Release Notes for Cisco NAC Profiler, Release 3.1.0

Revised: March 2, 2010, OL-20644-01

Contents

These release notes provide late-breaking and release information for Cisco NAC Profiler, release 3.1.0. 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
3.1.0-24 ED	March 2, 2010

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

Note Cisco recommends that you deploy Early Deployment releases in test network before deploying in a production network.

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*.

Hardware Supported

The Cisco NAC Profiler system consists of a Cisco NAC Profiler Server or Cisco NAC Profiler Lite Server, implemented as a standalone appliance or High Availability (HA) pair, and one or more Profiler Collectors that run on NAC Server appliances (NAC-3310 or NAC-3350). The Profiler Collectors can also be deployed as HA pairs when run on NAC Server HA pairs.

The Cisco NAC Profiler appliances leverage the Cisco NAC Appliance 3300 Series hardware platforms.

Cisco NAC Profiler Server

The Cisco NAC Profiler Server 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 is based on the NAC-3310 hardware platform and is also pre-installed with a default version of the Cisco NAC Profiler Lite software. Profiler Lite requires a separate ISO file.

Cisco NAC Profiler Collector (on Cisco NAC Server)

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

Note For proper operation, both the Profiler Collector component on the NAC Server and Cisco NAC Profiler Server (Profiler Server or Profiler Lite) **must** run the same version of the Cisco NAC Profiler software. Refer to Cisco NAC Appliance/ Cisco NAC Profiler Compatibility Matrix, page 3 for details.

Note You need to upgrade the default version of the Profiler Collector shipped with the NAC Server software for compatibility with the latest Cisco NAC Profiler release 3.1.0. For details refer to Cisco NAC Appliance/ Cisco NAC Profiler Compatibility Matrix, page 3.

See New and Changed Information, page 7 for details on the latest release 3.1.0 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 and Cisco NAC Profiler compatibility and software versions supported for each component of the Cisco NAC Profiler solution. For proper operation, both the Profiler Collector(s) and Profiler Server (Profiler Server or Profiler Lite) **must** run the same version of the Cisco NAC Profiler software.

Note Cisco NAC Profiler release 3.1.0 replaces and supersedes **all** previous releases. If running Cisco NAC Profiler release 2.x, upgrade your Cisco NAC Profiler appliance and Profiler Collector components to the latest available supported 3.1.0 release build.To upgrade a Cisco NAC Profiler system running version 2.1.8 or earlier to the Cisco NAC Profiler 3.1.0 release, refer to Upgrade Instructions for Release 3.1.0-24, page 22.

Note Cisco NAC Appliance 4.7 releases are shipped with Collector version 2.1.8-39 by default. When upgrading the NAC Server to a newer Cisco NAC Appliance release, the current version of the Collector is replaced with the default version of the Collector shipped with the Cisco NAC Appliance release. For example, if you are running NAC 4.7(1) and Profiler 3.1 and you upgrade to NAC 4.7(2), you need to manually re-install the 3.1.0 Collector and configure it after the NAC Server upgrade.

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

Cisco NAC Server Appliance Components[2]			Cisco NAC Profiler Appliance
Cisco NAC Appliance Version	**Cisco NAC Profiler Collector Version Shipped with Cisco NAC Server**	**Upgrade Cisco NAC Profiler Collector Version to: [3]**	**Upgrade Cisco NAC Profiler Server and Cisco NAC Profiler Lite[4] Server Version to:**
4.7(2)	2.1.8-39	3.1.0-24[5]	3.1.0-24
4.7(1)	2.1.8-39		
4.6(1)	2.1.8-37		

1. The Collector component and the Profiler Server **must** run the same version of the Cisco NAC Profiler software to inter-operate (e.g. 3.1.0-24).
2. Each version of the NAC Server software is shipped with a default version of the Profiler Collector component starting from Cisco NAC Appliance release 4.1.2.1 and later. The Profiler Collector can be upgraded independently of the NAC Server software for compatibility with a later Profiler Server/Profiler Lite Server release.

3. You must upgrade the Collector component on each NAC Server as described in Installing New/Upgrading Cisco NAC Profiler Collector Service on Cisco NAC Server, page 33.
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-3.1.0-24-K9.iso** file (or later) can be installed on the Profiler Lite platform. See Hardware Supported, page 2.
5. Cisco NAC Appliance 4.7 releases are shipped with Collector version 2.1.8-39 by default. When upgrading the NAC Server to a newer Cisco NAC Appliance release, the current version of the Collector is replaced with the default version of the Collector shipped with the Cisco NAC Appliance release. For example, if you are running NAC 4.7(1) and Profiler 3.1 and you upgrade to NAC 4.7(2), you need to manually re-install the 3.1.0 Collector and configure it after the NAC Server upgrade.

Cisco NAC Profiler Collector Support and Cisco NAC Server Deployment Modes

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

1. Integrated with Cisco NAC Appliance. In this mode, the Profiler Collectors run as an additional software service on the Cisco NAC Appliance NAC Servers that are part of an operational Cisco NAC Appliance solution where the Cisco NAC Manager and NAC Servers are providing posture and remediation.
2. Not integrated with Cisco NAC Appliance. In this mode, the Profiler Collectors also run on the NAC Servers, but the Cisco NAC Manager is not present and the Cisco NAC Appliance system is not used for posture or remediation. In this mode, the Cisco NAC Profiler system provides Endpoint Discovery, Profiling and Identity Monitoring. The Cisco NAC Profiler endpoint directory is enabled for LDAP access so that other systems (Cisco Secure ACS for example) can utilize the Cisco NAC Profiler as an external database for MAC Authentication/MAC Authentication Bypass (MAB).

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

Cisco NAC Profiler Integration with Cisco NAC Appliance Deployments

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

	Clean Access Server Operating Mode			
NAC Profiler Collector Module / Function	**Real-IP Gateway**	**Virtual Gateway**	**Real-IP Gateway OOB**	**Virtual Gateway OOB**
NetMap SNMP polling of switches and routers	Yes	Yes[1]	Yes	Yes [1]
NetTrap Receive SNMP traps from switches	Yes	Yes [1]	Yes	Yes [1]

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

NAC Profiler Collector Module / Function	Clean Access Server Operating Mode			
	Real-IP Gateway	Virtual Gateway	Real-IP Gateway OOB	Virtual Gateway OOB
NetWatch [2]				
• Observe traffic on eth2 (if not used for HA heartbeat)	Yes [3]	Yes [3]	Yes [3]	Yes [3]
• Observe traffic on eth3	Yes	Yes	Yes	Yes
NetInquiry Active Profiling of endpoints	Yes	Yes[1]	Yes	Yes [4]
NetRelay Reception of NetFlow Export Data Records	Yes	Yes [1]	Yes	Yes [1]

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

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

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

Cisco NAC Profiler Not Integrated with Cisco NAC Appliance

In this deployment mode, although the Cisco NAC Appliance-specific NAC Server services are not utilized, the Profiler Collector utilizes the operating system and underlying configuration of the NAC Server in order to perform the endpoint data collection process.

You will need to perform minimum configuration of the NAC Server, as described in the "Perform the Initial CAS Configuration" section of the *Cisco NAC Appliance Hardware Installation Guide, Release 4.7*. See also "Startup of NAC Profiler Collectors" in the *Cisco NAC Profiler Installation and Configuration Guide, Release 3.1*

Note Cisco NAC Profiler is not supported in FIPS-compliant deployments in Cisco NAC Appliance Release 4.7(0).

