Server is initially installed, the default database password is set to ‘profiler.’ It is suggested not to change the NAC Profiler 2.1.7 database password. However, if the password is changed then a corresponding change must also be made to the /usr/beacon/lib/GBS/Beacon/Db.pm file on the Profiler Server. Changing the database password without implementing this fix will result in communication failures between the Cisco NAC Profiler Server and the Cisco NAC Appliance Manager.

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

	Software Release- Cisco NAC Profiler Version 2.1.8-33	
DDTS Number	**Corrected**	**Caveat**
CSCsl23121	Yes	Add device to Filter list by Profiler does not trigger Switch port change In OOB scenarios, when the Profiler adds a device to the CAM's Filter list, a switch port change is not triggered. **Conditions** Configure Profiler to add Device to Filter list based on traffic type. When the specified traffic is generated, Profiler adds the device to the CAM Filter. There are no SNMP linkdown/up traps. Port profile does not change the device port from Auth to Access VLAN. Though in Allow Filter list, device does not have access to the network **Workaround** None.
CSCsm46219	Yes	Collector SPAN port not receiving traffic on ETH3 for NetWatch DHCP traffic not seen through a CAS SPAN port. Delivery of packets on eth2 and eth3 is not present on 4.1.3 CAS in Virtual Gateway mode, and is present only in Real IP Gateway mode. In addition, if the CAS service is stopped (service perfigo stop) on a Real IP Gateway CAS, the issue persists. The CAS Appliance still does not deliver packets on eth2 and eth3 as expected (and as it does on a Virtual Gateway mode CAS). **Conditions** CAS does not receive DHCP traffic seen on the NetWatch interface. **Workaround** None.

Open Caveats - Documentation

Table 7 List of Open Caveats- Documentation (Sheet 1 of 7)

	Software Release- Cisco NAC Profiler Version 2.1.8-39	
DDTS Number	**Corrected**	**Caveat**
CSCsq72661	No	Profiler: NAC Appliance Sync Config parameters need clarification When adding the address of the CAM in an HA-pair the guide is confusing because it asks for the CAM service IP and secondary CAM IP only. The confusion is that it is not readily known what the secondary IP is needed for if communication is always done to the service IP. **Conditions** When the CAM is deployed as an HA-pair, the Server configuration needs to have the following comma-separated DNS domain-names or IP addresses: • CAM HA-pair service (VIP) • CAM HA-pair secondary node **Workaround** The following needs to be added for clarification: These parameters are used for setup of Keyless SSH between the Profiler and the CAM pair. When the Profiler administrator runs the setup-CAM-key-auth.sh script (Page 11-6 Configure SSH Key-Based Authentication - HA Profiler Servers), it will establish SSH between the Profiler and the primary CAM appliance (via the service IP) and the secondary CAM appliance (via its eth0 IP address).
CSCsu46341	No	NAC Profiler documentation does not list port for NetFlow NDE CAS receives Documentation does not list what port is used to receive NetFlow/NDE from a switch/router. When configuring the device to send to the CAS Collector this information is needed and not documented. **Conditions** With the use of NetFlow/NDE from a router/switch to the CAS Collector **Workaround** When configuring NetFlow on the switch/router the NDE should be sent to CAS Collector service IP with port 2055.

Table 7 List of Open Caveats- Documentation (Sheet 2 of 7)

DDTS Number	Software Release- Cisco NAC Profiler Version 2.1.8-39	
	Corrected	**Caveat**

CSCsu46361	No	Collector doc should state to check Collector services after install
		After configuring CAS Collector modules, eth3 and the modules are not started and require a manual restart.
		Conditions When first configuring CAS Collector modules.
		Workaround Manually check and start the Collector services if needed using the Collector CLI:
		`service collector status`
		`service collector start`

CSCsu46400	No	NAC Profiler guide should indicate SNMP trap versions The NAC profiler documentation (Page 3-4 SNMP Trap Configuration) does not currently list the supported version of SNMP traps sent from a switch and then processed via the CAS Collector. • Version 2.1.8-37 supports SNMP version 1 traps and v2c (patch needed) • Version 2.1.8-38 and later support v1 and v2c natively **Conditions** When using SNMP traps (link up/down, MAC-notification) sent from a switch to a CAS Collector. **Workaround** None **Note** See also CSCsw70337, page 40.

