CA Anomaly Detector

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 7

Product Overview 7
Product Documentation 8
Third Party Acknowledgment and License Agreements 9

Chapter 2: System Requirements 11

Server Recommendations and Requirements 11
Software Compatibility 12
Co-Installation 13

Chapter 3: New Features and Enhancements 15

Upgrade Support 15
Administration Options and Reports 15

Chapter 4: Issues Fixed in This Release 19

Chapter 5: Known Issues and Workarounds 21

Performance Guidelines 21
Overlapping Data in Anomaly Detector Reports 21
Links in CA Performance Center Views 22
Flow Forensics Report Time Frames 22
Destinations for Report Links 23

Chapter 1: Welcome

Welcome to CA Anomaly Detector 9.3.0. Review these notes before you install or upgrade the CA Anomaly Detector 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
- How to locate information about known issues
- How to locate Third Party Acknowledgment and License Agreements

This section contains the following topics:

Product Overview (see page 7)
Product Documentation (see page 8)

Product Overview

CA Anomaly Detector is part of the Infrastructure Performance Analysis product suite. CA Anomaly Detector provides insight into customary network performance, traffic composition, and volumes. The program alerts you when it detects certain types of data or anomalous traffic patterns. Unlike other performance analysis products that are limited to one or two common traffic patterns, CA Anomaly Detector proactively alerts you to a wide range of anomalous behavior by monitoring data from the following components:

- Flow data distillation by CA Network Flow Analysis,
- SNMP collection by CA NetVoyant,
- Application performance derived from TCP through CA Application Delivery Analysis (SuperAgent), and
- Voice performance via CA Unified Communications Monitor.

By leveraging the data that is already collected, CA Anomaly Detector performs its monitoring with minimal configuration and with no need for ongoing data entry.

CA Anomaly Detector can be used with the following types of CA Network Flow Analysis Harvesters:

- Linux-based Harvester that runs a maximum of 2 million flows per minute
- Windows-based Harvester that runs a maximum of 4 million flows per minute and does not run the Flow Cloner
- Windows-based Harvester that runs a maximum of 2 million flows per minute and runs the Flow Cloner

Product Documentation

The following documentation is provided:

- CA Anomaly Detector Guide
- CA Anomaly Detector Release Notes

You can open the documents in PDF and HTML format in any of the following ways:

- Click Help in the CA Network Flow Analysis console and view the Bookshelf for CA Network Flow Analysis 9.3.0.
- View or download the latest CA Network Flow Analysis 9.3.0 bookshelf from the CA Network Flow Analysis product page at CA Support Online.
- View or download the latest CA Anomaly Detector documentation from the CA Anomaly Detector product page at CA Support Online.

The updated *CA Anomaly Detector 9.3.0 Guide* contains installation and upgrade instructions, as well as information for administrators and operators.

The documentation may have been updated since its release. To get the latest documentation updates, download the bookshelf and Readme files from CA Support.

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 and CA Anomaly Detector. 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 CA Network Flow Analysis software:

<install_path>\ThirdPartyContent\ThirdPartyLicenseInfo.pdf

Chapter 2: System Requirements

This section contains the following topics:

Server Recommendations and Requirements (see page 11)
Software Compatibility (see page 12)
Co-Installation (see page 13)

Server Recommendations and Requirements

We tested the product with the following hardware configuration. Your requirements may vary depending on the characteristics and volume of interfaces, applications, and operators in your network.

These recommendations and requirements apply to a physical or virtual dedicated installation server that hosts the CA Anomaly Detector software or hosts both the CA Network Flow Analysis and CA Anomaly Detector software. The specifications match CA appliances that are currently shipping. You can run the product successfully on a server that does not meet these specifications, but your performance may vary. You can also run the product on a server that exceeds these specifications.

