Release Notes for Cisco NAC Profiler, Release 2.1.7

Revised: February 9, 2009, OL-14332-01

Contents

These release notes provide late-breaking and release information for Cisco NAC Profiler, release 2.1.7. 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.

Cisco NAC Profiler Releases

Cisco NAC Profiler Version	Release Date
2.1.7 ED	August 31, 2007

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

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 8 for additional details.

Hardware Supported

Cisco NAC Profiler Server

The Cisco NAC Profiler Server appliance is based on the NAC-3300 series platform and is shipped pre-installed with the Cisco NAC Profiler software.

Cisco NAC Profiler Collector

The Cisco NAC Profiler Collector component is automatically included on NAC-3310 and/or NAC-3350 SERVER appliances only starting from Cisco NAC Appliance release 4.1(2).

See also Enhancements for Cisco NAC Profiler Release 2.1.7, page 4.

Software Compatibility

This section describes the following:

NAC Appliance/ 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. Versions for each component displayed in the same row are compatible with one another. Cisco recommends that you synchronize your software images to match those shown as compatible in the table.

Table 1 Cisco NAC Appliance / Cisco NAC Profiler Compatibility Matrix

Clean Access Server [1]	Cisco NAC Profiler Collector (on CAS) [2]	Cisco NAC Profiler Server [3]
4.1(2)	**2.1.7**	2.1.7

1. Each Cisco NAC Appliance release includes the latest version of the Cisco NAC Profiler Collector component for the CAS. For example, Release 4.1(2) of the CAS automatically includes version 2.1.7 of the Cisco NAC Profiler Collector.
2. The Collector will be able to be upgraded independently to a later Cisco NAC Profiler release (e.g. 2.1.8) via RPM package installation on the CAS.
3. The Profiler Server will be able to be upgraded independently to a later Cisco NAC Profiler release (e.g. 2.1.8) via ISO file installation.

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, 3]				
• Observe traffic on eth2 (can be HA heartbeat)	Yes [4]	Yes [4]	Yes [4]	Yes [4]
• Observe traffic on eth3	Yes	Yes	Yes	Yes
NetInquiry Active Profiling of endpoints	Yes	Yes[1]	Yes	Yes [5]
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 [5]).
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 the *Release Notes for Cisco NAC Profiler Release 2.1.8* for additional information.

3. For an OOB deployment, NetWatch can observe the endpoint traffic types only while an endpoint is in the untrusted state (with traffic contained to flow In-Band through the CAS). An endpoint that has completed the OOB logon/posture assessment process no longer sends traffic through the CAS.
4. 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.
5. 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
- Cisco NAC Profiler Collector (on CAS)

Cisco NAC Profiler Server

From Web UI:

1. Open a web browser and type the NAC Profiler Server's address as the URL: **https://<Profiler_address>/profiler/**.
2. Login as user **admin** (default password: **profiler**).
3. Navigate to **Home > Getting Started**. The software version installed is listed at the top of the page.

Via SSH

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

```
[root@profiler ~]# service profiler status
Profiler Status
   Version: Profiler-2.1.7-15
  o Server      Running
```

- Or, SSH to the NAC Profiler Server and type **`rpm -q Profiler`**.

Cisco NAC Profiler Collector (on CAS)

- SSH to the Clean Access Server machine running the Collector service and type **`rpm -q Collector`**.

New and Changed Information

This section describes enhancements added to the per release of Cisco NAC Profiler for the NAC Profiler Server and NAC Profiler Collector.

- Enhancements for Cisco NAC Profiler Release 2.1.7, page 4

Enhancements for Cisco NAC Profiler Release 2.1.7

Cisco NAC Profiler, release 2.1.7 leverages the Cisco NAC Appliance 3300 Series hardware platforms.

For release 2.1.7, the Cisco NAC Profiler **Server** appliance leverages the NAC-3350 SERVER platform and is pre-installed with the Cisco NAC Profiler software.

The Cisco NAC Profiler **Collector** component is available on the Clean Access Server starting from Cisco NAC Appliance release 4.1(2), and operates on the NAC-3310 and/or the NAC-3350 Appliance platforms only.

See also Hardware Supported, page 2.

Known Issues

This section describes the following:

Refer also to Open Caveats - Release 2.1.7, page 8 for additional important information.

Known Issues for Collector Modules

- NetFlow in not supported on the NAC Profiler Collector in version 2.1.7.
- NetMap (SNMP) polling of Cisco Catalyst 1900 and 2960 switches does not return the expected results.
- If the ifindex does not equal the bridging number in the MAC Notification Trap (used by the NetTrap Module), the resulting discovery will not function (e.g. Cisco 2960).

MAC Address Format

All MAC addresses in the Profiler Server database are in the format: aa: bb:00:11:22:33. If a Static MAC rule is defined within a Profile and the MAC address for the rule (MAC to match) is written with uppercase letters for hexadecimal values, it will not match the MAC address in the database.

When creating profiles under Profiler -> Endpoint Profiles, make sure to replace uppercase letters in the MAC address with lower case letters to ensure the CAM Device Filter can be updated by Profiler.

Use of "Custom API" Feature

The Custom API feature of the Cisco NAC Profiler Server (**Configuration > Profiler Modules > List Profiler Modules > "Server" > NAC Configuration | Custom API (Advanced)**) should only be implemented in specific situations as described in Cisco NAC Profiler documentation, or as directed by Cisco TAC.

Caution Cisco TAC does not support the running of tools/reports against or any other manipulation of the Cisco NAC Profiler Server postgres database.

Whenever upgrading Profiler or NAC Appliance (CCA) software, carefully consult these release notes to determine whether it is appropriate to enable or disable the Custom API.