Determining the Software Version

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

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

Cisco NAC Profiler Server

Via the UI

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

Via SSH

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

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

Profiler Status
   Version: Profiler-3.1.0-24

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

Cisco NAC Profiler Collector (on Cisco NAC Server)

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

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

Profiler Status
   Version: Collector-3.1.0-24

  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 3.1.0

Cisco NAC Profiler release 3.1.0 is a new feature release that contains significant enhancements to functionality from earlier versions as many new features and functionalities. Release 3.1.0 is available as an **ISO only** for the Profiler Server and Profiler Lite due to a change in the operating system. There is no upgrade file for Release 3.1.0.

The upgrade procedure for Profiler Server and Profiler Lite systems running version 2.1.8 or earlier to release 3.1.0 involves running a utility to migrate the existing database, including all Cisco NAC Profiler configuration and data, from the system running the earlier version to the system upgraded to version 3.1.0. Refer to Upgrade Instructions for Release 3.1.0-24, page 22 for detailed instructions on upgrading the Profiler Server and Profiler Server Lite running version 2.1.8.

The installation/upgrade of the Profiler Collector service on the NAC Server to version 3.1.0 is performed using the RPM update process as it was in earlier versions. The Collector service uses the operating system installed on the NAC Server and the configuration created during setup of those services. Installation/Upgrade of the Collector service is provided in Installing New/Upgrading Cisco NAC Profiler Collector Service on Cisco NAC Server, page 33.

New features and enhancements in version 3.1.0 of the Cisco NAC Profiler are detailed in the following sections:

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

Cisco NAC Profiler Server Operating System Change

The underlying operating system of the Cisco NAC Profiler Server/Cisco NAC Profiler Lite Server system has been changed from Fedora Core® to FreeBSD® in order to achieve performance enhancements and release stability for future versions.

User Interface Redesign

The Cisco NAC Profiler user interface has been completely redesigned to improve both navigation and presentation of system data and configuration. The 3.1.0 UI includes a new system dashboard providing at-a-glance system status indications and one-click navigation to the most frequently used areas of the interface.

As an option, Cisco NAC Profiler UI user authentication can now be performed via RADIUS to an external authentication service such as Cisco Secure ACS.

The admin UI user and other user accounts of type Operator are automatically logged out of the interface after 30 minutes of inactivity.

Endpoint Profile Creation and Management

Endpoint Profile creation/management in the UI has been significantly enhanced. The addition of a Certainty Calculator to the Edit Profile view eases determination of certainty value with any and all combinations of rule matches in multi-rule profiles.

The ability to group Endpoint Profiles containing endpoints with similar attributes (e.g., all printers or IP phones) was also added in this version. Endpoint Profiles can now be viewed by status (e.g., enabled, disabled, automatic) or by Profile Group.

Advanced XML Rule Editor

An Advanced XML Rule Editor was added in this version which provides the Cisco NAC Profiler Administrator assistance with the creation, editing and management of Advanced XML Rules within Endpoint Profiles. This eliminates the need to create the XML via a free-form text editor to assist with creation of Advanced rules with the correct syntax and format.

Cisco NAC Profiler Events

The Cisco NAC Profiler Events implementation, other than Cisco NAC Events, underwent a significant redesign in this version. This included a new Event Delivery method called Active Response, which can take the following actions on the switch port that connects endpoints which trigger events: Disable Port (admin down), Bounce Port, or force the 802.1X reauthentication of an endpoint on Cisco switches running compatible versions of IOS.

Note To support SNMP-triggered reauthentication by Cisco NAC Profiler, verify that your switch IOS release supports the AUTH-FRAMEWORK-MIB.

MAC Change Events have been removed from this version. Profile Change event functionality has been expanded to two sub-types: Profile Change Entering and Profile Change Exiting. Profile Change events are now configured globally and do not require configuration on the switch and port level. Two new events types were added in this version: Alarm Profile and Profile Consistency.

See *Chapter 12 - Integration with Cisco NAC Appliance* of the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1 for details on the Cisco NAC Profiler Events functionality.

Endpoint Data Collection and Profiling from Active Directory

Cisco NAC Profiler is now able to communicate with Microsoft Active Directory Servers for the purpose of collecting identity attributes for endpoints that are members of the Domain. Information collected for endpoints using this method can subsequently be used within Endpoint Profiles to profile endpoints based on their AD information. AD Membership, AD Computer Name, AD Information (OS, OS Version, OS Service Pack) profile rule types were added in this version.

CDP Data Collection and Profiling

Information collected by switches via the Cisco Discovery Protocol about endpoints connected to ports is now collected and made available for Endpoint Profiling. In previous versions, CDP information was used only for identification of links that interconnected switches with other switches or routers (Trunk Ports). Endpoints such as IP Phones, Virtual Gateways, etc. also use CDP to signal their presence to the switch connecting them to the network. Cisco NAC Profiler collects this information, which can be used to profile endpoints, via the CDP Platform Type rule added in this version.

RADIUS Accounting Data Collection and Profiling

RADIUS clients (switches) can be configured to forward RADIUS accounting data to Cisco NAC Profiler for the collection of endpoint data. Attributes such as RADIUS username can be used to profile endpoints using the RADIUS Username rule type added in this version.

Basic Endpoint Search

Basic Endpoint Search can now be initiated from any page of the UI at any time with search results presented in a secondary window to maintain the primary UI page. This prevents having to navigate away from the current page when searching/viewing results of basic endpoint searches. The Basic Endpoint Search queries the database for endpoint matches based on a single search criteria from the following list of endpoint identity attributes:

- MAC Vendor

- MAC Address (complete endpoint MAC address)
- IP/CIDR Block
- Profile Name
- Authenticated User
- Profile Data
- DNS Name
- DHCP Host Name

Redesigned Timeouts for Database Management

The Endpoint timeout scheme has been redesigned to provide more flexibility in the treatment of endpoints that are discovered and subsequently leave the network. See *Chapter 6- Cisco NAC Profiler Server Configuration* of the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1 for complete details on the database maintenance/timeout implementation in this and future versions.

MyNetworks Configuration

Networks in the MyNetwork configuration can now be specified to have one or more excluded network/subnets, which avoids collection of IP-learned attributes of endpoints on specified nets/subnets. This feature can be used to eliminate collection of endpoint data via IP-based learning for endpoints in sections of the network where it is not desirable to perform Profiling and Identity Monitoring.

Net Relay Module Configuration for NetFlow

NetRelay is now aware of the MyNetwork configuration: NetFlow processing is now enabled per NetRelay module by specifying a Network (Organization) Name in the Profiler Collector configuration. Network (Organization) Names are configured within MyNetwork and when configuring NetRelay modules on the system, the Organization (Network) Name bounds collection of endpoint traffic data from NetFlow to only source IPs within the range specified by the Organization (Network) Name. Specifying Network Blocks in the NetRelay module configuration is no longer required.

DNS Name Collection

DNS Name collection has been enhanced to utilize Zone Transfer (AXFR), resulting in significant performance enhancement in environments using DNS name collection/DNS rules for endpoint profiling.

Trap Handling by the Cisco NAC Profiler System

Community String validation for NetTrap has been added. If a community string is configured in the NetTrap module, NetTrap only processes traps received by the Profiler Collector that have a matching community string.