CSCsv46507	No	Profiler to CAM SSH key setup secure copy is missing file destination
		Symptom Secure copy of cleanaccess.conf will fail if using instructions from Profiler install and config guide.
		Conditions Copying cleanaccess.conf from primary to secondary Profiler using the command:
		`scp PRIMARY_IP:/usr/beacon/config/cleanaccess.conf`
		Workaround Add in the destination file to the secure copy command to complete the copy:
		`scp PRIMARY_IP:/usr/beacon/config/cleanaccess.conf cleanaccess.conf`

Table 7 List of Open Caveats- Documentation (Sheet 3 of 7)

	Software Release- Cisco NAC Profiler Version 2.1.8-39	
DDTS Number	**Corrected**	**Caveat**
CSCsv69829	No	Profiler doc incorrectly states IP helper traffic is sent to Profiler When configuring the NetWatch to support IP helper, the Profiler guide incorrectly states to use the NAC Profiler interface **Conditions** Page 1-6 2nd para, 1st line. Alternatively, DHCP redirection (sometimes referred to as IP Helper addressing) on the LAN-facing router interface can be utilized to forward a carbon copy of all DHCP requests from the LAN(s) served by that router interface directly to the management interface on a NAC Profiler running NetWatch. **Workaround** Change to the "NAC Profiler Collector running NetWatch." Be aware that eth0 of a CAS Collector is not supported for NetWatch (if running multicast such as HSRP); see defect CSCsm20254, page 29.
CSCsw70337	No	NAC Profiler install and config guide page 31 send traps to profiler is wrong **Symptom** Guide says to direct certain traffic to NAC Profiler IP **Conditions** Page 31 section 3-4 of Profiler 2.1.8 guide. The following notes provide instruction for configuration access switches to send desired traps to Cisco NAC Profiler. (config)# snmp-server enable traps mac-notification (config)# snmp-server enable traps snmp linkup linkdown (config)# snmp-server host <NAC Profiler-IP-address> traps version 1 <community-string> mac-notification snmp **Workaround** Direct traffic to NAC Profiler Collector IP and not <NAC Profiler-IP-address>. All communication from SNMP, IP Helper, etc should be directed to the Collector (Service IP in HA failover setup) and not the Profiler. See also CSCsu46400, page 39.

Table 7 List of Open Caveats- Documentation (Sheet 4 of 7)

DDTS Number	Software Release- Cisco NAC Profiler Version 2.1.8-39 Corrected	Caveat
CSCsw70447	No	NAC Profiler configuration guide page 6-16 IP addresses incorrect **Symptom** P. 6-16, Add Network Connection, Client Type, for CAS/Collector HA Pair. "Step 4: Note: When the Client radio button is selected, the add network connection form changes as shown in Figure 6-10. Note that the Allow Connections From section is shown at the bottom of the form. For standalone appliances, this should be populated with the loopback address (127.0.0.1) and the IP address of the eth0 interface of the Profiler Server. For HA Profiler Server pairs, the loopback and the eth0 interface addresses of both appliances should be displayed." **Conditions** Add Network Connection, Client Type, for CAS/Collector HA Pair. **Workaround** SHOULD BE: the loopback, VIP, and the eth0 interface addresses. The screen shot should reflect that both Eth0 and the service IP are listed on the Profiler GUI. The .6 and .8 are eth0 and .7 is the service IP

CSCsw70496	No	NAC Profiler configuration guide page 7-5 step 3a verify Collector name
		
		Symptom Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8 March 2008, Page 7-5 step 3a
		"To verify the hostname on a NA C Profiler, start a console or SSH session as user beacon, and enter the command 'hostname' at the prompt. The system will echo the current hostname."
		
		Workaround This should be connect to the CAS or one of the CAS in a pair (page 7-10 step 2) and use this command:
		
		`[root@cas1 beacon]# service collector verify`
		`Collector Network Configuration`
		`Collector Name = cas`
		Sections 3c and d should be subsections of 3b since they are configured under the forwarder configuration.

