Sentinel 7.2.2 Release Notes

January 2015

Sentinel 7.2.2 includes new features, improves usability, and resolves several issues.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the Sentinel forum on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the Sentinel NetIQ Documentation page. To download this product, see the Sentinel Product Upgrade Web site.

You can use Sentinel 7.2.2 only for upgrade installations and not for fresh installations of Sentinel. You can upgrade to Sentinel 7.2.2 from Sentinel 7.0 or later.

1 What’s New?

The following sections outline the key features and functions provided by this version, as well as issues resolved in this release:

1.1 Support for Internet Explorer Version 11

Sentinel 7.2.2 includes support for Microsoft Internet Explorer Web browser version 11.

1.2 Java 7 Upgrade

Sentinel 7.2.2 includes Java 7 update 72, which includes fixes for several security vulnerabilities.

1.3 Reports Support in .csv Format

Sentinel 7.2.2 adds support for generating Sentinel reports in `.csv` format.

To generate reports in `.csv` format:

1. Edit the following entries in the `/etc/opt/novell/sentinel/config/obj-component.JasperReportingComponent.properties` file as follows:
   - `reporting.csv.enable=true`
   - `reporting.csv.outputdir=<the directory where the reports must be stored>`

     The directory path that you specify must have novell permission.
2. Restart Sentinel.

When you generate a report, it is stored in `.csv` format in the folder specified in the `reporting.csv.outputdir` attribute.

1.4 Inclusion of rsync Utility in Appliance

Sentinel appliance now includes the `rsync` utility that helps in data synchronization activities.

1.5 Performance Improvements

Sentinel 7.2.2 improves the overall system performance and also improves the system stability under high events load.

1.6 Software Fixes

Sentinel 7.2.2 includes software fixes that resolve several previous issues.

For the list of software fixes and enhancements in previous releases, see Previous Releases.

1.6.1 Double Quotes Cause an Error in iTRAC Workflow Emails

Issue: When creating a workflow in iTRAC, Sentinel displays an error if emails contain double quotes (“ ”). (BUG 880401)

Fix: Sentinel 7.2.2 modifies the Email rules in iTRAC to allow double quotes in emails.

1.6.2 New Line Characters Cause an Error in iTRAC Workflow Emails

Issue: When creating a workflow in iTRAC, Sentinel displays an error if emails contain new line characters. (BUG 452424)

Fix: Sentinel 7.2.2 modifies the Email rules in iTRAC to allow new line characters in emails.

1.6.3 Security Vulnerability in SSL 3.0

Issue: A vulnerability exists in SSL 3.0, which might allow the plaintext of secure connections to be calculated. For more information, see CVE-2014-3566. (BUG 901536 and BUG 901493)

Fix: Sentinel 7.2.2 fixes the vulnerability in the following ports:

- 10013
- 61616
- 8443

The open ports now use only TLS protocol. Sentinel 7.2.2 disables all SSL 2.0 and SSL 3.0 protocols, and ciphers on these ports.

1.6.4 Sentinel Displays an Error When Creating New Users

Issue: An incorrect validation check prevents you from creating new users if any user is disabled. Sentinel displays the following error when creating a new user:

```
SEN-30005::A database user with the name:<new_user> already exists. Please use a
different user name.
```

(BUG 799946)

Fix: You can now create new users even if any user is disabled.

1.6.5 Validation Weakness in Plug-in Parameters

Issue: Validation checks for Sentinel plug-in configuration parameters are insufficient, and this allows authenticated users to trigger code execution of the inserted parameters. (BUG 894622)

Fix: Sentinel 7.2.2 validates the parameters properly.

1.6.6 Data Synchronization Populates Sentinel IP Address Fields in Hexadecimal Format

Issue: Data synchronization populates SourceIP, TargetIP, and other IP address fields to external databases in hexadecimal format, and not in a human readable format. (BUG 887969)

Fix: By default, Sentinel populates IP address fields in hexadecimal format for efficiency reasons. You can choose to populate the IP address fields in human readable dot notation automatically, by performing the following steps:

1. Log on to the Sentinel server as the novell user.
2. Open the `/etc/opt/novell/sentinel/config/configuration.properties` file.
3. Set the `datasync.saveIPinDottedNotation` property to `true`.
4. Restart the Sentinel server.

