CA Network Flow Analysis

Release Notes

Release 9.3.0

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Welcome

Welcome to CA Network Flow Analysis 9.3.0. Review these notes before you install or upgrade the CA Network Flow Analysis software.

This document contains important information, including the following topics:

- Availability of product documentation
- System specifications
- Deployment options
- Software version compatibility
- New features and enhancements
- Version compatibility
- Known issues
- How to locate Third Party Acknowledgment and License Agreements

Starting with CA Network Flow Analysis 9.3.0, the *Readme* and *Localization Status Readme* information has been incorporated into the *Release Notes*.

This section contains the following topics:

Product Documentation

CA provides a full set of technical documentation in the CA Network Flow Analysis Bookshelf. You can open the guides in PDF and HTML format from the Bookshelf. Open the Bookshelf from the Help menu in the user interface for the NFA console or the Performance Center Console. You also can view and download the Bookshelf from the product page on CA Support.

The documentation may have been updated since its release. To get the latest CA Network Flow Analysis documentation updates and localized documentation, download the Bookshelf from CA Support.

Use the online Help system when you need more information about administration tasks and user tasks.

To view the documentation PDF files, make sure that Adobe Reader is installed.

Third Party Acknowledgment and License Agreements

Third-party software was used in the creation of CA Network Flow Analysis. All third-party software has been used in accordance with the terms and conditions for use, reproduction, and distribution as defined by the applicable license agreements.

Information about third-party license agreements is provided in the following document, which is installed automatically with the software:

<install_path>\ThirdPartyContent\ThirdPartyLicenseInfo.pdf

Chapter 2: System Requirements

This section contains the following topics:

Deployment Options

You can install all CA Network Flow Analysis components on a stand-alone system or can distribute the components among multiple servers:

- A *stand-alone* system consists of a single, dedicated server or virtual machine that is used to install both the NFA console and the Harvester software.
- A *two-tier distributed* deployment has the NFA console and one or more Harvesters installed on separate dedicated servers or virtual machines.
- A *three-tier distributed* deployment has the NFA console, one or more Harvesters, and one or more Data Storage Appliances (DSAs) installed on separate dedicated servers or virtual machines.

The current version of CA Network Flow Analysis supports the following operating systems:

- *Microsoft Windows Server 2008 R2, Standard Edition on a 64-bit processor* on any of the installation servers.
- *Red Hat Enterprise Linux 5.5 or 5.6 on a 64-bit processor* on a Harvester server in a distributed deployment
- English, Chinese (Simplified), French (France), or Japanese language

Software Versions that Are Supported for Upgrade

CA Network Flow Analysis 9.3.0 supports upgrades from the following versions to the current configuration:

- CA Network Flow Analysis 9.2.1
- CA Performance Center 2.4/2.3 or CA NetQoS Performance Center 6.1.205 SP2
- (Optional) CA Anomaly Detector 9.2.1

From	Upgrade To
NFA 9.2.1 operating with CA PC 2.3.x	NFA 9.3.0 operating with CA PC 2.4/2.3
NFA 9.2.1 operating with NPC 6.1.205 SP2	NFA 9.3.0 operating with NPC 6.1.205 SP2

When you upgrade the software, you continue to use the same architecture you used for release 9.2.1, as shown in the following list:

- Stand-alone to stand-alone
- Distributed 2-tier to distributed 2-tier
- Distributed 3-tier to distributed 3-tier

CA Network Flow Analysis 9.2.1 is the only software version that you can upgrade directly to release 9.3.0. If you have an earlier version, upgrade to version 9.2.1 before you proceed. For more information, see the *CA Network Flow Analysis 9.2.1 Upgrade Guide*.

Notes:

- Upgrade CA Network Flow Analysis before any upgrade you make to Performance Center.
- Do not install or upgrade any CA Network Flow Analysis component on a server that has Performance Center installed. You can co-locate the NFA console or stand-alone deployment with CA Anomaly Detector, but not with any other related software.
- If you plan to switch between CA NetQoS Performance Center (NPC) and CA Performance Center (CA PC), unregister before you upgrade CA Network Flow Analysis. Unregister before a switch from NPC to CA PC or a switch from CA PC to NPC.
- Windows NT LAN Manager (NTLM) is not supported by the Single Sign-On tool.

Windows System Requirements and Recommendations

If you purchase servers from CA, the servers already have the software installed. If you purchase software only, verify that your hardware meets the specifications that are noted here, in the *CA Network Flow Analysis Installation Guide,* and in the *CA Network Flow Analysis Upgrade Guide*. For the latest version of the documentation, visit CA Support Online.

Setting or Component	Description
Operating System	Microsoft Windows Server 2008 Standard Edition on a 64-bit processor
Language	English, Chinese (Simplified), French (France), or Japanese language The appropriate language packs are required for localized deployments.
Operating System Updates	Latest service pack and all important updates installed Install only important Windows updates and service packs. Do not install an unsupported web browser.
Disk Space	C: drive with 40 GB of available space for the operating system We recommend installing CA Network Flow Analysis on a separate drive that is dedicated to CA Network Flow Analysis. Verify that the drive contains the following disk space available: ■ 41 GB for the installation or upgrade files ■ *NFA console or stand-alone server:* 200 GB or more available for data ■ *Harvester or DSA server:* 1 TB of available space for data **Note:** See below for upgrade space information.
CPU	■ *NFA console or stand-alone server:* One 2.26-GHz quad core processors ■ *Harvester or DSA server:* Two 2.26-GHz quad core processors
Memory	■ *NFA console or stand-alone server:* 3 GB RAM ■ *Harvester or DSA server:* 12 GB RAM
Hard drives	■ *NFA console or stand-alone server:* Three 146-GB 10,000-RPM SAS hard drives in RAID5 configuration ■ *Harvester or DSA server:* Six 300-GB 10,000-RPM SAS hard drives in RAID5 configuration
Ports	1-Gb Ethernet port
Screen resolution	Minimum display resolution of 1024x768 (XGA)