CSCsw70511	No	NAC Profiler configuration guide page 7-8 note wording incorrect **Workaround** page 7-8 change "must use be" to "must be" Note: When a Collector is implemented an HA-CAS pair, the Collector must use the Server Connection type, and the Server must use be configured as a Client Connection type.

Table 7 List of Open Caveats- Documentation (Sheet 5 of 7)

	Software Release- Cisco NAC Profiler Version 2.1.8-39	
DDTS Number	**Corrected**	**Caveat**
CSCsw70536	No	NAC Profiler configuration guide page 7-10 step 4,5,6 needs more detail **Symptom** Figure 7-3 is the figure of a contacted Collector. Note it is confusing since the steps were to add a Collector and it is not running until you apply changes per page 7-10 step 4,5 ,6. **Conditions** At this point since no modules are configured the status of the table of Collectors will show: One or More Modules Reporting an Error. **Workaround** Refer to the troubleshooting section or explain that the modules need to have a basic setup to show All Modules Running. The steps are not complete.
CSCsw70579	No	NAC Profiler configuration guide page 10-4 should state NAC Profiler page 10-4, Configuring Profiler Events, 1st and 2nd paragraph mention Profiler Events, needs to be changed to NAC Profiler Events. Figure 10-1 image for Profiler Events is old, it is now NAC Profiler Events, there are possibly other screen shots or text that need to change throughout the doc.
CSCsw70591	No	NAC Profiler configuration guide figure 11-2 2nd box label incorrect Figure 11-2 2nd box is now “Matches NAC Profiler Profiles”, old guide has “Profiler Profiles.” The next page paragraph for Profile Profiles should be changed to reflect this.
CSCsw85307	No	Profiler guide needs section for DHCP request directed to CAS Collector **Symptom** NAC profiler guide contains no guidance on the configuration of IP helper directed to Netwatch **Conditions** When configuring the switch to forward IP helper (DHCP request) redirection to the Collector **Workaround** This information is in the release notes for the NAC Profiler release 2.1.8-38

Table 7 List of Open Caveats- Documentation (Sheet 6 of 7)

DDTS Number	Software Release- Cisco NAC Profiler Version 2.1.8-39	
	Corrected	**Caveat**
CSCsx03759	No	Profiler: Event logic Profiler match needs a note stating / is required **Symptom** Profiler does not produce error message when a forward slash (“/”) is missing in the event match field. **Conditions** When adding a NAC event on Profiler, If you do not start and end the search criteria with a forward slash Profiler will accept this and not match any profiles. **Workaround** Use a forward slash to begin and end your search criteria.
CSCsy03646	No	NAC Profiler HA license requirements **Symptom** Based on CCO documentation it is not clear which License files are required for Profiler HA / Collector HA setup. http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/license.html#wp39197 •For NAC Profiler or NAC Profiler Failover (HA) licenses, submit the eth0 MAC address of the Primary NAC Profiler Server. •For NAC Profiler Failover (HA) license only, submit the eth0 MAC address of the secondary NAC 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 One Collector HA LIC file based on MAC address primary Profiler eth0 could lead to a cosmetic bug CSCsq42942, page 22.

Table 7 List of Open Caveats- Documentation (Sheet 7 of 7)

	Software Release- Cisco NAC Profiler Version 2.1.8-39	
DDTS Number	**Corrected**	**Caveat**
CSCta06865	No	Profiler Documentation does not cover configuring Failover NAC Managers **Symptom** NAC Profiler Documentation does not cover adding HA NAC Managers to the Profiler configuration. **Conditions** NAC Profiler 2.1.8 **Further Problem Description** Add the Manager Service IP/DNS Name followed by the Secondary Manager IP/DNS Name and separate them by a comma, for example: NACServiceIP.cisco.com,NACSecondaryIP.cisco.com.

Resolved Caveats - Documentation

Table 8 List of Resolved Caveats - Documentation (Sheet 1 of 3)

	Software Release- Cisco NAC Profiler Version 2.1.8-39	
DDTS Number	**Corrected**	**Caveat**
CSCsm83238	Yes	SSL certificate web management Currently there is no documented method to replace the default SSL certificate on NAC profiler. **Workaround** Detailed instructions to import SSL certificates and replace the default certificate are documented on Cisco.com in the *Importing SSL Certificates to NAC Profiler* tech note available at: http://www.cisco.com/en/US/products/ps6128/products_configuration_example09186a00809f0e60.shtml **Note** See also CSCsm72012, page 30.