NOTE: To hold IPv6-formatted IP addresses, the target database must have target fields that can hold a string of up to 39 bytes.

1.6.7 Sentinel Does Not Create Internal Audit Events for Raw Data File Verification or Download

Issue: Sentinel does not create internal audit events when a user verifies the integrity of the raw data file or downloads a raw data file from the Web UI. (BUG 897097)

Fix: Sentinel now creates the following audit events when a user verifies a raw data file's integrity:

- `VerifyRawDataFileIntegrity` audit event if integrity verification passes.
- `VerifyRawDataFileIntegrity-*-Failed` event if integrity verification fails.
- `DownloadRawDataFiles` audit event when a user downloads a raw data file.

1.6.8 Sentinel Performance Degrades When You Configure Multiple Collector Managers

Issue: In Sentinel environments with multiple Collector Managers, the Collector Managers buffer events because calculation of delay from Collector Managers is not efficient. This causes performance and stability issues in Sentinel environments with multiple Collector Managers. (BUG 903306)

Fix: Sentinel 7.2.2 improves the delay calculation mechanism, and improves Sentinel performance.

1.6.9 After Upgrading to Sentinel 7.2, the SessionType Field is Not Available

Issue: In systems that are upgraded to Sentinel 7.2, the `SessionType` field is not available in the list of available events and in the Tips table. (BUG 891922)

Fix: The `SessionType` field is now available in the systems that are upgraded to Sentinel 7.2.

1.6.10 Retention Period Not Set in Some Default RDD Policies

Issue: Some default RDD policies do not have a set retention period value, which prevents entries in the table associated with the data synchronization policy from being deleted. As a result, the table continues to grow in size and consume disk space. (BUG 894562)

Fix: By default, the retention period value is set to 30 days in all the RDD policies. However, you can change the retention period value.

To change the retention period value:

1. Log on to the Sentinel server as the novell user.
2. Open the `/etc/opt/novell/sentinel/config/configuration.properties` file.
3. Add the `default.global.datasync.retentionperiod` property and set it to the required value.
4. Restart the Sentinel server.

1.6.11 Automatic Triggering of Security Intelligence Data Migration Might Cause Problems

Issue: While upgrading Sentinel 7.1.1 or earlier to Sentinel 7.1.2 or later, security intelligence (SI) data migration is triggered by default. This might cause problems in migration. (BUG 899374)

Fix: Sentinel now disables SI data migration by default. If you choose to enable it, perform the procedure specified in Section 3.1, “Post Upgrade Configuration,” on page 6.

1.6.12 Sentinel Performance Degrades Because Events Queued for Correlation and Active Views Get Full

Issue: Sentinel performance degrades as events queued for correlation and active views get full up to 99% even if the correlation engine is stopped. This occurs even if fewer events are sent to the Sentinel server. For example, less than 1500 EPS fill up the queue even if the Correlation engines are stopped.(BUG 907943)

Fix: Sentinel 7.2.2 improves the performance of event processing components, such as storage, correlation, and active views.

1.6.13 Security Intelligence Dashboards Consume Large Amounts of Memory

Issue: SI dashboards consume large amounts of memory, which results in the Sentinel server shutting down. (BUG 906615)

Fix: Sentinel 7.2.2 fixes this issue by improving the SI processing mechanism.

1.6.14 Sentinel High Availability (HA) Logs Exceptions When You Configure Distributed Search

Issue: You cannot perform a distributed search in a Sentinel HA environment. When you configure a distributed search and specify a Sentinel HA cluster as the target, Sentinel triggers exceptions. (BUG 907376)

Fix: Sentinel 7.2.2 updates the distributed search configuration in Sentinel HA environments.

