Sentinel 7.2.1 Release Notes

October 2014

Sentinel 7.2.1 includes new features, improves usability, and resolves several previous 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.

Sentinel 7.2.1 can only be used for upgrade installations. You can upgrade to Sentinel 7.2.1 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 Integration with NetIQ Secure Configuration Manager

Sentinel 7.2.1 extends its compliance monitoring capability by integrating seamlessly with the upcoming release of NetIQ Secure Configuration Manager. Integration with the Secure Configuration Manager 6.0 and later helps you to assess system configurations against regulatory requirements, security best practices, and corporate IT policies to demonstrate compliance and manage information security risk. This integration helps you to view the security and audit information from both Sentinel and Secure Configuration Manager in a single interface. For more information, see Viewing Compliance to Configuration Policies in the *Sentinel Administration Guide*.

1.2 Searching and Reporting

Sentinel 7.2.1 now enables you to export the desired event fields when scheduling a search from the newly created search templates. To export the desired event fields, in the **Reports and Searches** panel, select the desired search template, and then click **Schedule**. Specify the event fields you want to export in the **Event fields** field.

For information about search templates, see Saving a Search Query as a Search Template in the *NetIQ Sentinel User Guide*.

NOTE: Search templates created before upgrading to Sentinel 7.2.1 do not support the export of specific event fields.

1.3 Java 7 Upgrade

Sentinel 7.2.1 includes Java 7 update 65, which includes fixes for several security vulnerabilities.

1.4 Software Fixes

Sentinel includes software fixes that resolve several previous issues.

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

1.4.1 Keystore and Truststore Passwords are Visible in the Logs

Issue: The keystore and truststore passwords are unmasked in the `server0.0.log` file. `(BUG 884298)`

Fix: The keystore and truststore passwords are now masked in the `server0.0.log` file.

1.4.2 Sentinel Incorrectly Prompts to Save the Correlation Rule When Not Modified

Issue: In the **Correlation** panel, when you select a correlation rule and click **Edit**, the correlation rule open in a new tab. When you close the correlation rule tab without making any changes, Sentinel still prompts you to save the rule. `(BUG 793034)`

Fix: Sentinel no longer prompts you to save the correlation rule if no changes are made.

1.4.3 A Blank Pop-up Appears on Clicking the Help Button in Solution Manager

Issue: In the first screen of the **Install Control Wizard**, when you click **Help** in the Solution Manager, a blank pop-up appears. This pop-up does not provide any help information. `(BUG 816481)`

Fix: This service pack removes the help button from the first screen of the **Install Control Wizard**.

1.4.4 The Next Button Does Not Perform Any Action in Solution Manager

Issue: The **Next** button that appears in the last screen in the **Install Control Wizard** in Solution Manager does not perform any action. `(BUG 816489)`

Fix: This service pack removes the Next button from the last screen of the **Install Control Wizard**.

1.4.5 EPS Column is Hidden in the Event Sources Table

Issue: In the Sentinel web interface, **Collection** > **Event Sources** > **Event Sources** table, the EPS column is not fully visible. `(BUG 885535)`

Fix: The EPS column is now fully visible in the Event Sources table.

1.4.6 Search Results Might Appear Blank

Issue: When you search a query with a large number of results, if you scroll down to see the last search result on the page and then scroll up back to see the previous results, the previous results are displayed as blank. (BUG 869553)

Fix: The Search results no longer appear blank.

1.4.7 Error When Importing a Modified Report Data Definition

Issue: When you use the Sentinel Plug-ins SDK to modify an existing Report Data Definition (RDD) and import the modified RDD into Sentinel, the following error is displayed: (BUG 873512)

```
There is already a report data definition in the system that has the same ID as the
one you are importing, but an error occurred on the system when comparing them:
null.
```

Fix: You can now import the modified RDD successfully without any error.