Cisco MAC Notification Trap trust was added in this version and enabled by default. When the Cisco NAC Profiler system (NetTrap module on a Profiler Collector) receives a Cisco MAC Notification trap indicating that an endpoint has connected to a port, the information about the endpoint within the trap is used by the Profiler system avoiding an SNMP query to the switch to verify the information.

To reduce the time required for the Profiler system to discover endpoints connected to switches that do not support Cisco MAC notification traps, an option has been added to the Network Device and Network Device Group configuration that disables the default behavior of the Cisco NAC Profiler to wait after receipt of a Link Up trap for a MAC notification trap which can reduce SNMP polling by Cisco NAC Profiler as described above. For switches that do not support MAC Notification traps, turning this option on allows the Profiler to complete the SNMP poll of the device immediately upon receipt of Link Up, reducing the time required for endpoint discovery on switches that do not support Cisco MAC notification traps.

Improved Management of Cisco NAC Profiler License Files through the UI

The display and management of Cisco NAC Profiler license files has been completely re-designed in this version. The UI now displays the license files uploaded to the system along with their type (such as, Server or Collector components) and a clear indication of the validity of the license file providing at-a-glance determination of the license status of the Cisco NAC Profiler System from a single page in the UI.

Scripted Support for SSL Certificate Management

Support for SSL certificates has been enhanced and automated through the Profiler Server Only system type startup scripts, and the 'service profiler' command set. A menu-driven script is utilized for creation of self-signed certificates and the ability to generate/download a CSR for submission to a CA.

Scripted Support for NTP Configuration

The Profiler Server startup scripts include automated setup of NTP when configuring the system initially, and can be called via the 'service profiler' command to manage NTP configuration. Use of NTP is recommended for all Profiler Server systems and mandatory for HA systems beginning with this version.

Advanced Search and Reporting Tool

An Advanced Search and reporting tool has been added to the system that significantly enhances the utility of the endpoint search function. The advanced search allows searching using multiple attributes (logical 'and' only), and supports 'not' and 'or' logical operations on any single attribute. Searches can be revised through multiple iterations to refine results, and search results may be exported from the UI directly in CSV and XML formats.

Exporting Cisco NAC Profiler Data

Exporting of Cisco NAC Profiler data from the Profiler Server has been greatly enhanced. Reporting via download in CSV and XML formats from the UI directly to the management PC has been added in most of the commonly-used views in the Endpoint Console as well as search.

Reporting of Network Devices in No Contact and or Lost Contact Status

The Cisco NAC Profiler UI tracks the status of Network Devices (switches and routers) that are being polled by NetMap. Devices that are unable to be contacted (No Contact) and or devices that have not been successfully polled for more than two regular polls by NetMap are displayed on the Device Connectivity pie chart displayed by default on the Configuration Tab.

Select View Functionality for Tables

Select View functionality improves UI performance by limiting tables that are likely to grow very large to display only the first 100 rows by default. The user can change these views to display these tables at 100, 250, 500, 1000 rows per page or show all via the Select View control.

Supported Web Browsers for Version 3.1.0

The Cisco NAC Profiler Version 3.1.0 User Interface has been tested thoroughly with Windows® Internet Explorer® Versions 7 and 8, and Firefox® 3.0.x and later.

Note Efforts have been made to extend support back to Windows® Internet Explorer® Version 6.0.2900.2180.xpsp_sp2_qfe.080814-1242. Cisco Systems recommends the use of Windows® Internet Explorer® Version 7, and Firefox® 3.0.x for optimal UI performance.

Caveats

This section describes the following caveats.

- Open Caveats - Release 3.1.0-24, page 12
- Resolved Caveats - Release 3.1.0-24, page 18

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 3.1.0-24

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 4)

DDTS Number	Software Release- Cisco NAC Profiler Version 3.1.0-24	
	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.

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
		
		Note This does not affect the function of the Profiler Server.

CSCsu46348	No	Cisco 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

Table 3 List of Open Caveats (Sheet 2 of 4)

DDTS Number	Software Release- Cisco NAC Profiler Version 3.1.0-24	
	Corrected	**Caveat**
CSCsw97514	No	Unable to delete a Collector from the Cisco NAC Profiler. An error pops up that Collector does not exist in the database. **Conditions** If user enters a Collector name when initially configuring the Collector service with greater than 24 characters, the name is truncated when added to the database resulting in a mis-match between what is displayed in the UI and what is stored in the DB preventing the deletion of the Collector. **Workaround** Manually delete the Collector from the Profiler database. 1. SSH to the Profiler Server as user 'beacon'. 2. Enter the following command at the prompt: echo "delete from beacon_component where name LIKE '<collector name as it appears in the GUI>';" | psql
CSCsy37604	No	Cisco NAC Profiler System does not indicate the version of the Collector service running on each Collector. **Conditions** No display in Cisco NAC Profiler UI of Collector version. When upgrading the system, the version of each Collector must be verified from the Collector command line. **Workaround** Verify version of Profiler Collector using the command line.
CSCtc34810	Yes	Endpoint location data is not displayed when trunk port info is received. **Conditions** If Profiler receives data that indicates the endpoint (a single mac address) is seen on two ports, such as a physical port and a trunk port, no information is displayed for the endpoint. **Workaround** None
CSCtd69946	Yes	In the CAM Device Filter list (integrated to Cisco NAC Profiler), upon clicking on the Profiler link in the Description field, the user cannot login to the profiler to view the summary information for the endpoint. **Conditions** No display of the endpoint summary in CAM Device Filter List if browsing through Internet Explorer. **Workaround** Right click on the profiler link and chose **Open link in new window** or **Open link in new tab** to view the Profiler summary information.You can also use Mozilla Firefox browser for this purpose.

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

DDTS Number	Software Release- Cisco NAC Profiler Version 3.1.0-24	
	Corrected	Caveat

CSCte41353	Yes	SNMP Session Reauthentication is not working.
		
		Conditions When the re-authentication event is triggered, the NAC Profiler has insufficient information about the authentication session on the switch to carry out the operation via an SNMP set. This issue is specific to Cisco NAC Profiler Release 3.1.
		
		Workaround Download **Patch-CSCte41353-K9.zip** from http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438162 and apply this patch on NAC Profiler/Collector 3.1 version in the following manner:
		
		There are two components to this patch:
		1. A script which needs to be run on the NAC Profiler appliance.
		2. A NetWatch binary file which needs to be put on the NAC Profiler Collector appliance (NAC Server)
		Below are the steps for both:
		Steps to run script on Cisco NAC Profiler Appliance:
		1. SCP **ReAuth.tgz** to NAC Profiler Server, /home/beacon
		2. As root system user, run the following commands:
		`tar xvfz ReAuth.tgz`
		`cd ReAuth`
		`/bin/sh reauth.sh`
		3. Check Server binary MD5 Sum:
		`md5 Server`
		`MD5 (Server) = bb125ccb349c9b825146ed97bb3419b0`
		Steps to run on Cisco NAC Profiler Collector Appliance (NAC Server):
		1. SCP **NetMap.reauth** to Collector/CAS appliance.
		2. As root system user, run the following commands:
		`service collector stop`
		`cd /usr/beacon/bin`
		`mv NetMap NetMap.old`
		`mv NetMap.reauth to /usr/beacon/bin/NetMap`
		3. Verify checksum:
		`md5sum NetMap`
		`20dfa277448368a747f895164fc37e28 NetWatch`

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

	Software Release- Cisco NAC Profiler Version 3.1.0-24	
DDTS Number	**Corrected**	**Caveat**

CSCte60976	Yes	Trap Handling for v2c traps are INOP for version 4.7.1 of the CAS/Collector Only. Older versions of SNMP Research in the CentOS build used for Cisco NAC Appliance Release 4.7.1 result in NetTrap being unable to determine the IP address of the trapping agent.
		