1.6.15 Documentation for Methods Related to Sentinel Plug-Ins Requires Updating

Issue: The documentation for some methods in Sentinel Plug-ins does not provide examples on how to use the Sentinel Plug-Ins REST APIs. (BUG 892361)

Fix: Sentinel plug-ins documentation contains examples on how to use the REST API for performing various operations.

2 System Requirements

For information about hardware requirements, supported operating systems, and browsers, see Meeting System requirements in the *NetIQ Sentinel Installation and Configuration Guide*.

3 Upgrading to Sentinel 7.2.2

You can upgrade to Sentinel 7.2.2 from Sentinel 7.0 or later.

Download the Sentinel installer from the NetIQ Download Web site. For information about upgrading to Sentinel 7.2.2, see Upgrading Sentinel in the *NetIQ Sentinel Installation and Configuration Guide*.

3.1 Post Upgrade Configuration

- If you are upgrading from Sentinel 7.1.1 or earlier, the installer does not migrate the security intelligence (SI) data by default.

  To manually migrate SI data from Sentinel 7.1.1 or earlier to Sentinel 7.2.2, complete the following steps:

  1. Log on to the Sentinel server as the novell user.
  2. Open the `/etc/opt/novell/sentinel/config/server.xml` file.
  3. Add the following property in the `BaseliningRuntime` component section:

     ```
     <property name="baselining.migration.check">true</property>
     ```

  4. Restart the Sentinel server.

  If the SI data is large, migration might take a long time.
- Sentinel 7.0.3.1 and earlier included an older version of the embedded PostgreSQL database. If you upgrade from Sentinel 7.0.3.1 or earlier, the PostgreSQL database undergoes a major upgrade. The major upgrade process for the embedded PostgreSQL database creates backup files that are only useful if the upgrade process fails. Therefore, after a successful upgrade, you should clean up those files to reclaim the disk space they occupy. For more information about clearing the old PostgreSQL files, see Upgrading Sentinel in the *NetIQ Sentinel Installation and Configuration Guide*.

4 Documentation Updates for Secure Configuration Manager Configuration

When configuring Secure Configuration Manager (SCM) to send compliance information to Sentinel, SCM administrator can configure it in the following two ways:

- To send compliance information as an event.
- To send compliance information as an event, with an attached report.

If SCM administrator configures to send compliance information as an event with attachment, you do not need to perform any configuration in Sentinel to receive compliance information from SCM. Perform the configuration procedure specified in the "Receiving Compliance Details from Secure Configuration Manager" section in the *NetIQ Sentinel Administration Guide* only if SCM administrator has configured to send compliance information just as an event.

5 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support.

5.1 After Upgrading Sentinel 7.2 to a Later Version, Event Fields are Missing in Scheduled Searches

Issue: After upgrading from Sentinel 7.2 to Sentinel 7.2.1 or 7.2.2, searches created and scheduled prior to the upgrade do not display the event fields. (BUG 900293)

Workaround: After you upgrade Sentinel, you must recreate and reschedule those searches that you created and scheduled before the upgrade.

5.2 Loopback IP Address in the Hosts File Causes Synchronization Issue In Sentinel HA

Issue: In Sentinel HA, the `/etc/hosts` file contains the loopback IP address (127.0.0.2) along with the hostname, and this causes synchronization issue. (BUG 906920)

Workaround: Remove the loopback IP address (127.0.0.2) in the `/etc/hosts` file.

5.3 Sentinel Prompts to Log in Again When Viewing NetIQ Change Guardian Reports

Issue: When you view the Change Guardian events and click the Change Guardian icon to view the report, Sentinel prompts you to log in again using the Sentinel credentials. (BUG 896816)

Workaround: There is no workaround at this time.

5.4 Sentinel Does Not Configure the Sentinel Appliance Network Interface By Default

Issue: When installing Sentinel Appliance, the network interface is not configured by default. (BUG 867013)

Workaround: To configure the network Interface:

1. In the Network Configuration page, click **Network Interfaces**.
2. Select the network interface and click **Edit**.
3. Select **Dynamic Address** and then select either **DHCP** or **Static assigned IP Address**.
4. Click **Next** and then **OK**.