1.4.8 The View Triggers Option is Disabled for Correlated Events

Issue: The View Triggers option is disabled for correlated events triggered by events received from remote Sentinel servers connected through Sentinel Link. (BUG 719106)

Fix: The **View triggers** option is now enabled for correlated events triggered by events received from remote Sentinel servers connected through Sentinel Link.

1.4.9 The TargetDataContainer Event Field Size is Restricted to 256 Characters

Issue: The TargetDataContainer event field size limit is 256 characters. This limit results in data truncation when parsing values more than 256 characters. (BUG 890571)

Fix: The TargetDataContainer event field size limit is now increased to 4000 characters.

1.4.10 Error While Running Reports After Changing the Sentinel Locale

Issue: After you change the Sentinel Locale and the operating system language, Sentinel displays an error when you run scheduled reports. (BUG 872685)

Fix: Sentinel now generates the scheduled reports properly after the locale has been changed.

1.4.11 Partitions on Secondary Storage are Not Deleted After their Retention Period

Issue: Sentinel fails to delete the partitions that exist only in the secondary storage, after their retention period is expired. (BUG 891809)

Fix: Sentinel now deletes the partitions from the secondary storage after their retention period is expired.

1.4.12 Sentinel Stores the User Credentials in the Server Logs When the Keystore Certificate is Large

Issue: When the keystore certificate is large and you attempt to log in to the Sentinel Web interface, the initial login attempt fails. When you try to log in again, the login is successful, but Sentinel stores the user name and password in the server log file. (BUG 889596)

Fix: Sentinel now allows you to log in successfully when the keystore certificate is large and no longer stores the user name and password in the server logs.

1.4.13 Error Message is Not Informative When Distributed Search Fails

Issue: When you perform a distributed search and a remote server fails to respond, an error is displayed. The error message does not indicate which remote server is unresponsive and is causing the error. (BUG 881076)

Fix: The error message now specifies the IP address of the remote server causing the error. The remote server IP address is also included in the logs.

1.4.14 Exceptions are Logged When an Invalid Regular Expression is Specified in the Match Regex Filter

Issue: When creating a correlation rule in the **Expression Builder**, if you build an expression using the **Match Regex** operator and specify an invalid regular expression, Sentinel does not validate the regular expression. Invalid regular expressions in the match regex filter causes Sentinel to log a large number of exceptions. (BUG 882461)

Fix: If the regular expression is not valid, Sentinel now displays an error and does not allow you to save the correlation rule.

1.4.15 Complex Active View Filters Slow Down the Overall Sentinel Performance

Issue: When you specify complex filters in Active View, overall Sentinel performance slows down. (BUG 847042)

Fix: A complex active view filter no longer affects the overall performance of Sentinel.

1.4.16 Sentinel Takes Long Time to Evaluate Large Events

Issue: Evaluation of large events to determine which event retention policy applies can decrease the overall Sentinel performance. (BUG 888778)

Fix: Sentinel now uses a multi-threaded approach to apply the retention policies. Therefore, Sentinel does not take a long time to evaluate the events.

1.4.17 Log Message is Not Informative When Sentinel is Unable to Read a Dynamic List

Issue: When Sentinel is unable to read a dynamic list, it generates an audit log message that does not include the dynamic list name. (BUG 885505)

Fix: The log message now specifies the name of the dynamic list that Sentinel is unable to read.

1.4.18 Collector Manager Drops Events When Disconnected From Sentinel

Issue: While sending events to Sentinel, the Collector Manager drops events if it gets disconnected from Sentinel or the Sentinel service is restarted. (BUG 875635)

Fix: Collector Manager no longer sends events while Sentinel is disconnecting or restarting. Therefore, no events are lost when Sentinel disconnects or when the Sentinel service is restarted.

1.4.19 Sentinel Does not Correlate Remote Correlated Events by Default

Issue: Sentinel does not correlate the correlated events received from remote Sentinel servers by default. (BUG 892954)

Fix: Sentinel now correlates the correlated events received from remote Sentinel server. For more information, see Creating Correlation Rules in the *NetIQ Sentinel User Guide*.