Setting or Component	Description
Web browser	Microsoft Internet Explorer version 8 ■ *NFA console or stand-alone server:* (Browser Optional) ■ Clients that log in to the NFA console: (Browser Required) Some other browsers or browser versions may work for logging in from a client, but they have not been tested. **Notes:** The following browser versions have known issues: ■ Microsoft Internet Explorer version 9 - The **Log In** dialog and screen may have display artifacts: The **Log In** button text may be white, although the button is functional. The **Log In** button is located in the bottom right corner of the dialog and has a blue box around it. If you position your cursor inside the box, the cursor changes to *Hand* mode. The log in function is active whenever the cursor is in *Hand* mode. The screen behind the **Log In** dialog may not be rendered in a uniform blue color. ■ Microsoft Internet Explorer version 10 - If you save reports as PDF files or set up scheduled reports to send PDF files, the PDFs are not searchable. The PDFs are rendered as pictures, which do not include searchable text. Working in the CA Performance Center Console: Use Internet Explorer with Compatibility View turned off. You can work in the NFA console with Compatibility View turned on or off. Changing the Compatibility View option for the current session: If you have Internet Explorer Developer Tools installed, press F12 on your keyboard. Select the option that does not contain the phrase "Compatibility View." For information about setting up the browser on the CA NetQoS Performance Center Console server, see the topic "Set Up Internet Explorer" in the *CA NetQoS Performance Center Installation Guide.*
Features, settings, and additional software	■ .NET Framework 3.5 SP1 ■ Java Runtime Engine (JRE) 1.6u45, which is installed automatically during the installation or upgrade of the CA Network Flow Analysis software. ■ Operating system configured as described in the *Installation Guide* or *Upgrade Guide*

Important! Upgrades to CA Network Flow Analysis 9.3.0 require additional space for database migration and backup. To determine the space needed:

1. Locate the following directory: CA\NFA\MySql51\data
2. Determine the size of the directory.
3. Add the size of the directory to the size of the 9.3.0 product install (~1.5 GB) to get the required free disk space.

Note: This is a high estimate; the overall size of the backups will be less than the size of the MySql51\data directory.

Linux System Requirements and Recommendations

If you install the Harvester software on a Linux system, verify that your hardware meets the recommendations and requirements that are noted here, in the *CA Network Flow Analysis Installation Guide,* and in the *CA Network Flow Analysis Upgrade Guide*. For the latest version of the documentation, visit CA Support.

Setting or Component	Description
Operating System	Red Hat Enterprise Linux 5.5 or 5.6 on a 64-bit processor
Language	English, Chinese (Simplified), French (France), or Japanese language The appropriate language packs are required for localized deployments.
Disk Space	Root partition that contains 40 GB of available space Partition for CA Network Flow Analysis that contains the following amounts of available space: ■ 41 GB for the installation files ■ 1 TB for data
CPU	Two 2.26-GHz quad core processors
Memory	12 GB RAM
Hard drives	Six 300-GB, 10,000-RPM SAS hard drives in RAID5 configuration If you do not have enough available space in the /tmp directory and you cannot configure it, relocate the directory. Export the IATEMPDIR environment variable (for the Install Anywhere temporary directory) to set a new location, and select a directory with sufficient available space.
Ports	1-Gb Ethernet port

Setting or Component	Description
Screen resolution	Minimum display resolution of 1024x768 (XGA)
Features, settings, and additional software	■ Java Runtime Engine (JRE) 1.6u45, which is installed automatically during the installation or upgrade of the CA Network Flow Analysis software. ■ System configured as described in the *Installation Guide* and *Upgrade Guide*

Language Support

The current version of CA Network Flow Analysis supports the following locales:

- Chinese (Simplified)
- English (US)
- French (France)
- Japanese

Additional languages may be supported in the future.

Localized versions of the CA Network Flow Analysis Bookshelf are also available on the CA Support product page.

Flow Support

The current version of CA Network Flow Analysis supports NetFlow versions 5, 7, and 9 and the following flow types, provided that they conform to the standards for NetFlow v5, v7, or v9:

- sFlow version 5
- IPFIX
- J-Flow
- cFlow
- Huawei NetStream flow

In order for data from non-sampled flows to appear in reports of 15-minute (historical) data, the following minimum fields are required:

- One of the following: 1 - IN_BYTES, 85 - IN_PERMANENT_BYTES, 231 - FW_INITIATOR_OCTETS, or 232 - FW_RESPONDER_OCTETS
- 4 - PROTOCOL

- 7 - L4_SRC_PORT
- 8 - IPV4_SRC_ADDR
- 10 - INPUT_SNMP
- 11 - L4_DST_PORT
- 12 - IPV4_DST_ADDR

  14 - OUTPUT_SNMP

Note: NetFlow provides a broad view of your network packet streams by creating flow records for all packets. The data from these flow records represents all packets. Sampled NetFlow/IPFIX and sFlow take samples from your packet streams, producing fewer flow records and lessening the impact to a collector. The lower your sampling rate, the less precise the data is likely to be.

Chapter 3: New Features and Enhancements

CA Network Flow Analysis 9.3.0 includes the following new features:

This section contains the following topics:

Performance Enhancements for Large-Scale Deployments

Performance improvements were made for processing Flow Traffic data and synchronizing interfaces between the harvester(s) and the console. Flow Traffic files (FLT) are now processed in a router-oriented way that greatly improves performance. Interface synchronization has also been updated to be router-oriented, thus benefiting from similar performance gains. The combination of the two changes enable large performance gains for calculating enterprise overview data, and keeping interfaces synchronized between harvesters and the console.

Site to Site Reports

Site to Site reports enable you to view volumes of data between two or more sites. A site may be defined as a collection of subnets that can also be discontiguous.