5.5 The Web Browser Displays an Error When Exporting Search Results in Sentinel

Issue: When exporting search results in Sentinel, the Web browser might display an error if you modify the operating system language settings. (BUG 834874)

Workaround: To export search results properly, perform either of the following:

- While exporting the search results, remove any special characters (outside the ASCII characters) from the export filename.
- Enable UTF-8 in the operating system language settings, restart the machine, and then restart the Sentinel server.

5.6 Launching the Sentinel Web Console with Port Forwarding or Destination Network Address Translation Displays a Blank Page

Issue: When you launch the Sentinel Web Console using port forwarding or Destination Network Address Translation (DNAT), Sentinel Web Console displays a blank page. (BUG 694732)

Workaround: Do not use port forwarding or Destination Network Address Translation (DNAT) to launch the Sentinel Web Console.

5.7 Sentinel Might Display an Error When You Create or Regenerate a Baseline

Issue: When you create or regenerate a security intelligence baseline, Sentinel creates the baseline successfully, but displays an error message. (BUG 848067)

Workaround: Ignore the error message. The creation of the baseline may take several minutes.

5.8 Partitions Removed from Secondary Storage are Also Removed from Primary Storage

Issue: If the number of days of data that secondary storage can hold is less than the number of days of data that primary storage holds, Sentinel does not use the disk space in primary storage efficiently. Partitions removed from secondary storage to free up space will also be removed from primary storage. (BUG 860888)

Workaround: Allocate enough space in secondary storage to hold data for the total number of days you want to keep online (searchable).

For more information, see “Event Data” in the *NetIQ Sentinel Administration Guide*.

5.9 Sentinel Services Might Not Start Automatically After the Installation

Issue: On systems with more than 2 TB disk space, Sentinel might not start automatically after the installation. (BUG 846296)

Workaround: As a one-time activity, start the Sentinel services manually by specifying the following command:

```
rcsentinel start
```

5.10 Cannot Enable Kerberos Authentication

Issue: If you configure Kerberos authentication in the Kerberos module, the console displays a confirmation message that the Kerberos client configuration was successful. When you view the Kerberos module again, however, the **Enable Kerberos Authentication** option is deselected. (BUG 843623)

Workaround: There is no workaround at this time.

5.11 Unable to Install the Remote Collector Manager If the Password Contains Special Characters

Issue: When you install a remote Collector Manager, if you specify a password that contains special characters, such as '$', '"', '\', or '/', the installation fails with errors. (BUG 812111)

Workaround: Do not use special characters in the remote Collector Manager password.

5.12 Restarting a Remote Collector Manager Causes Some Event Sources to Lose Connection

Issue: When you restart a remote Collector Manager appliance, the Syslog event sources connected on the UDP port lose connection. (BUG 795057)

Workaround: There is no workaround available at this time.

5.13 Unable to View More Than One Report Result at a Time

Issue: While you wait for one report result PDF to open, particularly report results of 1 million events, if you click another report result PDF to view, the report result is not displayed. (BUG 804683)

Workaround: Click the second report result PDF again to view the report result.

5.14 Agent Manager Requires SQL Authentication When FIPS Mode is Enabled

Issue: When FIPS mode is enabled in your Sentinel environment, using Windows authentication for Agent Manager causes synchronization with the Agent Manager database to fail. (BUG 814452)

Workaround: Use SQL authentication for Agent Manager when FIPS mode is enabled in your Sentinel environment.

5.15 Sentinel High Availability Installation in FIPS Mode Displays an Error

Issue: If FIPS mode is enabled, the Sentinel High Availability installation displays the following error:

```
Sentinel server configuration.properties file is not correct. Check the
configuration file and then run the convert_to_fips.sh script again to enable FIPS
mode in Sentinel server.
```

However, the installation completes successfully. (BUG 817828)

Workaround: There is no fix or workaround available at this time. Although the installer displays the error, the Sentinel High Availability configuration works successfully in FIPS mode.