1.4.20 A Few Weeks After Installation, Storage Forecast Charts Display Historical Data

Issue: A few weeks after Sentinel installation, the primary and secondary storage forecast charts in the Sentinel Web interface age and start displaying the historical data instead of the forecast data. (BUG 814228)

Fix: The storage forecast charts now display at least 30 days of forecast data at any time. Also, the **Total capacity needed (for the next 90 days)** value mentioned below the charts is correct.

1.4.21 Local Storage Space is Occupied When Report Fails

Issue: When running reports, Sentinel creates a temporary file and deletes it after creating the report. If the report creation is terminated abruptly, Sentinel does not delete the temporary file and it continues to occupy local storage space. (BUG 886395)

Fix: Sentinel now deletes the temporary file even if the report is terminated abruptly.

1.4.22 Sentinel Login Fails if the Webserver Certificate Key is Large

Issue: When you log into Sentinel, if the webserver certificate key is large, it results in large-sized tokens, which are not stored by the browser. Therefore, the login fails with the following error: (BUG 825640)

```
Error loading current user data.Object of type 'user' with key values '[_CURRENT_]' not found.
```

Fix: Sentinel now allows you to log in successfully without any errors even if the webserver certificate key is large.

1.4.23 Sentinel Allows Access Even After the Browser Session is Expired

Issue: Sentinel allows access to the sever using expired or invalid tokens through REST even after the browser session is expired or the Sentinel server is restarted. (BUG 873163)

Fix: Sentinel now checks for the authenticity of the token before granting access. Therefore, Sentinel does not allow access after the browser session is expired or Sentinel server is restarted.

1.4.24 Multiple Entries Are Created in the Vulnerability Database Tables For an Asset

Issue: Sentinel creates multiple entries in the vulnerability database tables, `VULN_RSRC` and `VULN_SCAN`, for the same asset when the collector sends vulnerability data. (BUG 890384)

Fix: Sentinel now creates only a single entry in the vulnerability database tables for an asset.

1.4.25 Sentinel Does Not Update the Vulnerability Database For Assets Properly

Issue: Sentinel does not insert or update the vulnerability data, received through the Process connector, in the database tables for assets that already exist in the table. (BUG 888369)

Fix: Sentinel now updates the vulnerability data in the database tables even for assets that already exist in the table.

1.4.26 The Database Table Displays Incorrect Size of the Event Storage

Issue: The database table, `ixlog_part`, displays incorrect size of the event storage in the `byte_count` column. (BUG 875671)

Fix: The event storage sizing calculation is now revised. The database table now displays the correct size of the event storage.

1.4.27 Sentinel Logs Exceptions When Deleting Expired Raw Event Data

Issue: Sentinel logs the following exception when deleting expired raw event data from the secondary storage according to the retention policies: (BUG 886587)

```
Error RAWDATA0004(RawData): No record found in database for raw data file
```

Fix: Sentinel no longer logs exceptions when deleting expired raw event data from the secondary storage.

1.4.28 Sentinel High Availability Appliance Installations Fail to Upgrade Through WebYast

Issue: Sentinel high availability appliance installations fail to upgrade through WebYast on the passive nodes in the cluster. (BUG 873467)

Fix: Sentinel high availability appliance installations now upgrade through WebYast successfully.

[Return to Top]

2 System Requirements

You can upgrade to Sentinel 7.2.1 from Sentinel 7.0 or later.

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

[Return to Top]

3 Upgrading to Sentinel 7.2.1

Download the Sentinel installer from the NetIQ Download Web site. For information about upgrading to Sentinel 7.2.1, see Upgrading Sentinel in the *NetIQ Sentinel Installation and Configuration Guide*.

NOTE: 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*.

[Return to Top]

4 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.