Use Site to Site reports to compare bytes in, rate in, bytes out, and rate out between pairs of sites. You can export the displayed data to a file in comma-separated value (CSV) format.

Create Site to Site reports from the NFA console menu.

You can use saved report definitions to generate an updated report at any time. As the number of reports grows, use the folder management system to keep the reports organized and accessible.

MySQL 5.6 Support

CA Network Flow Analysis 9.3.0 supports updating from MySQL 5.1 to MySQL 5.6.

- New installs and upgrades result in MySQL 5.6 being installed in directory 'MySql'.
- Upgrades result in MySQL application files in the 'MySql51' directory being updated with MySql 5.6 and moved to the 'MySql' directory.
- New installs and upgrades result in a service with the display name 'CA MySQL' and the service name 'NetQoS MySql'.
- Databases will be upgraded using the mysql-upgrade utility after being dumped and imported with 5.6.
- The new UDF will be loaded during MySQL Merge Module process.
- The current my.ini or my.cnf should be backed up.
- Other services' dependencies point to the new mysql 56 service.

Upgrades to CA Network Flow Analysis 9.3.0 require additional space for database backup and migration. For more information, refer to the System Requirements (see page 11).

Status Page Improvements

The **Active Interfaces: Router Information** page and **Available Interfaces: Router Information** page have the following modifications:

Last Poll is now **Flow Status**, a status indicator to show whether the most recent regular polling attempt was successful:

- Red: Any enabled interfaces have not had flow for longer than the **Interface Data Absence Limit**.
- Yellow: Any enabled interfaces have not had flow between 30 minutes and the **Interface Data Absence Limit**.
- Green: All enabled interfaces have had flow in the last 30 minutes.

Traffic Status applies to only the router interface and not all interfaces.

ifType Rejection

CA Network Flow Analysis rejects interfaces at the poller that it should not be receiving NetFlow data from based on ifType.

Some devices report thousands of interfaces via SNMP, but NetFlow is only received on a subset of these interfaces. Rejecting interfaces by type is one way CA Network Flow Analysis can reduce the overall number of interfaces stored in the database, in order to focus more on the interfaces that are actually sending NetFlow.

Chapter 4: Issues Fixed in This Release

This section describes issues that were resolved in CA Network Flow Analysis 9.3.0.

DE35997: Calendar Heat Chart Resolution

In RA 9.0.161, the Calendar Chart presented a 15-minute resolution for a monthly view. In NFA 9.1.3 and 9.2/9.2.1, the data was scaled to show hourly, bi-hourly, etc. data resolution and not the 15-minute resolution that was expected.

For a Monthly view, the calendar heat chart now displays 15-minute data and always at 15-minute resolution.

DE36897: ReportService can start a report more than once

There was a problem with the report scheduling service that could cause a given report to be executed multiple times. This could happen either due to a timing condition in the scheduling code, or when a user pressed **F5** while waiting for report status to update in the **Custom Reports** or **Analysis Reports** pages.

Chapter 5: Known Issues

The following known issues apply to the current release of CA Network Flow Analysis.

This section contains the following topics:

Cannot Upgrade to CA Network Flow Analysis 9.3.0 if NPC Detected

If you have CA NetQoS Performance Center installed on the same server as your NFA Console server, you will need to migrate NPC to a new server before starting the upgrade to CA Network Flow Analysis 9.3.0.

Upgrading to NFA 9.3.0 will upgrade the MySQL version to 5.6 which will not work with NPC.

Follow these steps:

1. Stop the NetQoS Mysql51 service from Windows Services. This should stop all of the NetQoS services.
2. Backup the following directories:
   - (Required) Database directories

     `<install_directory>\Mysql51\data\netqosportal\`

     `<install_directory>\Mysql51\data\em`
   - (Optional) Customized Event Manager Rules

     `<install_directory>\EventManager\EventManagerWS`
   - (Optional) Customized NPC logos or themes

     `<install_directory>\Portal\Website\CSS`
   - (Optional) If SSL was configured for NPC:

     `<install_directory>\SingleSignOn\Configuration\NetQoSPerformanceCenter.xml`
3. Disable NPC by deleting the following registry keys:
   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetQoS Device Manager Service
   - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetQoS EventManager Service
4. Reboot the NFA Console/NPC server and verify that the following services are removed from Windows Services:
   - NetQoS Device Manager Service
   - NetQoS Event Manager Service
5. Install the same version of NPC and Event Manager on the new server, following the instructions in the NPC *Installation Guide*.

   Install to the same drive and path, if possible. If you install to a different drive and/or directory, follow step 12 below after restoring the databases.

6. Stop the “NetQoS Mysql51” service on the new server. Copy the directories and files from step 2 above back to their original locations, to restore the databases and configuration settings.
7. Start all NetQoS services and verify that they start correctly.
8. Launch the NPC web page and go to **Admin > Data Sources**. Find the Event Manager Data Source, select it, and click **Edit**.
9. Change the **Host Name** (IP address) to reflect the IP address of the new Data Source.
10. Launch the Single Sign-On Configuration tool from the desktop, and select the **Performance Center** tab.

    Edit the **Web Service Host** and the **Web Site Host** to be the new IP address of the NPC server.

    Note: If using NPC 6.1SP2 / SSO 6.1.4, the **Web Service Host** and **Web Site Host** parameters do not get exposed in the Single Sign-On Configuration Tool. On the NPC server run the following, replacing the x.x.x.x with the IP address of the new NPC server:

    ```
    mysql -P3308 -D netqosportal -t -e "update
    performance_center_properties set propValue='x.x.x.x' where
    propName='NpcWebServiceHost' or propname='NpcWebSiteHost';"
    ```

    You can verify that these values are changed to the new NPC IP address by running the following query.