Table 8 List of Resolved Caveats - Documentation (Sheet 2 of 3)

	Software Release- Cisco NAC Profiler Version 2.1.8-39	
DDTS Number	**Corrected**	**Caveat**
CSCsq63961	Yes	Documentation does not say how to find ifIndex used with Port Filter The following link explains how to configure Profiler Events and enable events per Network Device: http://www.cisco.com/en/US/docs/security/nac/profiler/configuration_guide/218/p_prof_events.html. Refer to section "Enable Events per Network Device" and refer the Note under that section that says: "Note The syntax for the Port Filter list is the ifIndex of the port(s) to be excluded from event enablement. Individual ports can be specified separated by commas (e.g., 1,5,11, etc.) and or ranges of ifIndices (e.g., 1-5,7,8, etc.)" Note does not say how to find out ifIndex. The following should be added to the Note section: "ifIndex can be found from the following location. Endpoint Console--->View Manage Endpoints-->Display Endpoints by Device Ports and click on Ungrouped. Then click on "view" under port control. First column lists physical port and ifIndex in bracket."
CSCsr40160	Yes	Profiler: Doc should list XML fields that can be used in Advanced Rule Documentation should detail a list of the XML fields that can be used in an Advanced Rule. **Workaround** Section Appendix A, "Advanced XML Rules" is added to 2.1.8 config guide: http://www.cisco.com/en/US/docs/security/nac/profiler/configuration_guide/218/p_apx_xml_rules.html

Table 8 List of Resolved Caveats - Documentation (Sheet 3 of 3)

	Software Release- Cisco NAC Profiler Version 2.1.8-39	
DDTS Number	**Corrected**	**Caveat**
CSCsw70085	Yes	NAC Profiler configuration guide table 2-7 wording for operating mode #3 **Symptom** Documentation explanation of operating mode #3 inaccurate **Conditions** The mode or state of the clients does not determine what traffic can be seen by the collector netwatch. If netwatch is running on eth2/3 then it will only see what traffic the span/monitor session is sending to it. It is probably good practice not to span the authenticated vlan for regular users. It would be good to span the auth vlan plus the printer vlan (and any other special purpose networks) in case a machine masquerading as a simple device suddenly exhibits a PCs behavior and then profiled to be put in the auth vlan. **Workaround** Corrections provided in the 2.1.8-38 Release Notes, Table 2 “Collector Modules and NAC Appliance Server Operating Mode” at http://www.cisco.com/en/US/docs/security/nac/profiler/release_notes/218/218rn.html#wp123816 and in the 2.1.8 Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8 in Table 7-2, http://www.cisco.com/en/US/docs/security/nac/profiler/configuration_guide/218/p_cfgpcol.html#wpxref63610

New Installation of Release 2.1.8

If performing a new CD installation of the Cisco NAC Profiler software on the Cisco NAC Profiler Server or Cisco NAC "Profiler Lite" Server, use the steps described below.

If performing upgrade on an existing Cisco NAC Profiler system, refer to the instructions in Upgrade Instructions for Release 2.1.8, page 48.

Note To support Cisco NAC Profiler release 2.1.8, your CAM and CAS must already be configured and running the latest supported Cisco NAC Appliance release (4.1.2.1 is the minimum) and the Collector component must be upgraded on the CAS to the appropriate version as described in Software Compatibility, page 3 and Upgrading Collector Service on CAS, page 53.

Note The Profiler Lite appliance platform is supported starting from release 2.1.8-37 and later and requires a separate ISO file. Only the **nac_profilerlite_2.1.8-37-K9.iso** file (or later) 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.)