		Conditions This issue is specific to Cisco NAC Profiler Release 3.1 when integrated with Cisco NAC Appliance Release 4.7.1.
		
		Workaround Download **Patch-CSCte60976-K9.gz** from http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438162 and apply this patch on NAC Profiler/Collector 3.1 version in the following manner:
		
		As the root system user:
		1. SCP the patched NetTrap binary (in .gz) format to the /usr/beacon directory of the NAC Server/Collector
		2. Stop the Collector service using 'service collector stop'
		3. Unzip the patched NetTrap binary in the /usr/beacon directory:
		`gunzip NetTrap.gz`
		4. Verify the checksum of the modified NetTrap:
		`md5sum NetTrap; checksum = 817b5a8a157b937dd996e8751f1f3909`
		5. Rename current NetTrap binary to NetTrap.old:
		`mv bin/NetTrap NetTrap.old`
		6. Move patched NetTrap to bin:
		`mv NetTrap bin/NetTrap`
		7. Change ownership to root:beacon :
		`chown root:beacon NetTrap`
		8. Change execution privileges:
		`chmod 4750 NetTrap`
		9. Restart Collector:
		`service collector start`

CSCte93435	Yes	Profiler MAC Address OU DB is outdated for HP MAC address. **Conditions** New HP Printer MAC addresses are not being recognized by Profiler because the OU database does not have the entries. **Workaround** None

Open Caveats - Documentation

Table 4 List of Open Caveats - Documentation

	Software Release- Cisco NAC Profiler Version 3.1.0-24	
DDTS Number	**Corrected**	**Caveat**
CSCtd37697	No	Collector 3.1 on NAC 4.6.1 gets downgraded when NAC is upgraded to 4.7.1. When a user upgrades the Cisco NAC Profiler including the Profiler Collector to 3.1 in NAC 4.6.1 followed by upgrading the NAC 4.6.1 to 4.7.1, it overwrites the Collector 3.1 with Collector 2.1.8.39. **Workaround** After upgrading NAC 4.6.1 to 4.7.1, manually upgrade the Profiler Collector 2.1.8.39 to 3.1, because Profiler Collector 2.1.8.39 comes bundled in NAC 4.7.1.
CSCsy03646	No	Cisco 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 Cisco NAC Profiler or Cisco NAC Profiler Failover (HA) licenses, submit the eth0 MAC address of the Primary Profiler Server. •For Cisco NAC Profiler Failover (HA) license only, submit the eth0 MAC address of the secondary Profiler Server. http://www.cisco.com/en/US/docs/security/nac/appliance/support_guide/license.html#wp39086 •A Profiler Server license—installed on the Profiler Server •A Profiler Collector license for each CAS Collector— installed on the Profiler Server. ... -Failover Profiler Server (based on NAC-3350) - for HA pair **Conditions** Profiler HA / Collector HA setup **Workaround** One Profiler HA LIC file with MAC address primary Profiler eth0 and secondary Profiler eth0

Resolved Caveats - Release 3.1.0-24

Table 5 List of Resolved Caveats (Sheet 1 of 3)

	Software Release- Cisco NAC Profiler Version 3.1.0-24	
DDTS Number	**Corrected**	**Caveat**
CSCtb17189	Yes	Profiler incorrectly sets switch ports connecting endpoints other than IP Phones using CDP as trunk ports in the Cisco NAC Profiler UI. Cannot view endpoints on trunk ports in UI. **Conditions** In 2.1.8 version, automatic trunk detection was excluded only on ports that registered CDP Platform Type containing the string 'phone.' Endpoints using CDP Platform Type not containing phone would be marked as trunk ports in the UI. **Workaround** None. **Note** 3.1.0 version requires administrator configuration of CDP Trunk Exclusion parameter of Profiler Server module to exclude CDP Platform Types in addition to the default of 'phone.'.
CSCsl20917	Yes	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	Yes	Profiler Admin session should Logout after timed interval Cisco NAC Profiler GUI Admin logged in never gets logged out. **Workaround** None
CSCsm72012	Yes	Need SSL import/export certificate GUI tab for the Profiler Profiler needs to have an import/export utility for SSL certificates on the Profiler GUI. **Workaround** None.

Table 5 List of Resolved Caveats (Sheet 2 of 3)

	Software Release- Cisco NAC Profiler Version 3.1.0-24	
DDTS Number	**Corrected**	**Caveat**
CSCsq34147	Yes	Profiler: Standby Profiler shows database errors on Endpoint Console Standby Cisco NAC Profiler displays Unknown DB Error on the Endpoint Console Page. **Conditions** Cisco NAC Profiler running 2.1.8-37 in a failover pair. This will only show up on the Standby Profiler. **Workaround** 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	Yes	Cisco 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** Cisco NAC Profilers running in a failover pair. This is only seen on the secondary Profiler. This was observed in 2.1.8-37. **Workaround** None, this is a 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 ->XXXXXXXXXXX ERROR: (FlexLM): No match found in -> [<Count>2</Count><PrimaryMAC>YYYYYYYYYYY</PrimaryMAC>]`
CSCsu29905	Yes	Cisco NAC Profiler SNMP trap receive does not check community string Cisco NAC Profiler NetMap Collector solution is unable to verify network device (switch) snmp trap community string. Operationally the solution is processing endpoints and correctly profiling. **Conditions** Any SNMP (v1, v2c) trap sent community string **Workaround** None

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

	Software Release- Cisco NAC Profiler Version 3.1.0-24	
DDTS Number	**Corrected**	**Caveat**
CSCsu46247	Yes	Cisco NAC Profiler GUI allows duplication of Collector entry A Collector with the same name and IP can be created as a duplicate in the Cisco NAC Profiler GUI. **Conditions** When a Collector of the same info already exists. **Workaround** None.
CSCsu46273	Yes	Cisco NAC Profiler GUI needs the ability to set time and NTP information Currently there is no way to set the time 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	Yes	Cisco NAC Profiler GUI does not display IP or name of active Profiler When you click on the Config - Cisco NAC Profiler modules - List Config - Server server it displays Server Name: Server. The CLI name shows machines profiler1 and 2 but this is not shown nor the actual IP config on the boxes via the GUI. **Workaround** None
CSCsv66296	Yes	Changes of Collector NetWatch config corrupt network block formatting The formatting of the network block is corrupted and saving the config gives an error (example 172.16.17.0/24172.16.18.0/24 is not a IP v4 Address) **Conditions** Removing/adding/editing the NetWatch interface under the Collector configuration and then saving the Collector. **Workaround** Fix the blocks before saving the configuration or return to the configuration and correct it.
CSCsu46247	Yes	A collector with the same name and IP can be created as a duplicate in the Cisco NAC profiler UI without warning the user. **Conditions** Adding Collectors to the Cisco NAC Profiler configuration, no validation that the Collector Name already exists. **Workaround** None.

New Installation of Cisco NAC Profiler Release 3.1.0-24

Cisco NAC Profiler Server and Cisco NAC Profiler Lite Server

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

For upgrade of an operational Cisco NAC Profiler system running version 2.1.8, refer to the instructions in Upgrade Instructions for Release 3.1.0-24, page 22 in order to retain all system configuration and data.