4.1 Sentinel Web Interface Displays Remote Collector Manager Health Status Incorrectly

Issue: The Sentinel Web interface > **Collection** > **Event Sources** tab 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 5 seconds, you can ignore the warning status.

4.2 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.

4.3 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 (http://www.oracle.com/technetwork/java/javase/7u51-relnotes-2085002.html). This causes connection problems when Sentinel is running in FIPS mode and attempting to receive connections from clients like 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 doesn't 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.

4.4 The Sentinel Appliance Network Interface is Not Configured 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 **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**.

4.5 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.

4.6 Sentinel Web Console Displays a Blank Page When Launched Using Port Forwarding or Destination Network Address Translation

Issue: When Sentinel Web Console is launched 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.

4.7 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.

4.8 The Message Queuing Service Utilizes Large Amount of Memory of the Central Computer in Sentinel Agent Manager

Issue: The message queuing service (mqsvc.exe) utilizes 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 the message queuing service (mqsvc.exe) does not utilize 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.

4.9 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, some of these certificates are deleted. This is a known issue in Microsoft Windows. Therefore, the Agent Manager service does not start after the upgrade. (BUG 847891)

Workaround: Before you upgrade Windows, back up the Agent Manager system certificates and restore them after you upgrade Windows.

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.

4.10 The Agent Manager Drops the Windows Insertion String Fields With Null Values at the End of the Insertion String Array

Issue: The Agent Manager drops the Windows Insertion String fields with null values at the end of the Insertion String array. This issue applies only if you are building or customizing a Collector and using the insertion string array for your data. `(BUG 838829)`

Workaround: There is no workaround at this time.

4.11 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 utilize 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 the total number of days worth of data you want to keep online (searchable).

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

4.12 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.

4.13 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.

4.14 Sentinel Services Might Not Start Automatically After the Installation

Issue: On systems with more than 2 TB, 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 in `/usr/sbin/rcsentinel`:

```
rcsentinel -start
```

4.15 Cannot Enable Kerberos Authentication

Issue: In the Kerberos module, when you select **Enable Kerberos Authentication**, configure Kerberos authentication, and click **Save**, the console displays a message to confirm that the Kerberos client configuration was successful. However, the Kerberos authentication is not enabled and when you view the Kerberos module again, the **Enable Kerberos Authentication** option is deselected. (BUG 843623)

Workaround: There is no workaround at this time.

4.16 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 does not proceed and results in errors. (BUG 812111)

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

4.17 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 the time of this release.

4.18 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.

4.19 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.

4.20 Sentinel High Availability Installation in FIPS Mode Displays an Error

Issue: If FIPS mode is enabled, the Sentinel High Availability installation displays the `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` error. However, the installation completes successfully. (BUG 817828)

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

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

Issue: The Sentinel High Availability installation in non-FIPS mode displays the `/opt/novell/sentinel/setup/configure.sh: line 1045: [: too many arguments` error twice. However, the installation completes successfully. (BUG 810764)

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

4.22 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*.

4.23 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.

4.24 Solution Manager Installation of 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 all correlation rules have a unique name.

4.25 Sentinel Link Action Displays Incorrect Message

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

Workaround: There is no workaround at this time.

4.26 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.

4.27 Active Search Jobs Duration and Accessed Columns Inaccuracies

Issue: The Sentinel Web interface displays negative numbers in the Active Search Job Duration and Accessed columns when the Sentinel Web interface computer clock is behind the Sentinel server clock. For example, the Duration and Accessed columns display negative numbers when the Sentinel Web interface 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 interface is the same as or later than the time on the Sentinel server computer.

4.28 When You Log In to the Security Intelligence Dashboard, the IssueSAMLToken Audit Event Displays Incorrect Information

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.

[Return to Top]

5 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.

[Return to Top]

6 Legal Notice

NetIQ Domain Migration Administrator is protected by United States Patent No(s): 05829001.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, 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/.

[Return to Top]