Step 2 Log into the Security Software download site for Cisco NAC Appliance and download the latest Cisco NAC Profiler ISO image from http://www.cisco.com/kobayashi/sw-center/ciscosecure/cleanaccess.shtml

- For standard Profiler Server, download the latest **nac-profiler_2.1.8-37-K9.iso**
- For Profiler Lite, download the latest **nac_profilerlite_2.1.8-37-K9.iso**

Note Version 2.1.8-38 and 2.1.8-39 are available as software upgrade files only. See Upgrade Instructions for Release 2.1.8, page 48 for details.

Step 3 Burn the ISO as a bootable disk to a CD-R.

Step 4 Insert the CD into the CD-ROM drive of each installation server, and follow the instructions in the auto-run installer. Refer to the Installation and Initial Configuration chapter of the *Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8* for complete installation instructions for both standalone and high availability (HA) Profiler Servers.

Step 5 Log into the web console for the Profiler Server (default username/password: **admin/profiler**) and navigate to **Home > Upload License** to install license files for your Cisco NAC Profiler deployment. For details, refer to section "*How to Obtain and Install New Cisco NAC Profiler Server/Collector Licenses*" at http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/license.html#wp39197

Step 6 Upgrade the Collector component on each Clean Access Server to the appropriate version as described in Upgrading Collector Service on CAS, page 53.

Step 7 Continue the configuration of your Cisco NAC Profiler deployment from the Profiler Server web console as described in the *Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8.*

Upgrade Instructions for Release 2.1.8

This section provides instructions for how to upgrade the Cisco NAC Profiler Server and the Cisco NAC Profiler Collector component on the CAS to the latest version of the software.

Note To support Cisco NAC Profiler release 2.1.8, your CAM and CAS must already be configured and running the latest supported Cisco NAC Appliance release (4.1.2.1 is the minimum) and the Collector component must be upgraded on the CAS to the appropriate version as described in Software Compatibility, page 3 and Upgrading Collector Service on CAS, page 53.

Note The Profiler Lite appliance platform is supported starting from release 2.1.8-37 and later and requires a separate ISO file. Only the **nac_profilerlite_2.1.8-37-K9.iso** file (or later) 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 Cisco NAC Profiler Server include both standalone and HA-pair configurations and explain the HA Failover procedure.

Overview

Note The Release upgrade files for the Cisco NAC Profiler Server and Cisco NAC Profiler Collector are available from Cisco Secure Software at http://www.cisco.com/cgi-bin/tablebuild.pl/nacprofiler-2.1.8

You must login with your Cisco registration user name and password to download the files.

- The upgrade file for the Cisco NAC Profiler Server is a single compressed format (.zip) file
- The Collector RPM is a complete package that can be used to upgrade an existing Collector service on a Clean Access Server to the latest version of the Collector. It can also be used for a “fresh” install on a CAS that does not have the Collector service running on it.

Note An MD5 checksum is posted along with each upgrade package to ensure file integrity. When clicking through the screens prior to software download, take note of the MD5 value in the Details table. Verify this against the MD5 checksum provided with the upgrade package to ensure the upgrade files are not corrupted before you start.

The Cisco NAC Profiler Server software upgrade package includes all necessary files for upgrading the Profiler Server software, underlying components, and the database. The filename of the upgrade package indicates the latest version of the Profiler Server, for example:

nac-profiler_upgrade-2.1.8-39-K9.zip

Caution Cisco highly 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 Cisco NAC Profiler Servers and Collectors in the system to bring all components to the most current version.

Caution The procedures for upgrading Profiler Server are different for systems operating in HA mode. Refer to Upgrading Profiler Server HA Pairs, page 50 for instructions specific to the upgrade of HA Profiler Server pairs.

Upgrading Profiler Server Standalone Systems

Upgrading the software on standalone Profiler Server systems is a straightforward process. The upgrade script automatically upgrades all installed components as needed. Follow the steps below to upgrade standalone Profiler Servers.

Step 1 Download the latest upgrade package for Cisco NAC Profiler Version 2.1.8 from Cisco Secure Software by logging into http://www.cisco.com/cgi-bin/tablebuild.pl/nacprofiler-2.1.8:

nac-profiler_upgrade-2.1.8-39-K9.zip

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

Step 2 SCP the upgrade package.zip file to the /home/beacon directory of the Profiler Server to be upgraded.