    ```
    mysql -P3308 -D netqosportal -t -e "select * from
    performance_center_properties where propname='NpcWebServiceHost'
    or propname='NpcWebSiteHost';"
    ```
11. From the NPC web UI, go to **Admin > Data Sources** and click **Resync All** on each of the Data Sources. This pushes the updated SSO settings down to all data sources.
12. If you have installed NPC to a different drive or path than where it was originally installed, run the following, replacing ”C:/NetQos/portal/tzinfo” with your installation path:

    ```
    mysql -P3308  -D netqosportal –t –e “Update general set
    value=”C:/NetQos/portal/tzinfo” where
    attribute=’TimeZoneDirectory’;”
    ```
13. Recycle the NetQoS Device Manager Service and verify that all data sources are syncing properly on the NPC **Admin > Data Sources** page.
14. You can now safely upgrade your NFA Console server to 9.3.0.

Scheduled Reports on Linux Harvesters

On Linux Harvesters that are involved in scheduled reports, you may notice memory growth over time with repeated execution of reports. If this memory growth becomes problematic, you can schedule a custom storage engine restart via crontab. The following command needs to be run as root in crontab:

```
/etc/init.d/nfa_mysqlCSE restart
```

Note that restarting the custom storage engine will NOT impact data integrity. The only impact would be on any reports that are scheduled to run at the time of the restart.

Requirements for Naming Custom Installation Directories

If you install CA Network Flow Analysis software to a custom directory, make sure that no spaces are included in the installation path or directory name. In addition, use English alphanumeric characters. Non-English characters are not supported.

If you install CA Network Flow Analysis in an environment that is localized for Chinese or Japanese, make sure that you use only ASCII characters for directories in the installation path.

The installation will complete without any easily detected warnings in spite of the invalid path or directory names. Problems occur when you start to use the software, however.

Installation and Upgrade Pre-Requisite Checks

Several pre-requisite checks are performed during an installation or upgrade to help you avoid failure. The pre-requisite checks are designed to detect some obvious problems, but the checks are not comprehensive. You are responsible for preparing and configuring your servers as described in the *CA Network Flow Analysis 9.3.0 Installation Guide* and the *CA Network Flow Analysis 9.3.0 Upgrade Guide*.

Uninstallation Support

The Uninstall option has the following limitations:

- The Uninstall option cannot remove the product if it has been upgraded at any point from CA NetQoS ReporterAnalyzer 9.0.1 (9.0 upgrade 1). The Uninstall program completes successfully, but leaves the system in a state that does not support successful reinstallation of the software. In this case, the Custom Storage Engine (NetQoS NQMySql) service cannot be started.
  To recover from this situation, re-image the system and re-install the software.
  We support using the Uninstall for new installations and for software that has been upgraded from CA Network Flow Analysis versions 9.1.00 through 9.2.0.
- The Uninstall option can remove the MySQL software only if CA Network Flow Analysis was installed before any other related software.
- Other related software that is co-installed with CA Network Flow Analysis is disabled by uninstalling CA Network Flow Analysis.
- Some directories and files are not removed during uninstallation (such as \CA\NFA). You have the option to remove these directories and files manually.
- On a singlebox installation, running the Console uninstall removes files necessary for the Harvester to run (such as the JRE). To switch from a singlebox installation to a Harvester-only installation, you need to uninstall everything and then re-install the Harvester.
- After an uninstall and attempted reinstall, the CA Network Flow Analysis 9.3.0 Console is unreachable. In order to successfully reinstall CA Network Flow Analysis after an uninstallation on the same system:

  1. In the **Control Panel**, **Folder Options**, **View** tab, **Advanced Settings** select **Show hidden files, folders, and drives**.
  2. Navigate to
     `C:\Program Files\Zero G Registry\`
  3. Rename
     `.com.zerog.registry`

     to
     `.com.zerog.registry_backup`
  4. Remove the NetQoS MySql service on each machine with a CA component.
     From a command line:
     `sc delete "NetQoS MySql"`
  5. If running the singlebox (stand-alone) configuration, run the Harvester installer.
  6. Run the Console installer.
  7. Delete the newly created
     `.com.zerog.registry`

8. Rename
   `.com.zerog.registry_backup`

   to
   `.com.zerog.registry`

Error Opening CA NetQoS Performance Center

An error message may open when you attempt to log in to the Single Sign-On program or click the NPC link in the NFA console under the following conditions:

- CA Network Flow Analysis and CA NetQoS Performance Center 6.1 are installed on the same system (this is not a supported configuration)
- CA NetQoS Performance Center 6.1 was installed after CA Network Flow Analysis

In this case a Page Not Found (404) error opens. The program cannot locate the CA NetQoS Performance Center Console because a mixture of forward and backward slashes are used in some directory paths.

Note: This issue applies to deployments that include CA NetQoS Performance Center. If your deployment includes CA Performance Center, this issue does not apply to you.

Workaround:

Complete the following steps to define in the virtual path directories with backward slashes.

1. Log in to the NFA console server as a user with administrator privileges.
2. Open the Internet Information Services (IIS) Manager: Select Start, Administrative Tools, Internet Information Services (IIS) Manager.
3. Expand the tree in the left pane to display the virtual directories:
   a. Click the plus sign next to the server name.
   b. Expand the Sites node.
      The virtual directories appear at the end of the list.
4. Select one of the virtual directories (for example, ProxyServices).
5. Click the Basic Settings link in the right pane.
   The Edit Application dialog opens.
6. Replace any forward slashes in the Physical path value with backward slashes.
7. Click OK to save any changes you made.
8. Repeat the steps to make the correction for each remaining virtual directory.