Setting or Component	Description
Operating System	Microsoft Windows Server 2008 R2, Standard Edition on a 64-bit processor
Operating System Updates	Latest service pack and all important updates installed **Note**: 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 Anomaly Detector on a separate drive than the operating system. Verify that the drive contains the following disk space available: ■ 41 GB for the installation files ■ 200 GB or more available space for data
CPU	Two 2.26-GHz quad core processors
Memory	12 GB RAM
Hard drives	Three 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	A web browser is required on client systems that are used to view CA Anomaly Detector reports and to configure settings. We recommend Internet Explorer version 8. To work in the Console for CA Performance Center or CA NetQoS Performance Center, use Internet Explorer with Compatibility View turned off. You can work in the NFA console with Compatibility View turned on or off. To change 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."
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 *CA Network Flow Analysis Installation Guide* and the *CA Network Flow Analysis Upgrade Guide,* including: ASP.NET 2.0, including COM+ network access, IIS, and ASP **Note:** ASP.NET 2.0 comes with .NET Framework 3.5.

Notes:

- We support installing CA Anomaly Detector on servers with IPv4 addresses, but not on servers with IPv6 addresses.
- We recommend that you configure a single NIC (network interface card) on the installation server.

Software Compatibility

CA Network Flow Analysis 9.3.0 runs with CA Anomaly Detector 9.3.0, but not with previous versions of CA Anomaly Detector. Upgrade any previous version of CA Anomaly Detector that is currently installed.

CA Anomaly Detector requires that certain software is installed in your environment. The following table describes which software versions are supported:

Program	Supported Version	Required?
CA Anomaly Detector installation that you intend to upgrade *	9.2.1	Required for upgrades
CA Performance Center	2.4/2.3	Required in a deployment that includes CA Performance Center

Program	Supported Version	Required?
CA NetQoS Performance Center	6.1.205 SP2/6.1.194	Required in a deployment that includes CA NetQoS Performance Center
CA Network Flow Analysis (1 instance)	9.3.0	Required to enable AD 9.3.0 operation
CA NetVoyant (1-2 instances)	7.1 SP7	Optional data source for anomaly monitoring
CA Application Delivery Analysis (SuperAgent) (1-2 instances)	10.1	Optional data source for anomaly monitoring
CA Unified Communications Monitor (1-2 instances)	3.7	Optional data source for anomaly monitoring

* If your pre-upgrade CA Anomaly Detector version is earlier than 9.2.1, upgrade to version 9.2.1 before you begin.

Co-Installation

You can install CA Anomaly Detector on the same server that hosts CA Network Flow Analysis software or on a separate server. The following table shows the supported configurations for co-installing CA Anomaly Detector with related software.

- Installation Order: Follow the order shown in the table.
- With CA Network Flow Analysis: You can install CA Anomaly Detector on a server that already hosts the CA Network Flow Analysis stand-alone deployment or the NFA console.
- With Other Related Software: You cannot install CA Anomaly Detector on a server that hosts any of the following software:
  - CA Performance Center
  - CA NetQoS Performance Center
  - CA Application Delivery Analysis (SuperAgent)
  - CA Unified Communications Monitor
  - CA NetVoyant

Components Installed on a Single Server	Supported?
CA Anomaly Detector (AD) with no other related software	Yes
NFA stand-alone (Harvester + NFA console software) + AD	Yes
NFA console + AD	Yes
NPC + the current release of NFA or AD	No

Components Installed on a Single Server	Supported?
CA PC + AD or any NFA component	No
ADA (SA), UCM, or NetVoyant + AD	No

Chapter 3: New Features and Enhancements

The new features for this release are described in this section.

This section contains the following topics:

Upgrade Support (see page 15)
Administration Options and Reports (see page 15)

Upgrade Support

CA Anomaly Detector 9.3.0 supports upgrades from CA Anomaly Detector 9.2.1. CA Anomaly Detector 9.3.0 operates with CA Performance Center 2.3.4/2.3.3 or CA NetQoS Performance Center 6.1.205 SP2/6.1.194. You can use CA Anomaly Detector to gather anomaly data from the later-generation products described in Co-Installation (see page 13).