Step 3 Connect to the Profiler Server being upgraded via SSH. Login as user beacon with the beacon user password (default is profiler).

Step 4 Elevate to root user using the su - command and enter the password for the root user:

```
[beacon@profiler ~]$ su - root
Password:
```

Step 5 Change directory to **/home/beacon**

```
cd /home/beacon
```

Step 6 Verify the MD5 checksum of the upgrade package against the checksum specified for the file on Cisco Software Download. Use the following command to generate the checksum of the file on the Profiler Server:

```
md5sum nac-profiler_upgrade-2.1.8-39-K9.zip
```

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

Step 7 Unzip the upgrade package:

```
unzip nac-profiler_upgrade-2.1.8-39-K9.zip
```

This command uncompresses the files required for upgrade, and creates a new subdirectory named ProfilerUpgrade-2.1.8-39 in the /home/beacon/ directory.

Step 8 Change directory to the ProfilerUpgrade directory created when the upgrade package was unzipped:

```
cd ProfilerUpgrade-2.1.8-39
```

Step 9 The directory should include a script named upgrade.pl. Execute the upgrade script by entering the following command:

```
./upgrade.pl
```

Step 10 During the upgrade process, several messages may be sent to the console indicating progress as installed components are upgraded. When the update script completes successfully, the Profiler service(s) running on the system restart at the following message, followed by the return of the system prompt:

```
To modify the configuration of the Profiler, use 'service profiler config'
```

Step 11 Verify the successful upgrade of the system by entering the 'service profiler status' command:

```
service profiler status
```

The output includes the current version of the Profiler Server, and should indicate Running status for the Server module on the system.

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

Profiler Status
   Version: Profiler-2.1.8-39

  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
```

Upgrading Profiler Server HA Pairs

When upgrading the software on a HA Profiler Server pair, you must upgrade the Secondary appliance in the pair first, then perform upgrade on the Primary appliance. In the process of the upgrade, the system that was the Secondary prior to the upgrade will take over the functions of the Primary, similar to what would occur in the event of the failure of the Primary.

Caution Upgrading the Profiler software on a HA pair should 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.

Note 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 member that was Primary prior to the upgrade back to that state.

Use the following procedures to upgrade the Cisco NAC Profiler Server software on the HA-Profiler pair.

Step 1 Download the latest upgrade package for Cisco NAC Profiler Version 2.1.8 by logging into Cisco Secure Software at http://www.cisco.com/cgi-bin/tablebuild.pl/nacprofiler-2.1.8:

nac-profiler_upgrade-2.1.8-39-K9.zip

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

Step 2 SCP the upgrade package.zip file to the /home/beacon directory of each Profiler Server in the HA pair to be upgraded. (Use the eth0 interface IP address for each appliance in the pair. Do not use the VIP.)

Step 3 Determine which appliance is currently the Secondary appliance in the pair.

Step 4 SSH to the IP address of the eth0 interface on the Secondary system being upgraded, and elevate to root user 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 Cisco Software Download.Use the following command to generate the checksum of the file on the target system:

```
md5sum nac-profiler_upgrade-2.1.8-39-K9.zip
```

This command will calculate and display the checksum of the file to the console so it can be checked against the one supplied with the file.

Step 6 Unzip the upgrade package (unzip nac-profiler_upgrade-2.1.8-39-K9.zip). This will uncompress the files required for upgrade, and create a new subdirectory in named ProfilerUpgrade-2.1.8-39 in the beacon/home directory.

Step 7 Change directory to the ProfilerUpgrade-2.1.8-39 directory created when the upgrade package was unzipped.

Step 8 The directory should include a script named upgrade.pl. Execute the upgrade script by entering the following command:

```
./upgrade.pl
```

Step 9 During the upgrade process, several messages may be sent to the Console indicating progress of the upgrade as installed components are upgraded. When the update script completes successfully, the Profiler service(s) running on the system will be restarted at the following message displayed:

```
To modify the configuration of the Profiler, user 'service profiler config'
```

Followed by the return of the system prompt.

Step 10 Verify the successful upgrade of the system by entering the 'service profiler status' command. The output will include the current version of the Profiler system, and should indicate the Running status for the installed module(s) on the system.

Step 11 This completes the upgrade of the software on the original Secondary appliance.

Proceed with performing the upgrade process on the appliance that was Primary at the outset of the upgrade procedure by following the steps above. The original Primary should now be the Secondary after the failover initiated by the upgrade script completing on the original Secondary.

Once the second appliance has been successfully upgraded, both members of the HA pair are now at the new revision. To restore the pair to the state prior to the upgrade, making the original Primary the Primary for the pair again, failover the system manually using the HA Failover Procedure, page 52 (if desired).

HA Failover Procedure

When performing the failover procedure, either after the initial configuration of an HA pair, or after an induced failover within the HA pair, you must allow enough time for the database synchronization to complete fully before failing the system over again.

Note The time required for database synchronization depends on the database size. In most cases, Cisco recommends allowing 15-30 minutes to elapse after initial HA configuration or a forced failover before failing the system over again.

Caution Repeatedly forcing an HA pair to fail over without providing ample time for the system to stabilize will result in undesirable behavior and may require removing and re-configuring the HA protocol in order to return the HA subsystem to stable operation.

Follow the procedure below to force the failover of an HA pair:

Step 1 SSH to the eth0 interface of the current Primary appliance in the HA pair that is to be failed over as user beacon. The SSH session should be to the eth0 interface IP and not the VIP so that the session will remain active through the failover.

Step 2 Change directory to /usr/beacon/sql, and run `./chk_status_master.sh` to verify that the system you are currently on is Primary (script returns “is master”).

Step 3 Switch user to root via `su -`

Step 4 SSH to the eth0 interface of the other appliance in the pair, the current Secondary which will become Primary upon the failover.

Step 5 Change directory to /usr/beacon/sql, and run `./chk_status_master.sh` to verify that the system is in fact currently the Secondary (script returns “is slave”).

Step 6 When ready to failover the pair, return to the SSH session on the current Primary, then enter the following command to temporarily stop the heartbeat from the Primary to the Secondary which will induce the desired failover:

```
service heartbeat stop
```

Step 7 Wait several seconds then return to the SSH session to the former Secondary, which now should be the current Primary. Verify that is the case by running `./chk_status_master.sh` to verify that the system is now the Primary (script returns “is master”).

Step 8 On the former Primary which now should be the Secondary, run the following command as root to start the heartbeat again:

```
service heartbeat start
```

Step 9 Exit back to the beacon user then run `./chk_status_master.sh` to verify that the system is currently the Secondary (script returns “is slave”). This indicates that the system successfully failed over.

At this juncture the system should now be operating in HA mode after the swap of the Primary duties.

Upgrading Collector Service on CAS

Upgrading the Collector service on a Clean Access Server NAC Appliance is accomplished via a single RPM file. The Collector RPM is a complete package that can be used to upgrade an existing Collector service on a Clean Access Server to the latest 2.1.8 version. It can also be used for a "fresh" install on a CAS that does not have the Collector service running on it. Use the following steps to upgrade the Collector.

Step 1 Download the latest Collector RPM file (e.g. **nac-collector-2.1.8-39-K9.rpm)** from the Cisco NAC Profiler Version 2.1.8 location on Cisco Secure Software http://www.cisco.com/cgi-bin/tablebuild.pl/nacprofiler-2.1.8.

Note Prior to download, 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 CAS/Collector(s) to be upgraded.

Note If the CAS/Collector is implemented as an HA pair, copy the upgrade file to each CAS appliance using the eth0 IP address of each CAS. Do not use the Service IP address of the HA-CAS pair.

Step 3 Initiate an SSH session to the Clean Access Server being upgraded and login as the root user with 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-2.1.8-39-K9.rpm
```

Step 5 Run the RPM file by issuing the following command:

```
rpm -Uhv nac-collector-2.1.8-39-K9.rpm
```

Step 6 The RPM will complete and the command prompt will return when completed successfully.

Step 7 Issue the following command to restart the Collector service on the CAS.

```
service collector start
```

Step 8 Issue the 'service collector status' command to verify the version and check the status of the Collector service.