'Access Denied' Error for LDAP Users

Users with LDAP-generated accounts may get an "Access Denied" error message when they attempt to log in or to drill in to CA Network Flow Analysis from Performance Center. The problem can be caused by one of the following conditions:

- The SSO LDAP configuration is set up with inadequate product permissions to allow access.
  An administrator configures the Single Sign-On program to enable the automatic creation of user accounts at LDAP sign-in. If the configuration is modeled on a user account that lacks the proper product permissions, the LDAP users who are created cannot drill in to the NFA console from Performance Center.
- The LDAP user attempts to drill in before the account information is synchronized between the products. LDAP users acquire product permissions when synchronization is complete.
- The LDAP user attempts to log in to the NFA console before logging in to the Performance Center Console. To create an LDAP-generated user accounts properly, users first must log in to the Performance Center Console. If you attempt to log in to the NFA console first and are denied access, log in to the Performance Center Console, then wait for your user account data to be synchronized with the NFA console.
- The user account was created from a properly configured LDAP model, but the user account was changed later in a way that blocks access.
- An outdated SSO LDAP configuration is in use, which has not been updated since the deployment was upgraded from CA NetQoS ReporterAnalyzer release 9.0.1. Reconfigure the SSO LDAP settings as described in the *Single Sign-On User Guide.*

Complete the following tasks to ensure that LDAP users can drill in:

1. Configure the LDAP settings for the Single Sign-On (SSO) program. For information about this task, download the *Single Sign-On User Guide* from the appropriate Performance Center Bookshelf. If you need further assistance, contact CA Support.
2. Verify that the LDAP settings can be used to authenticate users successfully, as described in the topic 'Validate LDAP Settings' in the *Single Sign-On User Guide.*
3. Create a test case by having a user log in with an LDAP account.
4. Check the user product permissions in the Manage Users page (CA PC) or User List page (NPC).
5. If necessary, revise the model for LDAP configuration to correct any permission problems, then repeat steps 2 through 4.
6. Wait 10 minutes for the next synchronization or perform a Resync on the Manage Data Sources page (CA PC) or the Data Source List page (NPC).

7. Verify that the user can drill in to the NFA console from a view in the Performance Center Console. For example:
   - Click an interface in the Top Flows By Interface - Out view on the Infrastructure Management page.

     This action opens the CA Performance Center Interface Pages.
   - Click the IP Performance tab. and click a link in the Host Name column of the Top Hosts (Pie) - Out view.

     The test user drills in to the NFA console without an Access Denied error message: The NFA console opens to the Interfaces page for the selected host.

Error Creating Custom or Analysis Reports

An error message may open when you attempt to create a Custom Report or Analysis report. This error message includes the text string "System UnauthorizedAccessException." The error occurs because insufficient permissions are assigned to the Internet Guest User Account (IUSR).

On a Windows Server 2008 R2 server, the report is created in spite of the error message.

To correct the problem, complete the following steps.

Workaround:

1. Log in to the NFA console as a user who has administrator privileges.
2. Open the Component Services window:
   a. Select **Start > Run**.
   b. Enter dcomcnfg in the Run window that opens.
   c. Click **OK**.
   The **Component Services** window opens.
3. Display the nqreporter properties:
   a. Expand the following nodes in the left pane:
      - Component Services
      - Computers
      - My Computer
      - DCOM Config

   b. Locate the nqreporter service under DCOM Config.
   c. Right-click nqreporter and select **Properties** from the context menu.
   The nqreporter **Properties** window opens.

4. Display the nqreporter group and user launch permissions:
   a. Click **Security**.
      The Security tab opens.
   b. Select the **Customize** radio button in the **Launch and Activation Permissions** section.
   c. Click **Edit**.
      The **Launch and Activation Permissions** dialog opens.
5. Verify that the IUSR exists:
   a. Click **Add** if the following account is not shown in the "Group or user names" list.
      - Windows Server 2008 R2: IUSR

      The **Select Users or Groups** dialog opens.
   b. Locate and select or enter the object name
      - Windows Server 2008 R2: IUSR
   c. Click **OK**.
      The parent dialog now shows IUSR in the list.
6. Verify that launch and activation permissions are enabled:
   a. Select IUSR in the top pane.
   b. Verify that the **Allow** check box is selected for all of the listed permissions: Local Launch, Remote Launch, Local Activation, and Remote Activation.
7. Save your changes and exit:
   a. Click **OK** in the **Launch and Activation Permissions** dialog.
   b. Click **OK** in the nqreporter **Properties** dialog.
   c. Select **File > Exit** in the Component Services window.
      Users who have the proper permissions now can create Custom Reports and Analysis reports without seeing an error.

Deleting a Harvester

If you delete a Harvester in CA Network Flow Analysis 9.3.0, you cannot add the same Harvester instance again successfully unless the installation server has been re-imaged and the Harvester software has been re-installed. Once you delete a Harvester, you cannot recover any of the data that the Harvester collected.

Manually Updating Polling When Changing SNMP Profiles

If you add or edit an SNMP profile to correct longstanding polling failures, it can be some time before the affected routers are polled again automatically. If polling has been disabled for some time, we recommend that you manually assign the SNMP profile to the routers and refresh polling as described in the following steps.

Follow these steps:

1. Make sure that the SNMP profile is set up correctly on the Manage SNMP Profiles page (CA PC) or SNMP Profiles List page (NPC).
2. Open the Active Interfaces page:
   a. Select Administration from the NFA console menu.
   The Administration page opens.
   b. Select Interfaces: Physical & Virtual from the Administration menu.
   The Active Interfaces page opens, which lists the current routers and their active interfaces.
3. Assign the SNMP profile to the routers:
   a. Select the affected routers in the Active Interfaces list.
   b. Click Edit.
   The Edit Routers dialog opens.
   c. Select the appropriate profile from the SNMP Profile list.
   d. Click Save.
   Your setting is saved for each one of the selected routers. The Edit Routers dialog closes.
4. Refresh the polling for the routers manually:
   a. Select System: Enable Interfaces from the menu on the Administration page.
   The Available Interfaces page opens.
   b. Click the Refresh icon (circular arrow) on the row for each router that has a newly assigned SNMP profile.
   CA Network Flow Analysis attempts to poll the router, then a message opens, which informs you about the success or failure of the polling attempt. Each Refresh icon that you clicked appears dimmed to show that the Refresh operation has been performed.