Administration Options and Reports

Administration options for CA Anomaly Detector 9.3.0 are in the following locations:

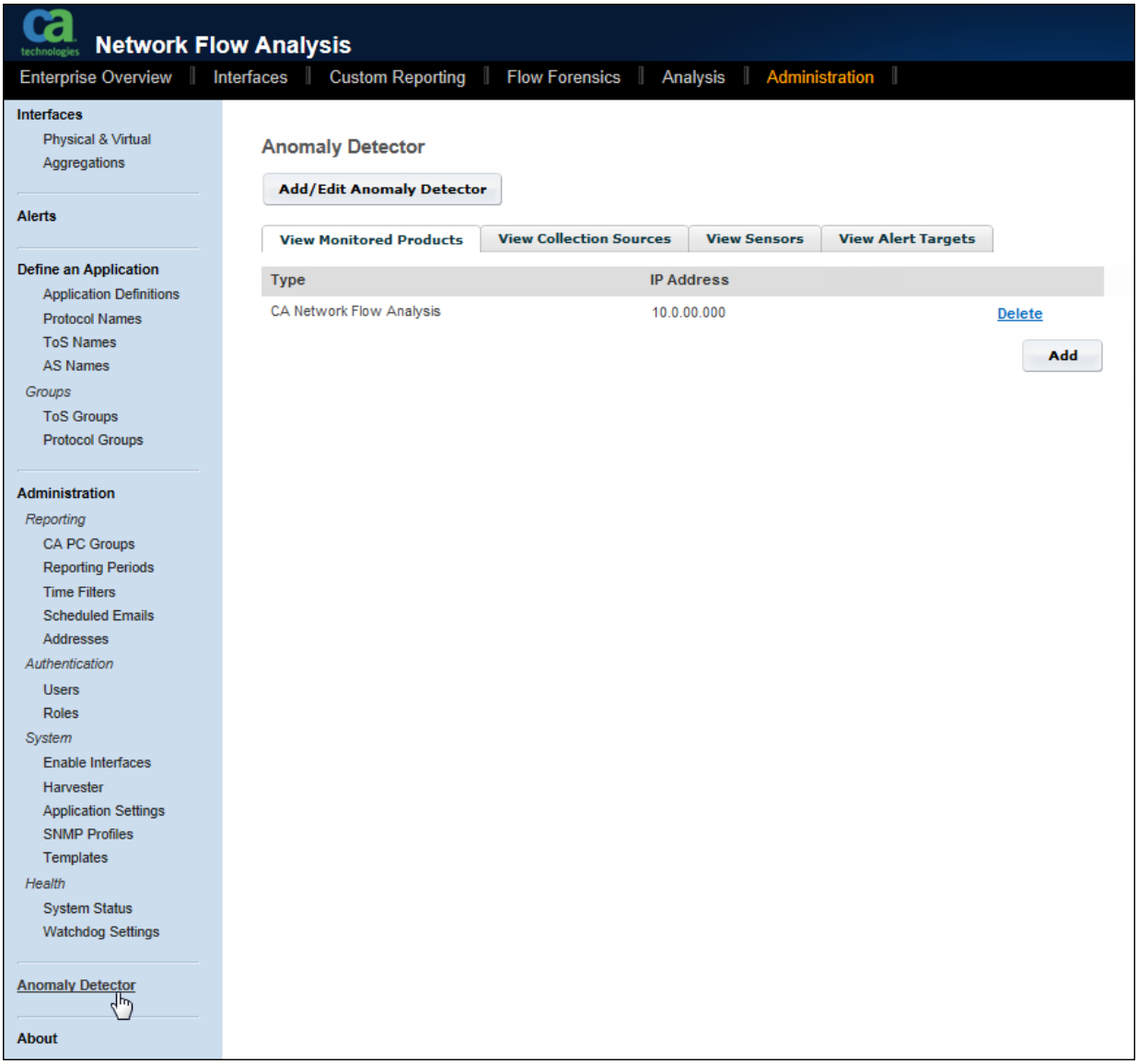
- (CA PC) Anomaly Detector page in the NFA console, which is accessible from the Administration menu
- (NPC) Monitored Products page in the CA NetQoS Performance Center Console, which is accessible by clicking Admin, Product Settings: Name of the CA Anomaly Detector instance.

The options in both locations provide the same functionality. For a CA NetQoS Performance Center deployment, we recommend that you use the functions in the CA NetQoS Performance Center Console. Working in a single location helps to reduce the possibility of multiple users writing to the database simultaneously. If that happens, unexpected results can occur.

Anomaly reports are located on the Anomaly Detector page in the Console for CA Performance Center or CA NetQoS Performance Center.