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

Profiler Status
   Version: Collector-2.1.8-39

  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]#
```

Documentation Updates

Table 9 Updates to Release Notes for Cisco NAC Profiler, Release 2.1.8

Date	Description
11/4/09	Updates for Cisco NAC Profiler Release 2.1.8-39 • Cisco NAC Profiler Releases, page 2 • Hardware Supported, page 2 • Cisco NAC Appliance/ Cisco NAC Profiler Compatibility Matrix, page 3 • Enhancements in Cisco NAC Profiler Release 2.1.8-39, page 6 • Updated Open Caveats - Release 2.1.8-39, page 21 (added CSCsr91618, CSCsw30875, CSCsw97514,CSCsx03749, CSCsx42320, CSCsy84379, CSCta25695, CSCtb02389, CSCtb17189) • Updated Resolved Caveats - Release 2.1.8-38, page 29(moved CSCsm20254, CSCsm55679, CSCsm58145, CSCsm71798, CSCsm72012) • Updated Open Caveats - Documentation, page 38, added Resolved Caveats - Documentation, page 44; moved both tables to end of Caveats section.
1/20/09	• Updated NetWatch section of Table 2Collector Modules and NAC Appliance Server Operating Mode, page 4. • CSCsw70085 added to Resolved Caveats - Release 2.1.8-38, page 29
1/8/09	Added CSCsw85307 and moved CSCsm83238 to Open Caveats - Documentation, page 38. Format and hypertext link corrections.
12/22/08	Updates for Cisco NAC Profiler Release 2.1.8-38: • Cisco NAC Profiler Releases, page 2 • Hardware Supported, page 2 • Cisco NAC Appliance/ Cisco NAC Profiler Compatibility Matrix, page 3 • Enhancements in Cisco NAC Profiler Release 2.1.8-38, page 7 • CAS/Collectors Running in Real IP Gateway Mode, page 13 • Open Caveats - Release 2.1.8-39, page 21 • Open Caveats - Documentation, page 38 (added) • Resolved Caveats - Release 2.1.8-38, page 29 • New Installation of Release 2.1.8, page 47 • Upgrade Instructions for Release 2.1.8, page 48
10/3/08	Update Table 1 “Cisco NAC Appliance / Cisco NAC Profiler Compatibility Matrix” for Cisco NAC Appliance release 4.5.
7/31/08	Updated Table 1 “Cisco NAC Appliance / Cisco NAC Profiler Compatibility Matrix” for Cisco NAC Appliance release 4.1(6)

Table 9 Updates to Release Notes for Cisco NAC Profiler, Release 2.1.8

Date	Description
6/26/08	Updates for "Profiler Lite" hardware platform: • Hardware Supported, page 2. • Cisco NAC Appliance/ Cisco NAC Profiler Compatibility Matrix, page 3 • New Installation of Release 2.1.8, page 47 • Upgrade Instructions for Release 2.1.8, page 48 Corrected broken Cisco Secure Download links.
6/24/08	Updates for "Profiler Lite" hardware platform: Hardware Supported, page 2.
4/7/08	Updates for Cisco NAC Profiler Release 2.1.8-37: • Cisco NAC Profiler Releases, page 2 • Cisco NAC Appliance/ Cisco NAC Profiler Compatibility Matrix, page 3 • Enhancements in Cisco NAC Profiler Release 2.1.8-37, page 9 • Known Issues in Version 2.1.8, page 12 • Open Caveats - Release 2.1.8-39, page 21 (updated) • Resolved Caveats - Release 2.1.8-37, page 35 (new) • Upgrade Instructions for Release 2.1.8, page 48 (updated for build 37)
3/4/08	Cisco NAC Profiler Release 2.1.8-33

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/ps6128/tsd_products_support_series_home.html

or simply http://www.cisco.com/go/nac/appliance

- *Cisco NAC Profiler Installation and Configuration Guide, Release 2.1.8*
- *Release Notes for Cisco NAC Profiler, Release 2.1.8* (this document)
- *Release Notes for Cisco NAC Appliance*
- *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide*
- *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide*
- *Cisco NAC Appliance Service Contract / Licensing Support*

Obtaining Documentation and Submitting a Service Request

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

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

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

This document is to be used in conjunction with the documents listed in the Related Documentation, page 55 section.