5.16 Sentinel High Availability Installation in Non-FIPS Mode Displays an Error

Issue: The Sentinel High Availability installation in non-FIPS mode completes successfully but displays the following error twice:

```
/opt/novell/sentinel/setup/configure.sh: line 1045: [: too many arguments
```

(BUG 810764)

Workaround: There is no fix or workaround available at this time. Although the installer displays the error, the Sentinel High Availability configuration works successfully in non-FIPS mode.

5.17 Appliance Update From Versions Prior to Sentinel 7.2 Fails in WebYaST

Issue: Appliance update from versions prior to Sentinel 7.2 fails because the vendor for the update packages has changed from Novell to NetIQ. (BUG 780969)

Workaround: Use the zypper command to upgrade the appliance. For more information, see Upgrading the Appliance by Using zypper in the *NetIQ Sentinel Installation and Configuration Guide*.

5.18 Issue with Sentinel Appliance Login

Issue: If you specified a $ character in the password, Sentinel stores the password differently in the database depending on where the $ is placed in the password. If the password starts with the $ special character, Sentinel stores the password with a file name. If the $ character is somewhere in the middle of the password, Sentinel truncates the password to the location of the $ character. (BUG 734500)

Workaround: The actual password is stored in the `home/novell/.pgpass` file. Obtain the password from this file and then log in to Sentinel. For example, if you specified the password as abc$123, the Sentinel stores the password as abc in the `.pgpass` file. You can log in to Sentinel by specifying abc as the password.

5.19 Error While Installing Correlation Rules

Issue: Solution Manager does not install correlation rules when a correlation rule with an identical name already exists on the system. A `NullPointerException` error is logged in the console. (BUG 713962)

Workaround: Ensure that all correlation rules have a unique name.

5.20 Sentinel Link Action Displays Incorrect Message

Issue: When you execute a Sentinel Link action from the Web console Sentinel displays a success message even though the Sentinel Link Connector integrator test failed from the Sentinel Control Center. (BUG 710305)

Workaround: There is no workaround at this time.

5.21 Dashboard and Anomaly Definitions with Identical Names

Issue: When a Security Intelligence dashboard and an anomaly definition have identical names, the dashboard link is disabled on the Anomaly Details page. (BUG 715986)

Workaround: Ensure you use unique names when creating dashboards and anomaly definitions.

5.22 Active Search Jobs Duration and Accessed Columns Inaccuracies

Issue: The Sentinel Web console displays negative numbers in the Active Search Job Duration and Accessed columns when the Sentinel Web console computer clock is behind the Sentinel server clock. For example, the Duration and Accessed columns display negative numbers when the Sentinel Web console clock is set to 1:30 PM and the Sentinel server clock is set to 2:30 PM. (BUG 719875)

Workaround: Ensure the time on the computer you use to access the Sentinel Web console is the same as or later than the time on the Sentinel server computer.

5.23 IssueSAMLToken Audit Event Displays Incorrect Information in the Security Intelligence Dashboard

Issue: When you log in to the security dashboard and perform a search for `IssueSAMLToken` audit event, the `IssueSAMLToken` audit event displays incorrect hostname (InitiatorUserName) or (IP address) SourceIP. (BUG 870609)

Workaround: There is no workaround at this time.

5.24 Sentinel Web Console Displays Remote Collector Manager Health Status Incorrectly

Issue: The **Event Sources** tab in the Sentinel Web console displays the Remote Collector Manager health status incorrectly as Warning. (BUG 895343)

Workaround: Check the delay duration of the Remote Collector Manager in the **General Information** section. If the delay is less than five seconds, you can ignore the warning status.

5.25 Distributed Search Results with More Than 50,000 Events Cannot be Exported to a File

Issue: You cannot export distributed search results with more than 50,000 events to a file. (BUG 863985)

Workaround: There is no workaround at this time.

5.26 Sentinel Control Center Does Not Launch When NetIQ Identity Manager Designer is Installed on the Client Computer

Issue: Sentinel Control Center does not launch when the NetIQ Identity Manager Designer is installed on the client computer and Designer uses the system JRE. Designer needs to add some supporting jar files like `xml-apis.jar` to the `lib/endorsed` directory. Some of the classes in the `xml-apis.jar` file override the corresponding classes in the system JRE that is used by the Sentinel Control Center. (BUG 888085)

Workaround: Configure Designer to use its own JRE.