- (CA PC) If your deployment includes CA Performance Center, you run a special script to display the Anomaly Detector report page for the first time, as described in the *CA Anomaly Detector 9.3.0 Guide*.
- (NPC) The Anomaly Detector page is already included in the CA NetQoS Performance Center Console, so no extra step is needed for this type of deployment.

The following example shows the Anomaly Detector page in the NFA console. After you add an instance of CA Network Flow Analysis on the View Monitored Products tab, the other administration options are enabled.



Chapter 4: Issues Fixed in This Release

This section describes issues that were resolved in CA Anomaly Detector 9.3.0.

154628: Report Links in CA Performance Center Views

Clicking Host links in the CA Performance Center Console views sometimes caused an unexpected page to display.

182440: CA Anomaly Detector Installer Doesn't Install NSAS Database

This issue identified an error in the prerequisites for installing the NSAS database.

182449: CA Anomaly Detector Views in CA NetQoS Performance Center 6.1 Show Errors Related to UTF8

The installer was not specifying the default character set for the server.

Chapter 5: Known Issues and Workarounds

This section describes known issues and suggested workarounds.

Performance Guidelines

Symptom:

CA Anomaly Detector cannot connect to a high-flow Harvester that also runs the Flow Cloner.

Workaround:

Although you can run CA Anomaly Detector with most Harvesters, some limitations apply. In our testing, the following configurations were the maximum configurations that had acceptable performance:

- Linux-based Harvester that runs a maximum of 2 million flows per minute
- Windows-based Harvester that runs a maximum of 4 million flows per minute and does not run the Flow Cloner
- Windows-based Harvester that runs a maximum of 2 million flows per minute and runs the Flow Cloner

Overlapping Data in Anomaly Detector Reports

Symptom:

CA Anomaly Detector reports in the CA NetQoS Performance Center Console sometimes appear to have overlapping data. For example, the 8-hour Anomaly Activity bar chart sometimes shows two bars in a single 15-minute time period.

Description and Workaround:

Any appearance of overlapping data in the reports is a rendering artifact. Changing the reporting time frame may eliminate the artifact. If you drill into the data, you will find that the data is sound.

Links in CA Performance Center Views

Symptom:

When I click Host links in the CA Performance Center Console views, an unexpected page sometimes opens.

Description and Workaround:

In the CA Performance Center Console Enterprise-Wide Anomalies view and Anomaly Drill-in views, Host links for some anomaly types do not behave as expected. If you click a Host link for a CA Unified Communications Monitor or CA Application Delivery Analysis (SuperAgent) anomaly, the Flow Forensics page opens in the NFA console.

If you use CA Anomaly Detector with CA Performance Center, click the Discovered By link for the following anomaly types. Clicking this link displays the parent program for the anomalous data. The affected anomaly types are:

- Voice Call Fan Out
- Voice Call DoS
- Voice Server Distress
- Retransmission Time
- Refused Sessions
- Packet Load

Note: The Host link works as expected for all anomaly types in the CA NetQoS Performance Center Console.

Flow Forensics Report Time Frames

Symptom:

When I click some report links and run the Flow Forensics report definition that opens, the report shows data from a different time frame.

Description and Workaround:

For several anomaly types, the Host links in the Enterprise-Wide Anomalies view and the Anomaly Drill-In views take you to the Flow Forensics page in the NFA console. The Flow Forensics page is pre-defined with filters that correspond to the data you were investigating, such as the host, port, and protocol.

Before you run the Flow Forensics report, check and correct the time frame if necessary. The Flow Forensics report definition is not pre-configured to match the time frame from the original anomaly report.

Destinations for Report Links

Symptom:

I switched from CA NetQoS Performance Center to CA Performance Center. Now when I click links in some anomaly reports, the top-level product page opens for CA NetVoyant, CA Application Delivery Analysis (SuperAgent), or CA Unified Communications Monitor. In CA NetQoS Performance Center, the same links opened more detailed reports.

Description and Workaround:

This is a known limitation of working in CA Performance Center currently. You can drill in to CA NetVoyant, CA Application Delivery Analysis (SuperAgent), or CA Unified Communications Monitor to find the data related to the original anomaly.