Previous Button in Harvester and Console Installation Program

The installation program for the Harvester and for the NFA Console has a nonfunctional Previous button on the Choose Install Folder page. If you click the Previous button on this page, the program does not return you to the previous page. In addition, the Previous, Next, and Cancel buttons become inactive.

If you encounter this problem, take one of the following actions:

- Modify the installation directory to reactivate the Next button.
- Close the installation program and restart installation.

DNS Resolution Required for Polling

CA Network Flow Analysis requires DNS name resolution. If host names do not resolve to their corresponding IP addresses, SNMP polling fails.

To determine whether an IP address resolves to a host name on a Linux server, enter the hostname -i command in a command prompt window, as shown in the following example:

```
[root@NFAHARV ReaperArchive15]# hostname -i
```

If the command fails to return the corresponding IP address, you can edit the /etc/hosts configuration file on the Harvester server manually. Add a line for the local server, which associates the host name and IP address.

Follow these steps:

1. Log in to the Harvester server as root or with a sudo user account.
2. Open the /etc/hosts file in a text editor.
3. Add a line that associates the IP address with the local host name, as shown in the following example:

   ```
   [root@NFAHARV ReaperArchive15]# more /etc/hosts;
   # Do not remove the following line, or various programs
   # that require network functionality will fail.
   127.0.0.1             localhost localhost.localdomain localhost
   ::1             localhost6.localdomain6 localhost6
   10.0.0.10      NFAHARV
   ```

   where:

   - 10.0.0.10 = IP address of the Harvester server
   - NFAHARV = Host name of the Harvester server
4. Save and close the /etc/hosts file.
5. Restart the CA Network Flow Analysis services on the Harvester server, including the following services:

   - NFA CollpollWS (nfa_collpollws): CA NFA Collection and Poller Webservices
   - NFA Proxies (nfa_proxies): CA NFA DNS/SNMP Proxies
   - NFA Poller (nfa_poller): CA NFA Poller

   Your change takes effect immediately.

Notes:

- Use this workaround only if DNS resolution fails.

- For additional help with this task, contact CA Support.

Problems from Exporting Flow to Multiple Harvesters

Make sure that you configure flow export to be directed to a single Harvester.

A number of problems result if you configure routers or interfaces to export flow to multiple Harvesters. If this problem occurs, contact CA Support.

You can clone the flow from Harvesters and forward it to other destinations by using the Flow Cloner feature, as described in the *CA Network Flow Analysis Administrator Guide*.

Volume Calculations

Volume totals differ slightly between CA Performance Center views of CA Network Flow Analysis data and corresponding CA Network Flow Analysis reports and pages. The mismatch occurs in pie charts, for example.

Note: The calculation mismatch applies to deployments that include CA Performance Center. If your deployment includes CA NetQoS Performance Center, this issue does not apply to you.

The difference is caused by different calculation methods:

- CA Network Flow Analysis calculates a megabyte as 1,000 kilobytes, which is the standard definition in the context of network data (as recommended by the International System of Units (SI) and the International Electrotechnical Commission IEC).
- CA Performance Center calculates a megabyte as 1,024 kilobytes, which is a typical definition in the context of capacity for server storage and memory.

Interface Names and Descriptions

Interface names and descriptions may not match between the NFA console and the CA Performance Center Console.

Note: Changes to the interface names and descriptions are limited to the product that you use to make the changes. If you change interface descriptions in one product console, the changes are not displayed in the other console, for example. To show the same interface names and descriptions in both locations, make revisions in one product to match the other product.

NFA Console

- The interface name and description is formatted as defined by the interface template, which uses the following values by default:
  - Interface Name: ifName or ifDescr value, whichever is found first
  - Interface Description: portName or ifAlias value, whichever is found first

  For information about changing the default template behavior, see the CA Network Flow Analysis topic 'Edit the Interface Template.'
- To customize interface names and descriptions individually, use the Active Interfaces page. For more information about this task, see the CA Network Flow Analysis topic 'Edit Details for a Router, Interface, or CVI.'

  Any changes you make are shown in a number of locations, including the Active Interfaces page, Enterprise Overview reports, drilldown Interface page reports, and the Interface Index. You use the Interface Index to select interfaces as filters in Custom reports and Analysis reports and to navigate to an interface in the Interface pages.

CA Performance Center Console

- The CA Performance Center Interface Details, Inventory pages, and trend views display interface names and descriptions that use the following default values:
  - Interface Name: ifName, ifDescr, or "Interface {ifIndex}" value, whichever is found first
  - Interface Description: ifDescr value, unless you apply an Interface Description Override to the parent domain

- To customize interface descriptions, apply an Interface Description Override when you create a domain, as described in the CA Performance Center topic 'Add an IP Domain.' To change the Interface Description Override settings for an existing domain, complete the following steps:

  1. Prepare a .csv file with the interface description overrides that you want to use. Include the following columns and populate a row for each interface whose description you want to override: Device IP, Name, Description, and Interface Description Override.
  2. Log in to the CA Performance Center Console as a user with administrator privileges.
  3. Select Admin, IP Domains.

     The Manage IP Domains page opens.
  4. Select the domain that you want to edit.
  5. Click Edit.

     The IP Domains Administration dialog opens.
  6. Click Browse next to the Interface Description Override field.
  7. Locate and select the .csv file that contains the appropriate overrides.
  8. Click Save in the IP Domains Administration dialog.

     The dialog closes.
  9. Resynchronize the CA Network Flow Analysis data source:

     a. Select Admin, Data Sources from the console menu bar.

        The Manage Data Sources page opens.

     b. Select the CA Network Flow Analysis data source.

     c. Click Resync.

        The data source is resynchronized.