Note The Profiler Lite appliance platform is supported starting from release 2.1.8-37 and requires a separate ISO file. Only the **nac-profilerlite-3.1.0-24-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 version 3.1.0 ISO image from http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=279515766

- For standard Profiler Server, download the latest **nac-profiler-3.1.0-24-K9.iso**
- For Profiler Lite, download the latest **nac-profilerlite-3.1.0-24-K9.iso**

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

Step 4 Insert the CD into the CD-ROM drive of the appliance that Profiler Server/Profiler Lite Server is to be installed on, and reboot the appliance to start the ISO process.

Step 5 Follow the on-screen instructions to complete a “standard” (e.g., no custom keyword) ISO of the Profiler Server or Profiler Lite Server appliance, or appliances in the case of high availability (HA) Profiler Servers. At the completion of the ISO installation, the appliance ejects the ISO CD and boot to the root prompt. It is now in the same state a new Profiler Server and Profiler Lite Server would be shipped from the factory with version 3.1.0-24 installed.

Step 6 Upgrade the Profiler Collector component on each Clean Access Server to the appropriate version as described in Installing New/Upgrading Cisco NAC Profiler Collector Service on Cisco NAC Server, page 33.

Step 7 Refer to *Chapter 4 - Installation and Initial Configuration* of the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1 for complete installation and configuration instructions for new Cisco NAC Profiler systems.

Upgrade Instructions for Release 3.1.0-24

This section provides instructions for the upgrade of operational Cisco NAC Profiler systems running all earlier versions, to version 3.1.0-24.

Note To support Cisco NAC Profiler release 3.1.0-24, the NAC Server(s) must already be configured and running the latest supported Cisco NAC Appliance release as described in Software Compatibility, page 3. The Profiler Collector component must also be upgraded on the NAC Server to the corresponding version as described in Software Compatibility, page 3 and Installing New/Upgrading Cisco NAC Profiler Collector Service on Cisco NAC Server, page 33.

Note The Profiler Lite appliance platform is supported starting from release 2.1.8-37 and requires a separate ISO file. Only the **nac-profilerlite-3.1.0-24-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 Profiler Server include both standalone and HA-pair configurations.

Overview

The Cisco NAC Profiler Release 3.1.0 installation files are available from Cisco Secure Software at http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438162.

The following files are available:

- **DB-utility_218to31x.tgz** - This utility is used to migrate the 2.1.8 database to the 3.1.0 system.
- **nac-profiler-3.1.0-24-K9.iso** - This is the ISO installation file for the Cisco NAC Profiler appliance
- **nac-profilerlite-3.1.0-24-K9.iso** - This is the ISO installation file for the Cisco NAC Profiler Lite appliance
- **nac-collector-3.1.0-24-K9.rpm** - This is the Collector RPM that gets loaded onto the NAC Server (CAS)

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

Note

- Due to the change in Operating System, the upgrade file for the Profiler Server version 3.1.0 is distributed as an ISO image only.
- For the upgrade of 2.1.8 Profiler Server systems to version 3.1.0, an additional package is required to migrate the 2.1.8 database so that it is forward-compatible with version 3.1.0.

- The version 3.1.0 Profiler Collector RPM is a complete package that can be used to upgrade an existing Collector service on a NAC Server to the latest version of the Profiler Collector. It can also be used for a “fresh” install on a NAC Server that does not have the Collector service running on it.

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

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

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

As outlined in Cisco NAC Profiler Server Operating System Change, page 8, the Operating System of the Profiler Server system has changed in version 3.1.0, requiring systems running 2.1.8 to undergo complete reinstallation of the Profiler Server software to successfully upgrade to release 3.1.0.

The upgrade process utilizes a standalone database migration script run on the system prior to upgrade that brings the 2.1.8 database forward to release 3.1.0 compatibility. After the ISO upgrade to release 3.1.0, the Profiler Configuration and endpoint data from the 2.1.8 system are restored to the 3.1.0 system.

Before beginning the upgrade procedure, complete the following preparations:

1. Download the 2.1.8-to-3.1.0 Database Migration Utility (**DB-utility_218to31x.tgz**) from http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438162 to the PC used to manage the Cisco NAC Profiler system

Note Prior to download, take note of the MD5 value in the Details table of the Software Download screens. Once the files have been downloaded, MD5 checksums should be verified to ensure file integrity.

2. Download the Cisco NAC Profiler Server ISO (**nac-profiler-3.1.0-24-K9.iso**) or Cisco NAC Profiler Lite Server ISO (**nac-profilerlite-3.1.0-24-K9.iso**) from http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438162.

Note Profiler Server Lite requires a special ISO unique to the Lite configuration. If you are upgrading a Profiler Lite system, ensure that the correct ISO is downloaded. Loading the Profiler Server software on the NAC Server 3310 appliance results in system instability.

3. The ISO installation of the Profiler Server requires physical access to the appliance and is completed using keyboard and monitor or console (serial) connection to the Profiler Server appliance for the completion of the basic IP configuration/startup scripts post-ISO installation to version 3.1.0. Ensure that physical access to the appliance is available for placement of the ISO CD into the CD drive, and that a console session can be made via keyboard and monitor or serial connection.

4. Locate the license files for the Cisco NAC Profiler system as they need to be uploaded via the UI after the ISO installation of the system to version 3.1.0. If the license files cannot be located, they can be copied from the Cisco NAC Profiler system before beginning the upgrade procedure. The license files (.lic files) can be found on the Profiler Server in the /usr/beacon/working/flexLM directory and can be moved off-appliance using SCP.
5. Review and record the base configuration of the standalone Profiler Server appliance. Parameters such as IP address and mask, gateway, name server, NTP server(s), and self-signed certificate parameters for the standalone Profiler Server are completed via the startup scripts that are run after the Profiler Server appliances are ISO installed to version 3.1.0, prior to restoration of the database.
6. Complete a database backup of the Cisco NAC Profiler system to be upgraded and move it off the system using the Cisco NAC Profiler UI. This database snapshot is required should the 2.1.8 system need to be restored in the event of the upgrade failing and back-out is required. Roll-back to 2.1.8 is accomplished via ISO installation (from CD) to the 2.1.8 version of Cisco NAC Profiler and restoration of this database backup. Consideration should be given to securing a copy of the 2.1.8-37 Cisco NAC Profiler and Cisco NAC Profiler Lite ISO.

Once these preparations are completed, proceed with the upgrade of the standalone Profiler Server as outlined below.

Step 1 SCP the 2.1.8-to-3.1.0 database migration utility package (**DB-utility_218to31x.tgz**) downloaded previously to the /home/beacon directory of the standalone Profiler Server to be upgraded from version 2.1.8 to 3.1**.**

Step 2 Connect to the Profiler Server being upgraded via SSH. Login as the beacon system user.

Step 3 Elevate to root user using the su - command and enter the password for the root user:

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

Step 4 Change directory to **/home/beacon**

```
cd /home/beacon
```

Step 5 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 DB-utility_218to31x.tgz
```

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 6 Untar the database migration utility package:

```
tar xvfz DB-utility_218to31x.tgz
```

This command uncompresses the files to the /home/beacon directory required for migration of the Profiler database containing the configuration and data of the 2.1.8 system so that it can be restored on the 3.1.0 system, including a script that performs the migration named upgrade.pl

Step 7 Execute the database migration script by entering the following command:

```
./upgrade.pl
```

Step 8 The following message is displayed requiring user input to continue with the migration of the database:

```
Attention:
```

```
You are about to perform a major upgrade to this system. If this system has been
customized outside of the normal product configuration please contact support BEFORE
proceeding.