5.27 Connection Problems between Clients and Sentinel Running in FIPS Mode

Issue: Sentinel 7.2.1 includes Oracle Java 1.7 update 65, which has a known issue related to RSA client key exchange in FIPS mode. For more information, see the Java SE Development Kit 7, Update 51 Release Notes. This causes connection problems when Sentinel is running in FIPS mode and attempting to receive connections from clients such as Security Manager and Sentinel Agent Manager. (BUG 872305)

Workaround: To successfully establish the SSL connection in FIPS-compatible mode, downgrade the Java version on all Sentinel servers to Java 7 update 45 (which does not have the key exchange issue).

For more information, see the instructions in TID 7014980 in the NetIQ Support Knowledge Base.

NOTE: To establish successful connection between Sentinel Agent Manger and Sentinel running in the FIPS mode, ensure you install or upgrade to Sentinel Agent Manager Connector 2011.1r3. To download the Sentinel Agent Manager Connector, see the Sentinel Plug-ins Web site.

5.28 The Network Flow Charts Appear Blank if there is no Packets Information

Issue: If the network flow data from network devices does not include packets information, the network flow charts appear blank in the Sentinel Web console. (BUG 875055)

Workaround: Configure the network device such that it sends all the three counters: bytes, flows, and packets. To configure the network device, see the relevant network device documentation.

5.29 The Message Queuing Service Uses Large Amount of Memory of the Central Computer in Sentinel Agent Manager

Issue: The message queuing service (mqsvc.exe) uses a large amount of memory of the Central Computer in the Sentinel Agent Manager. The Microsoft Message Queuing (MSMQ) does not perform a cleanup operation after the remote transactional read. For more information about this issue, see http://support.microsoft.com/kb/2566230. (BUG 869980)

Workaround: To ensure that mqsvc.exe does not use a lot of memory:

- Apply the latest hotfix of the Microsoft Message Queuing (MSMQ) from the Microsoft Web site.
- Increase the overall memory in proportion to the increase in size of the MSMQ journal.

5.30 Sentinel Agent Manager Stops Working After You Upgrade Windows

Issue: The Agent Manager uses certificates for authentication between Central Computer and Agents. When you upgrade the Windows operating system, a known issue in Microsoft Windows deletes some of these certificates and prevents the Agent Manager from restarting after the upgrade. (BUG 847891)

Workaround: Before you upgrade Windows, back up the Agent Manager system certificates and restore them after you upgrade Windows, by performing the following steps:

1. Export the registry key:
   - **1a** Open the command prompt as an administrator and enter the command `regedit`.
   - **1b** In the Registry Editor, Expand **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Microsoft** > **SystemCertificates**.
   - **1c** Under **SystemCertificates**, right-click the **NetIQ Security Manager** folder and select **Export**. Save the registry key as a `.reg` file.
   - **1d** Back up the `.reg` file.
2. (Conditional) If you have changed the default location for the SAM certificate installation, back up the certificates from the custom location.
3. (Conditional) If you have installed any custom certificates for authentication between the Central Computer and Agents, back up the custom certificates.
4. Perform the Windows upgrade.
5. Double-click the `.reg` file generated in Step 1 to import the certificates into the registry.
6. (Conditional) Reinstall the certificates that were backed up in Step 2 and Step 3 at the appropriate locations.
7. Restart the Agent Manager service.

5.31 The Agent Manager Does Not Capture the Windows Insertion String Fields With Null Values

Issue: While collecting event data, the Agent Manager does not capture the Windows Insertion String fields with null values. `(BUG 838825)`

Workaround: There is no workaround at this time.

6 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information Web site.

For general corporate and product information, see the NetIQ Corporate Web site.

For interactive conversations with your peers and NetIQ experts, become an active member of our community. The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

7 Legal Notice

THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material (“Module”) is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

For information about NetIQ trademarks, see http://www.netiq.com/company/legal/.