     Note: You can wait 5 minutes for the next synchronization to complete automatically instead of resynchronizing manually.
  10. Verify that the overrides have been applied in the Interface Details page, Inventory pages, and trend views.

The interface descriptions apply to devices that have already been discovered and to devices that will be discovered in the future.

False Alarms on the System Status Page

False alarms appear on the System Status page during an initial period after you add a Harvester or DSA in the NFA console. It is expected that Harvesters and DSAs do not pass some system checks until they are fully functional. For example, you may see false alarm status messages that mention the following DSA or Harvester problems:

- Zero value for the Last Load Timestamp and Watchdog polling time
- Unknown usage for memory and disk
- Unknown or high usage for CPU
- Unknown or stopped state for services
- DSA database is down

False alarms typically clear up within an hour of component startup. In some cases, however, the false alarms continue.

If you suspect that the System Status page continues to list false alarms, restart the Watchdog service on the standalone or NFA console server. The current false alarms are cleared from the System Status page and no new false alarms are posted.

DSA Status

If you have a two-tier architecture deployment of CA Network Flow Analysis 9.3.0, the System Status page always shows a green icon for Data Storage Appliances. Data Storage Appliances are not active in the two-tier architecture, but are active for three-tier architecture deployments.

Display Notes Field

Notes fail to display in the NFA Console.

Setting the **Display Notes Field** to **True** (in the **Administration** page, under **System > Application Settings**), causes the **Notes** icon to display in the **Interfaces** page. Clicking the icon displays an error.

Show Device Name

You are allowed to set an Application Setting to remove Device Names from view. If you set **Show Device Name** to **false**, it removes the Device Name for views in NFA Console **Interfaces** page. However, it does NOT remove them for **Enterprise Overview** and **Custom Reports**.

FATAL Error During NFA 9.3.0 Migration

The below ERROR messages will be seen in CA\NFA\MySql_Backups\Backup.log during a migration to 9.3.0, however, these errors will NOT affect the functionality of the product. These are mysql errors that are part of STDERR because the NFA product does not use the MySQL innodb storage engine. These ERRORS can be safely ignored.

```
ERROR 1146 (42S02) at line 62: Table 'mysql.innodb_table_stats' doesn't exist
ERROR 1243 (HY000) at line 63: Unknown prepared statement handler (stmt) given to
EXECUTE
ERROR 1243 (HY000) at line 64: Unknown prepared statement handler (stmt) given to
DEALLOCATE PREPARE
ERROR 1146 (42S02) at line 66: Table 'mysql.innodb_index_stats' doesn't exist
ERROR 1243 (HY000) at line 67: Unknown prepared statement handler (stmt) given to
EXECUTE
ERROR 1243 (HY000) at line 68: Unknown prepared statement handler (stmt) given to
DEALLOCATE PREPARE
ERROR 1146 (42S02) at line 81: Table 'mysql.slave_relay_log_info' doesn't exist
ERROR 1243 (HY000) at line 82: Unknown prepared statement handler (stmt) given to
EXECUTE
ERROR 1243 (HY000) at line 83: Unknown prepared statement handler (stmt) given to
DEALLOCATE PREPARE
ERROR 1146 (42S02) at line 110: Table 'mysql.slave_master_info' doesn't exist
ERROR 1243 (HY000) at line 111: Unknown prepared statement handler (stmt) given to
EXECUTE
ERROR 1243 (HY000) at line 112: Unknown prepared statement handler (stmt) given to
DEALLOCATE PREPARE
ERROR 1146 (42S02) at line 128: Table 'mysql.slave_worker_info' doesn't exist
ERROR 1243 (HY000) at line 129: Unknown prepared statement handler (stmt) given to
EXECUTE
ERROR 1243 (HY000) at line 130: Unknown prepared statement handler (stmt) given to
DEALLOCATE PREPARE
ERROR 1146 (42S02) at line 1894: Table 'mysql.slave_master_info' doesn't exist
ERROR 1146 (42S02) at line 1895: Table 'mysql.slave_master_info' doesn't exist
ERROR 1146 (42S02) at line 1896: Table 'mysql.slave_master_info' doesn't exist
ERROR 1146 (42S02) at line 1897: Table 'mysql.slave_worker_info' doesn't exist
ERROR 1146 (42S02) at line 1898: Table 'mysql.slave_relay_log_info' doesn't exist
ERROR 1146 (42S02) at line 1902: Table 'mysql.innodb_table_stats' doesn't exist
ERROR 1146 (42S02) at line 1906: Table 'mysql.innodb_index_stats' doesn't exist
FATAL ERROR: Upgrade failed
```

User Interface Localization Issues

The topics in this section describe limitations for translated user interfaces in CA Network Flow Analysis 9.3.0.

Installation Directory Names

Installation paths and directories must be named with alphanumeric characters from the Latin alphabet. The installation will complete without any warnings in spite of invalid path or directory names, but a series of problems occur when you start to use the software.

If you use a custom installation path, specify a path that consists of characters from the Latin alphabet. In addition, make sure that the installation path directory names do not contain spaces.

Decimal Value for Regional Setting

The Regional Settings must use a period (.) to indicate a decimal value. If your deployment is localized to French, use the following steps to customize the decimal symbol value. The steps apply to a Windows Server 2008 R2 system.

Follow these steps:

1. Log in to the installation server as a user with administrator privileges.
2. Select Start, Control Panel.
3. Click the Region and Language icon in the Control Panel.

   The Region and Language window opens.
4. Click Additional Settings.

   The Customize Format dialog opens.
5. If the Decimal Symbol value is set to a comma (,), select the period (.) from the drop-down list.

   Note: If the Format value in the Region and Language window is set to French (France), the default setting for the Decimal Symbol is a comma.
6. Save your changes and exit:
   a. Click OK in the Customize Format dialog.
   b. Click OK in the Region and Language window.
   c. Close the Control Panel.