Be sure to copy the resulting backup file from this upgrade script to a secure location as
a fail safe.

Please press Enter to continue (or ctrl+c to abort)
```

Press Enter to begin the database migration on the 2.1.8 Cisco NAC Profiler System.

Step 9 Successful execution of the database migration script is indicated by the following messages followed by return of the command prompt as shown below:

```
Preparing for upgrade...

Migrating GUI passwords to database
Backing up current DB.

The files required for the upgrade have been bundled and placed in
/backup/upgrade/dbbackup-218.gz.

Please copy /backup/upgrade/dbbackup-218.gz to a secure location (on a different system)
and proceed with the upgrade per the instructions.

** When the above file has been placed into a secure location insert the Profiler 3.1
installation CD and type "reboot" and press Enter to proceed with the next phase of
upgrade process.

{root@nac-profiler beacon}#
```

Step 10 Using SCP, copy the **dbbackup-218.gz** file from the Profiler Server to another system so that it can be restored to the standalone Profiler Server after the upgrade.

Warning **The file system on the Profiler Server is reformatted and all files on the appliance are replaced during the subsequent ISO installation to version 3.1.0. Ensure the dbbackup-218.gz file created in the proceeding steps is moved off the appliance and placed in a secure location prior to proceeding with the ISO installation. If this file is not available for restore to the system after the upgrade, all Cisco NAC Profiler configuration settings and endpoint data are irrecoverable.**

Step 11 If the console session (keyboard and monitor or serial connection to the appliance) required to complete/monitor the ISO process and run the startup scripts after upgrade has not been established, establish it now.

Note Upon proceeding with the next step, the Profiler Server being upgraded is temporarily unable to communicate via the network. It is not reachable via SSH, nor can the Cisco NAC Profiler UI be accessed until the ISO installation is completed and the system provided with its basic configuration through completion of the startup scripts as described below.

Step 12 Ensure that the Cisco NAC Profiler and Cisco NAC Profiler Lite v3.1.0 ISO CD is in the CD drive, and enter the following command to initiate a reboot and ISO installation of the standalone Profiler Server being upgraded to the 3.1.0 version.

```
reboot
```

Step 13 Upon completion of the reboot to the ISO CD, the Profiler Server ISO process begins. The process is interrupted with a screen requiring user input to proceed with installation of the Profiler. Choose the **1. Standard --> Install Profiler** option, and make sure OK is highlighted (default), then press Enter to proceed with the ISO imaging of the appliance.

Step 14 The ISO process then presents one last warning that all files on the hard drive are overwritten. Ensure that the **dbbackup-218.gz** has been moved off the appliance and if it has, press Enter to proceed with the ISO imaging to version 3.1.0.

Tip If the ISO installation is cancelled by selecting No on the Confirmation page, the system returns to the prompt. Reboot the appliance to restart the ISO process when ready.

Step 15 At the completion of the ISO, the CD ejects and the appliance reboots the 3.1.0 image. Upon first boot, login as the root system user (no password) and the appliance displays the Initial Configuration screen to signify the initiation of the startup scripts.

Note The initial configuration screen indicates the flavor of Profiler Server that was installed: Cisco NAC Profiler or Cisco NAC Profiler Lite. Verify that the correct flavor was installed via ISO.

Step 16 Refer to *Chapter 4 - Installation and Initial Configuration* of the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1 to complete the startup scripts to provide the standalone Profiler Server appliance with its basic configuration.

Step 17 Open the Cisco NAC Profiler UI using a browser and log into the system as the admin user using the password selected in the last step. Select the "Upload License" link from the secondary menu of the Home Tab and upload the license files back to the system. Refer to *Chapter 5 - Configuring the Cisco NAC Profiler for the Target Environment* of the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1 for instructions on the management of license files through the UI in the current version. Verify that the Server module recognizes the licenses files and returns to a running state prior to proceeding.

Step 18 Upgrade the Profiler Collector(s) on the NAC Server(s) to version 3.1.0 as outlined in Installing New/Upgrading Cisco NAC Profiler Collector Service on Cisco NAC Server, page 33.

Note All Collectors configured on the NAC Server should be upgraded using this procedure before proceeding with restoring the database to the Profiler Server.

Step 19 SCP the **dbbackup-218.gz** file to the upgraded standalone Profiler Server, placing it in the /backup directory.

Step 20 SSH to the Profiler Server as the beacon system user and use the following commands to restore the migrated Profiler database to the upgraded system using the restore database procedure:

a. Change directory to /usr/beacon/scripts/maint:

```
cd /usr/beacon/scripts/maint
```

b. Restore the database snapshot taken from the 2.1.8 system prior to upgrade:

```
./restoreDB.pl /backup/dbbackup-218.gz
```

Step 21 Perform an Apply Changes -> Update Modules from the UI to restart the system with the restored database.

Step 22 Verify that the Cisco NAC Profiler System configuration and endpoint data was successfully restored to the 3.1 system by navigating through the UI.

Note The following features in version 3.1.0 have undergone significant changes or are no longer supported:

1. MAC Change Events are not supported. MAC Change Events that were configured on the 2.1.8 system are not carried forward through the upgrade to version 31.

2. Profile Change Events have been re-engineered and must be reconfigured after the upgrade to version 3.1. Any Profile Change Events that were configured on the 2.1.8 system are deleted.

3. If one or more NetRelay modules were configured for the processing of NetFlow on the 2.1.8 system, the Network Blocks section of the NetRelay module configuration is converted to an Organization (Network) name in the MyNetwork configuration via the upgrade. They are named <collector name>-nr-addrs, and the NetRelay module is reconfigured to use the Organization Name to configure the address space for NetFlow collection.

4. The time outs that control Database Maintenance functions of the Server module (e.g., endpoint timeout, port timeout, etc.) have been re-engineered in this version, and all configured values are reset to zero (no timeout). Review the information in *Chapter 6- Cisco NAC Profiler Server Configuration* of the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1 regarding the new timeouts, and reconfigure these time out values to be consistent with the new mode of operation.

Note If the Cisco NAC Profiler system being upgraded is not integrated with Cisco NAC Appliance, the upgrade of the standalone system is now complete. For systems integrated with Cisco NAC Appliance, the steps below must be completed in order to re-initialize the Cisco NAC Appliance integration layer of Cisco NAC Profiler.

Step 23 Using the Cisco NAC Profiler UI, verify Cisco NAC Appliance integration parameters of the Server module configuration are set correctly. Of particular interest is the parameter labeled 'Enable NAC Integration' that is new in the 3.1 release. This parameter must be on (checked) for the integration to function normally.

Step 24 SSH to the Profiler Server as the beacon system user.

Tip The next step requires the entry of the root system user password for the Cisco NAC Manager. Ensure that the root system password on the Cisco NAC Manager is known before proceeding.

Step 25 Execute the command **service profiler setupccakey** to re-establish the keyless SSH with the Cisco NAC Manager (or HA NAC Manager pair if applicable) necessary for the Cisco NAC Appliance synchronization operation.

Step 26 Perform an Apply Changes -> Update Modules to perform a complete synchronization of the Cisco NAC Manager Device Filter List.

Upgrading Cisco NAC Profiler Server HA Pairs from Version 2.1.8 to 3.1.0

As outlined in Cisco NAC Profiler Server Operating System Change, page 8, the Operating System of the Profiler Server system has changed in version 3.1.0, requiring systems running the 2.1.8 have a complete re-installation of the Profiler Server software to successfully upgrade to the 3.1.0 version.

The upgrade process utilizes a database migration script run on the system prior to upgrade that brings the 2.1.8 database forward to version 3.1.0 compatibility. After the upgrade ISO to version 3.1.0, the Profiler Configuration and endpoint data from the 2.1.8 system are restored to the 3.1.0 system.

Before beginning the upgrade procedure, complete the following preparations:

1. Download the 2.1.8-to-3.1.0 Database Migration Utility from http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438162 to the PC used to manage the Cisco NAC Profiler system

Note Prior to download, take note of the MD5 value in the Details table of the Software Download screens. Once the files have been downloaded, MD5 checksums should be verified to ensure file integrity.

2. Download the Cisco NAC Profiler Server (or Cisco NAC Profiler Lite Server ISO) from http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=268438162 and burn 2 ISO CDs.

Note Cisco NAC Profiler Server Lite requires a special ISO unique to the Lite configuration. If you are upgrading a Cisco NAC Profiler Lite system, ensure that the correct ISO is downloaded. Loading the Cisco NAC Profiler Server software on the NAC Server 3310 appliance results in system instability.

3. The ISO of the Cisco NAC Profiler Server pair requires physical access to the appliances and is completed using keyboard and monitor or console (serial) connection to the Cisco NAC Profiler Server Appliances for the completion of the basic IP configuration/startup scripts post-ISO to version 3.1.0. Ensure that physical access to the appliances is available for placement of the ISO CDs in the drives, and that a console session can be made via keyboard and monitor or serial connection to the appliances in the pair.
4. Locate the license files for the Cisco NAC Profiler System as they need to be uploaded via the UI after the ISO of the system to version 3.1.0. If the license files cannot be located, they can be copied from the Cisco NAC Profiler system before beginning the upgrade procedure; the license files (.lic files) can be found on the Primary node of the Profiler Server HA pair in the /usr/beacon/working/flexLM directory and can be moved off-appliance using SCP.
5. Review/note the base configuration of the appliances in the Profiler Server HA pair. Appliance-specific parameters such as IP address and mask, gateway, name server, NTP server(s), and self-signed certificate parameters for the Profiler Servers in the pair are completed via the startup scripts that are run after the Profiler Server appliances are ISO installed to version 3.1.0. The HA protocol is also re-established prior to restoration of the database completing the upgrade.
6. Complete a database backup of the Cisco NAC Profiler system to be upgraded and move it off the system using the Cisco NAC Profiler UI. This database snapshot is required should the 2.1.8 system need to be restored in the event of the upgrade failing and back-out be required. Roll-back of the to

2.1.8 is accomplished by an ISO (from CD) to the 2.1.8 version of Cisco NAC Profiler and restoration of this database backup. Consideration should be given to securing a copy of the 2.1.8-37 Cisco NAC Profiler and Cisco NAC Profiler Lite ISO.

Once these preparations are completed, proceed with the upgrade of the standalone Profiler Server as outlined below.

Step 1 SCP the 2.1.8-to-3.1.0 database migration utility package (DB-utility_218to31x.tgz) downloaded previously to the /home/beacon directory of the Primary node of the Profiler Server HA pair to be upgraded from version 2.1.8 to 3.1**.**

Step 2 Connect to the Primary node of the Profiler Server pair being upgraded via SSH using its eth0 IP address (not the VIP). Login as the beacon system user.

Step 3 Elevate to root user using the su - command and enter the password for the root user:

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

Step 4 Change directory to **/home/beacon**

```
cd /home/beacon
```

Step 5 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 DB-utility_218to31x.tgz
```

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 6 Untar the database migration utility package:

```
tar xvfz DB-utility_218to31x.tgz
```

This command uncompresses the files to the /home/beacon directory required for migration of the Profiler database containing the configuration and data on the 2.1.8 system so that it can be restored on the 3.1.0 system, including a script that performs the migration named upgrade.pl

Warning **When upgrading a Profiler Server HA pair, proceeding to the next step requires that the upgrade process be fully completed once begun. Migration of the database requires stopping HA services on the pair. Do NOT proceed until the upgrade procedure can be completed in its entirety.**

Step 7 Execute the database migration script by entering the following command:

```
./upgrade.pl
```

Step 8 The following message is displayed requiring user input to continue with the migration of the database:

```
Attention:

You are about to perform a major upgrade to this system. If this system has been
customized outside of the normal product configuration please contact support BEFORE
proceeding.

Be sure to copy the resulting backup file from this upgrade script to a secure location as
a fail safe.

Please press Enter to continue (or ctrl+c to abort)
```

Press Enter to begin the database migration on the 2.1.8 Cisco NAC Profiler System.

Step 9 Successful running of the database migration script is indicated by the following messages followed by return of the command prompt as shown below:

```
Preparing for upgrade...

Migrating GUI passwords to database
Backing up current DB.

The files required for the upgrade have been bundled and placed in
/backup/upgrade/dbbackup-218.gz.

Please copy /backup/upgrade/dbbackup-218.gz to a secure location (on a different system)
and proceed with the upgrade per the instructions.

** When the above file has been placed into a secure location insert the Profiler 3.1
installation CD and type "reboot" and press Enter to proceed with the next phase of
upgrade process.

{root@nac-profiler beacon}#
```

Step 10 Using SCP, copy the **dbbackup-218.gz** file from the Profiler Server to another system so that it can be restored to the standalone Profiler Server after the upgrade.

Warning **The file system on the Profiler Servers in the pair is reformatted and all files on the appliances are replaced during the following ISO to version 3.1.0. Ensure the dbbackup.gz file is moved off the Primary node and placed in a secure location prior to proceeding with the ISO installation of the appliances in the pair. If this file is not available for restore to the system after the upgrade, all Cisco NAC Profiler configuration settings and endpoint data are irrecoverable.**

Timesaver ISO installation of the Profiler Server appliances in the pair can be done in parallel if desired. Complete Step 11 to Step 13 to ISO image both appliances in the pair to version 3.1.0. When both appliances have completed the ISO process, proceed with Step 14 to provide the pair with its base configuration so that the database can be restored to the system.

Step 11 If the console session (keyboard and monitor or serial connection to the appliances) required to complete/monitor the ISO process and run the startup scripts after upgrade has not been established, establish it now.

Note Upon proceeding with the next step, the Profiler Server appliances being upgraded are temporarily unable to communicate via the network. They are not reachable via SSH, nor can the Cisco NAC Profiler UI be accessed until the ISO installation is completed and the HA pair provided with its basic configuration through completion of the startup scripts as described below.

Step 12 Ensure that the Cisco NAC Profiler and Cisco NAC Profiler Lite v3.1.0 ISO CD is in the CD drive, and enter the following command to initiate a reboot and ISO of the standalone Profiler Server being upgraded to the 3.1.0 version.

```
reboot
```

Step 13 Upon completion of the reboot to the ISO CD, the Profiler Server ISO process is begun. The process is interrupted with a screen requiring user input to proceed with installation of the Profiler. Choose the **1. Standard --> Install Profiler** option and ensure **OK** is highlighted (default), then press Enter to proceed with the ISO imaging of the appliance.

Step 14 The ISO process then presents one last warning that all files on the hard drive are overwritten. Ensure that the **dbbackup-218.gz** file has been moved off the appliance and if it has, press Enter to proceed with the ISO imaging to version 3.1.0.