Cisco recommends use of the Custom API for the following specific scenarios. Each scenario requires its own patch file to be used to enable the Custom API:

- CCA v4.0, Access Types CHECK and IGNORE
- CCA v4.1.x, Out-of-Band deployments

CCA v4.0, Access Types CHECK and IGNORE

The Cisco NAC Appliance API for release 4.0 does not support Device Filter List access types CHECK and IGNORE.

If either of these access types to be used with NAC-Event-Rules, then the Custom API must be enabled, using patch file **cca4_api_addmac.diff**. Refer to Implementing Custom API, page 6.

CCA v4.1.x, Out-of-Band deployments

Typically, when Profiler Behavior Monitoring is in use, any access provisioned via Profiler/NAC integration is immediately updated when an endpoint's profile changes. For example, with a typical behavior monitoring deployment, a “Printer” that is suddenly observed to exhibit user-like behavior will have its network access immediately revoked.

Currently, in NAC Appliance Out-of-Band (OOB) deployments when a Device Filter List entry is removed or changed, this immediate adjustment to an OOB endpoint's network access does not occur. If this behavior is desired, then the Profiler Server Custom API must be enabled, using patch file **cca41x_api_bounceport.diff**. Refer to Implementing Custom API, page 6.

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

- Cisco Clean Access v4.1.1
- Cisco Clean Access v4.1.2

Implementing Custom API

Prerequisite

Configure Cisco NAC Profiler / Cisco NAC Appliance integration before enabling the Custom API.

Enable Custom API

Perform the following steps to enable the Custom API.

Note

- PATCH_FILE is the selected patch file (either **cca4_api_addmac.diff** or **cca41x_api_bounceport.diff**)
- CAM is the IP or DNS address of the Clean Access Manager system.

Step 1 **Patch API File**

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

a. `profiler# cd /usr/beacon/etc`

b. `profiler# scp root@CAM:/perfigo/control/tomcat/normal-webapps/admin/cisco_api.jsp cisco_api.jsp`

c. `profiler# patch < cca_api/PATCH_FILE`

d. `profiler# scp cisco_api_alt.jsp root@CAM:/perfigo/control/tomcat/normal-webapps/admin/`

Step 2 **Patch ssl.conf**

Note This step is not needed for Scenario A (CCA v4.0, Access Types CHECK and IGNORE, page 6), but is required for all others.

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

a. `profiler# cd /usr/beacon/etc`

b. `profiler# scp root@CAM:/perfigo/control/apache/conf/ssl.conf ssl.conf`

c. `profiler# patch < cca_api/cca41x_ssl_conf.diff`

d. `profiler# scp ssl.conf root@CAM:/perfigo/control/apache/conf/ssl.conf`

Step 3 **Turn on Feature**

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

a. Browse to Server module configuration screen via **Configuration > Profiler Modules > List Profiler Modules > "Server"**

b. In the **NAC Configuration** section of the **Configure Server** page that appears, enable the checkbox labeled **Custom API**.

c. Click **Update Server**.

d. Restart the Server module via **Configuration >Apply Changes > Re-Model**.

Caveats

This section describes the following caveats.

- Open Caveats - Release 2.1.7

Note If you are a registered cisco.com user, you can view Bug Toolkit on cisco.com at the following website: http://www.cisco.com/pcgi-bin/Support/Bugtool/home.pl

To become a registered cisco.com user, go to the following website: http://tools.cisco.com/RPF/register/register.do

Note For caveats related to Cisco NAC Appliance, see the applicable *Release Notes for Cisco NAC Appliance (Clean Access)* at http://www.cisco.com/en/US/products/ps6128/prod_release_notes_list.html

Open Caveats - Release 2.1.7

Table 3 List of Open Caveats (Sheet 1 of 2)

	Software Release- Cisco NAC Profiler v2.1.7	
DDTS Number	Corrected	Caveat
CSCsk25865	No	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). Also there shouldn't be any colons in between. If necessary, simply edit the format of the MAC address to correct this issue.
CSCsk25881	No	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 3 List of Open Caveats (Sheet 2 of 2)

	Software Release- Cisco NAC Profiler v2.1.7	
DDTS Number	**Corrected**	**Caveat**
CSCsl23121	No	Add device to Filter list by Profiler doesn't trigger Switch port change Symptom: 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 doesn't have access to the network Workaround: None.
CSCsl59431	No	Devices in L3 IB NAC deployments can't be added/removed from CAM filter list Devices in L2 can be added and 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 addip/removeip type of APIs to add IP addresses to the IP filter list. This is not currently done for L3 IB devices.

Documentation Updates

Table 4 Updates to Release Notes for Cisco NAC Profiler, Release 2.1.7

Date	Description
11/11/08	• Removed "Clean Access Server on CCA-3140-H1" section
6/24/08	• Updated Hardware Supported section.
3/3/08	• Updated Collector Support and CAS Deployment Modes, page 3 • removed CSCsk25881 from List of Open Caveats and added known issue, MAC Address Format, page 5. • Updated boilerplate
12/4/07	Added caveats CSCsl20885, CSCsl23121, CSCsl59431 to List of Open Caveats.
11/02/07	Update to caveat CSCsk25865, page 8. Repost to new category.
8/31/07	Cisco NAC Profiler Release 2.1.7

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 Notes for Cisco NAC Profiler, Release 2.1.7* (this document)
- *Release Notes for Cisco NAC Appliance, Release 4.1(2)*
- *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(2)*
- *Cisco NAC Appliance - Clean Access Server Installation and Configuration Guide, Release 4.1(2)*
- *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" section.