Events in the CA Performance Center Console

The messages in the Event Displays dashboard in the CA Performance Center Console for non-English locales currently contain untranslated entries in the following columns: Event Type, Event SubType, and Description.

Exporting Data to .CSV Files

If you export data from some of the views and reports in the NFA console, the column headings in the .CSV files are not localized. In addition, if non-ASCII characters are used in names of interfaces or other elements, the non-ASCII characters are replaced by question marks in the body of the report.

If you create .CSV files for the CA Network Flow Analysis views that appear in the CA Performance Center Console, the column headings are localized. CA Performance Center does not support non-ASCII characters in custom names currently, and this limitation is reflected in .CSV file data.

Interfaces Over Threshold View

The Direction terms "In" and "Out" are displayed in English in the Interfaces Over Threshold view on the Enterprise Overview dashboard in CA Performance Center. These two terms are not translated in the current release.

SQL-Generated Errors During Installation or Upgrade

If you run an installation or upgrade program in Debug mode, the errors that SQL generates are not translated. The potential SQL errors include:

- Unable to connect to any of the specified MySQL hosts

  Cause: The NetQoS Mysql service on the DSA server is stopped or the NFA console server cannot contact the DSA server.

- Unknown database 'nqrptr'

  Cause: The nqrptr database was not found on the DSA server, which indicates that the DSA software was not installed successfully.

The following MySQL database installation or restore errors are not translated

- During MySql database backup:
  - MySql Database Backup Failed

    An error occurred while attempting to create database backups needed for the MySql upgrade. Please see C:\CA\NFA\MySql_Backups\Backup_Log.log for more information, refer to your installation guide, or contact CA Support for help in upgrading your product.

    The upgrade will be cancelled.

- During MySql database restore:
  - MySql Database Restore Failed

    An error occurred while attempting to restore the database backups created for the MySql upgrade. Please see C:\CA\NFA\MySql_Backups\Backup_Log.log for more information, refer to your installation guide, or contact CA Support for help in upgrading your product.

Installation and Upgrade Messages

The following unlocalized messages may appear during an installation and upgrade.

- Warning that the standalone or NFA console server installation server did not pass the prerequisite check for IIS: "IIS does not appear to be installed"

  Correct this configuration problem by completing the steps in the topic "Enable IIS, COM+, and ASP." You can address this prerequisite warning before or after the installation or upgrade.

- Warning that the Windows installation server did not pass the prerequisite check for DEP: "DEP is disabled or is set for Windows programs only"

  Correct this configuration problem by completing the steps in the topic "Configuring DEP." You can address this prerequisite warning before or after the installation or upgrade.

Installation Pre-Installation Summary Screen

The text string "Install Folder" in the Pre-Installation Summary screen is not properly translated in localized environments.

Report Definition Summary for Analysis Reports (French)

The following Analysis and Custom Report elements are translated poorly when they are localized to French:

- Analysis Report Definition Summary page: Threshold Settings value
- Specify Filters & Rollup page: 'Rollup data using this mask:' label. The terminal punctuation is displayed on a second line--away from the label text.

Default Names for Flow Forensics Reports

The default report names that are automatically generated for Flow Forensics reports are not worded clearly when they are localized to French.

We recommend that report creators assign custom names to their reports. This practice helps make report names more meaningful and avoids the issues with localizations of the default report names.

Harvester Descriptions

When you add a Harvester in the NFA console on a localized CA Network Flow Analysis deployment, the default description may not be clearly worded.

To correct this problem, edit the Harvester description:

1. Log in to the NFA console as a user with administrator privileges.
2. Click Administration, System: Harvester.

   The Harvester page opens.
3. Select the Harvester whose description you want to edit.
4. Click Edit.
5. Enter the new text string in the Description field.
6. Click Save.

   The Harvester description is corrected.

Component Names

The names of some CA Network Flow Analysis components may be unintentionally translated in some localized documentation. The affected components include:

- Harvester
- Data Storage Appliance (DSA)
- Reporter (NFA console)

Third-Party License Agreements

The license agreements for third-party products used in CA Network Flow Analysis are not translated. These license agreements are required to be presented with no alteration of any kind, so they are provided in English only.

Documentation Known Issues

Wildcards Not Supported for Document Searches

Wildcards are not supported for searching documents that you open from the bookshelf. If you use wildcard characters in combination with a text string, the wildcard characters are treated as plain text. In this case, a search returns only the locations that match the literal search entry.

This aspect of the Search function behavior does not match the "Search Tips" information that is included with the Bookshelf. The "Search Tips" information applies only to searches on the Bookshelf landing page.

Documentation Localization Issues

The topics in this section describe the limitations that are associated with translated documentation in CA Network Flow Analysis 9.3.0.

NFA Console Colors in Screen Captures

Elements in the NFA console may look slightly different than they do in localized documentation screen captures.

Content That Is Not Applicable to Localized Documentation

Some documentation content is not applicable to localized audiences:

- CA Anomaly Detector: The optional CA Anomaly Detector program can be installed and used in a localized environment, but the program is not localized for the current release.
  - The English-language Bookshelf contains the *CA Anomaly Detector Guide* and *Release Notes,* which are not included in the localized versions.
  - The *CA Network Flow Analysis Operator Guide* contains localized descriptions of the CA Anomaly Detector views in the Performance Center Console. The views themselves are in English.
  - If you use the CA NetQoS Performance Center Console administration options, the user interface is in English.
  - If your deployment includes CA Performance Center, the CA Anomaly Detector administration options in the NFA console are localized.
  - CA Anomaly Detector sensor names and anomaly messages are in English for all deployments.
  - The CA Anomaly Detector installation program is in English.
- Flow Cloner feature:

  The English version of the *CA Network Flow Analysis Administrator Guide* contains topics about flow cloning, which are not included in the localized Bookshelf. The Flow Cloner feature can be used in a localized environment, but its installation program, configuration options, and logging are not localized.