Tip If the ISO installation is cancelled by selecting No on the Confirmation page, the system returns to the prompt. Reboot the appliance to restart the ISO process when ready.

Step 15 At the completion of the ISO installation, the CD ejects and the appliance reboots the 3.1.0 image. Upon first boot, login as the root system user (no password) and the appliance displays the Initial Configuration screen to signify the initiation of the startup scripts.

Note The initial configuration screen indicates the version of Profiler Server that was installed: Cisco NAC Profiler or Cisco NAC Profiler Lite. Verify that the correct version was installed via ISO.

Step 16 Refer to *Chapter 4 - Installation and Initial Configuration* of the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1 to complete the startup scripts to provide the Profiler Server HA pair beginning with the appliance designated to be the Primary node. Configuration of the HA pair continues with the startup of the Secondary node and completion of the startup of HA services on the pair.

Step 17 Open the Cisco NAC Profiler UI using a browser and log into the system as the admin user using the password selected in the last step. Select the "Upload License" link from the secondary menu of the Home Tab and upload the license files back to the system. Refer to *Chapter 5 - Configuring the Cisco NAC Profiler for the Target Environment* of the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1 for instructions on the management of license files through the UI in the current version. Verify that the Server module recognizes the licenses files and returns to a running state prior to proceeding.

Step 18 Upgrade the Profiler Collector(s) on the NAC Server to version 3.1.0 as outlined in Installing New/Upgrading Cisco NAC Profiler Collector Service on Cisco NAC Server, page 33. All Collectors configured on the NAC Server should be upgraded using this procedure before proceeding with restoring the database to the Profiler Server.

Step 19 SCP the migrated database backup from the 2.1.8 system (**dbbackup-218.gz**) to the Primary node of the upgraded Profiler Server HA pair via the VIP placing it in the /backup directory.

Step 20 SSH to the Primary node as the beacon system user and use the following commands to restore the database from the 2.1.8 system to the upgrade using the restore database procedure:

a. Elevate to root system user using the **su -** command

a. Change directory to /usr/beacon/scripts/maint:

```
cd /usr/beacon/scripts/maint
```

b. Restore the database snapshot taken from the 2.1.8 system prior to upgrade:

```
./restoreDB-HA.pl /backup/dbbackup-218.gz
```

Step 21 Perform an Apply Changes -> Update Modules from the UI to restart the Profiler Server HA pair with the restored database.

Step 22 Verify that the Cisco NAC Profiler System configuration and endpoint data was successfully restored to the 3.1 system by navigating through the UI.

Note The following features in version 3.1.0 have undergone significant changes or are no longer supported:

1. MAC Change Events are not supported. MAC Change Events that were configured on the 2.1.8 system are not carried forward through the upgrade to version 31.

2. Profile Change Events have been re-engineered and must be reconfigured after the upgrade to version 3.1. Any Profile Change Events that were configured on the 2.1.8 system are deleted.

3. If one or more NetRelay modules were configured for the processing of NetFlow on the 2.1.8 system, the Network Blocks section of the NetRelay module configuration is converted to an Organization (Network) name in the MyNetwork configuration via the upgrade. They are named <collector name>-nr-addrs, and the NetRelay module is reconfigured to use the Organization Name to configure the address space for NetFlow collection.

4. The time outs that control Database Maintenance functions of the Server module (e.g., endpoint timeout, port timeout, etc.) have been re-engineered in this version, and all configured values are reset to zero (no timeout). Review the information in *Chapter 6- Cisco NAC Profiler Server Configuration* of the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1 regarding the new timeouts, and reconfigure these time out values consistent with the new mode of operation.

Note If the Cisco NAC Profiler system being upgraded is not integrated with Cisco NAC Appliance, the upgrade of the standalone system is now complete. For systems integrated with Cisco NAC Appliance, the steps below must be completed in order to reinitialize the Cisco NAC Appliance integration layer of Cisco NAC Profiler.

Step 23 Using the Cisco NAC Profiler UI, verify Cisco NAC Appliance integration parameters of the Server module configuration are set correctly. Of particular interest is the parameter labeled 'Enable Cisco NAC Integration' that is new in the 3.1 release. This parameter must be on (checked) for the integration to function normally.

Step 24 SSH to the Primary node of the NAC Server HA pair as the beacon system user.

Tip The next step requires the entry of the root system user password for the Cisco NAC Manager. Ensure that the root system password on the Cisco NAC Manager is known before proceeding.

Step 25 Execute the command **service profiler setupccakey** to re-establish the keyless SSH with the Cisco NAC Manager (or HA NAC Manager pair if applicable) necessary for the Cisco NAC Appliance synchronization operation.

Tip The setupccakey process detects the presence of HA on the pair and performs the setup of keyless SSH on both nodes of the pair when initiated on the Primary node.

Step 26 Perform an Apply Changes -> Update Modules to perform a complete synchronization of the Cisco NAC Manager Device Filter List.

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

New installation or upgrade of the Profiler Collector service on a Cisco NAC Server to version 3.1.0 is accomplished via a single RPM file. The Profiler Collector RPM is a complete package that can be used to upgrade an existing Collector service on a NAC Server to version 3.1.0. It can also be used for a "fresh" install on a NAC Server that does not have the Collector service running on it. Use the following steps to upgrade or install the Collector service on a NAC Server.

Note When upgrading the Collector service only on a NAC Server via this process, the existing configuration of the Profiler Collector remains intact. For new installations, the Collector service must be provided an initial configuration via the NAC Server CLI, using the **service collector config** command. Refer to *Chapter 4 - Installation and Initial Configuration* of the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1 for complete instructions on initial startup of Profiler Collectors.

Note Cisco NAC Appliance 4.7 releases are shipped with Collector version 2.1.8-39 by default. When upgrading the NAC Server to a newer Cisco NAC Appliance release, the current version of the Collector is replaced with the default version of the Collector shipped with the Cisco NAC Appliance release. For example, if you are running NAC 4.7(1) and Profiler 3.1 and you upgrade to NAC 4.7(2), you need to manually re-install the 3.1.0 Collector and configure it after the NAC Server upgrade.

Step 1 Download the latest Profiler Collector RPM file (that is **nac-collector-3.1.0-24-K9.rpm**) from the Cisco NAC Profiler Version 3.1.0 location on Cisco Secure Software.

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 NAC Server(s) to be upgraded.

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

Step 3 Initiate an SSH session to the NAC Server being upgraded and login as the root user 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-3.1.0-24-K9.rpm
```

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

```
rpm -Uhv nac-collector-3.1.0-24-K9.rpm
```

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

Step 7 For newly installed Profiler Collectors, refer to *Chapter 4 - Installation and Initial Configuration* of the Cisco NAC Profiler Installation and Configuration Guide, Release 3.1 for complete instructions on initial startup of Profiler Collectors.

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

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

```
service collector start
```

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

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

Profiler Status
   Version: Collector-3.1.0-24

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

[root@bcas1 beacon]#
```

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

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

Documentation Updates

Table 6 Updates to Release Notes for Cisco NAC Profiler, Release 3.1.0

Date	Description
March 2, 2010	Cisco NAC Profiler Release 3.1.0-24.

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 3.1*
- *Release Notes for Cisco NAC Profiler, Release 3.1* (this document)
- *Release Notes for Cisco NAC Appliance*
- *Cisco NAC Appliance Hardware Installation Guide* (Release 4.7 or later)
- *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 35 section.