NetIQ Sentinel 7.2 Release Notes

June 2014

Sentinel 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 inputs. We hope you continue to help us ensure our products meet all your needs. You can post feedback in the Sentinel Community Support Forums, our community Web site that also includes product notifications, blogs, and product user groups.

The documentation for this product and the latest release notes are available on the NetIQ Web site 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 7.2 Documentation Web site.

To download this product, see the Sentinel Product Web site.

1 What's New?

The following sections outline key features and enhancements, and also the issues resolved in this release:

1.1 Visualizing Network Traffic

To perform a complete investigation and analysis of a security event, you might want to monitor network activities in detail. Sentinel helps you monitor your enterprise network by collecting, visualizing, and analyzing network flow data. For more information, see "Visualizing Network Traffic" in the *NetIQ Sentinel Administration Guide*.

1.2 Data Feed Plug-Ins

Sentinel now provides a new type of plug-in, Data Feed, to download the external intelligence data. In this release, Sentinel provides three data feed plug-ins: Palevo tracker, ZeuS tracker, and SpyEye tracker that download lists of known botnet IP addresses and domains. These plug-ins help you detect botnets in your enterprise network. The Data Feed plug-ins are bundled in Solution Packs, which are installed by default when you install Sentinel. For more information about data feeds, see "Managing Data Feeds" in the *NetIQ Sentinel Administration Guide*.

1.3 Out-of-the-Box Solution Pack for Threat Intelligence

Sentinel includes the Solution Pack for Threat Intelligence that helps you manage complex network security threats in your enterprise. This Solution Pack integrates data from Sentinel Advisor service, third-party vulnerability scanner, and intrusion detection applications and devices to provide an unprecedented visibility into your enterprise security. This Solution Pack also includes the new data feed plug-ins that help you detect botnet connections in your enterprise network. For more information about this Solution Pack, see the Solution Pack for Threat Intelligence documentation on the Sentinel Plug-ins Web site.

1.4 Ability to Configure Password Complexity

A complex password improves security by preventing password guessing attacks. Sentinel provides a set of password validation rules that help you maintain a complex password for all local user passwords. You can select the desired validation rules as applicable for your environment. For more information, see "Configuring Password Complexity" in the *NetIQ Sentinel Administration Guide*.

1.5 Optional High Availability Configuration in Appliance Installations

Sentinel now supports high availability configuration in appliance installations. This feature requires a separate license. For more information, contact NetIQ Sales Support.

For information about configuring High Availability in appliance, see "Configuring Sentinel for High Availability" in the *NetIQ Sentinel Installation and Configuration Guide*.

1.6 Latest Plug-Ins

Sentinel 7.2 includes new and updated versions of Sentinel plug-ins. The latest version of Collectors and Connectors are available only when you perform a new installation. The latest versions of Integrators and Actions are available in both new and upgrade installations. For upgrade installations of Sentinel 7.2, you can visit the Sentinel Plug-ins Web site, review the revision history of the latest Collectors and Connectors in the specific documentation, and then determine which plug-ins to download and install.

NOTE: Before you upgrade to Microsoft Active Directory and Windows Collector 2011.1r4, you must upgrade to Sentinel Agent manger 7.2 to ensure that it is compatible.

1.7 Enhancements

Sentinel 7.2 includes the following enhancements:

1.7.1 Java 7 Upgrade

Sentinel 7.2 now includes Java 7 update 51, which includes fixes for several security vulnerabilities.

1.7.2 Content Backup Utility for Sentinel Agent Manager

Sentinel 7.2 includes the Content Backup utility that helps you back up and restore the Agent Manager data collection policies. For more information about the Content Backup utility, see the Backing Up and Restoring Data Collection Policies in the NetIQ Agent Manager™ Installation Guide.

1.7.3 Managing Event Sources in the Sentinel Web Console

You no longer need to launch the Event Source Management in the Sentinel Control Center to manage event sources. Sentinel 7.2 allows you to manage the event sources in the Sentinel Web Console by using **Collection** > **Event Sources**. You can now perform the following tasks in the Event sources page:

- Start event sources
- Stop event sources
- Delete event sources
- Configure No Data alerts for event sources
- Configure the time zone of event sources
- Configure raw data storage for event sources

For more information, see "Viewing the Event Sources Page" in the *NetIQ Sentinel Administration Guide*.

1.7.4 Managing Delayed Events Storage

Sentinel 7.2 includes several fixes, which help you to monitor and manage the storage for delayed events. You can now set the limit for acceptable delay between the event time and Sentinel processing time by using the `esecurity.router.event.delayacceptthreshold` property. The event router drops the events if the event time delay exceeds the specified limit. Sentinel also allows you to report the event sources sending the delayed events within the specified delay limit by using the `sentinel.indexedlog.eventdelay.reportthreshold` property. You can modify these properties in the `configuration.properties` file.

1.7.5 Latest Advisor Feeds

Sentinel 7.2 includes the latest Advisor feeds that contain information about the latest known security vulnerabilities and threats. For more information about Advisor feeds, see the " Understanding Advisor" in the *NetIQ Sentinel Administration Guide*.

1.7.6 Inclusion of iotop in the Appliance

The Sentinel appliance now includes the iotop package that helps you to monitor the input and output usage by the processes in the system and make adjustments accordingly.

1.7.7 Regular Expression Queries

Sentinel 7.2 includes the regular expression queries that allow you to search events that match a pattern. For example, you can search for an initiator user name that ends with a certain character. You can also include special characters in your query by preceding them with the backslash (\) character. For more information about regular expression queries, see "Regular Expression Queries"in *NetIQ Sentinel Administration Guide*.

1.7.8 Google Chrome Support

Sentinel 7.2 includes support for the Google Chrome Web browser.

1.7.9 Session Type Event Field

Sentinel 7.2 includes the `SessionType` event field that provides information about the logon attempts to Windows computers. This helps you to monitor all attempts to access the computer. The Sentinel tag for the SessionType field is rv143.

1.8 Software Fixes

Sentinel 7.2 provides software fixes for the following issues:

1.8.1 Correlation Engine Runs Out of Memory When it Receives Large Volumes of Events

Issue: When the Correlation Engine receives large volumes of events, it runs out of memory. (BUG 847345)

Fix: The Correlation Engine no longer runs out of memory when it receives large volumes of events.

1.8.2 Cross-Site Scripting (XSS) Vulnerability

Issue: A user might append a string to the Sentinel help page link to access the session key information, which could allow XSS attacks. (BUG 845194)

Fix: Whenever there is a change made to the Sentinel Help page link, Sentinel reverts it back to the correct help page link.

1.8.3 Active Views with a Long Filter Criteria Do Not Display events

Issue: If the filter criteria to view events in Active Views is too long, the Active View might not display events. (BUG 822251)

Fix: Active View now displays events appropriately regardless of the length of the filter criteria.

1.8.4 Distributed Search Fails if the Search Target is Sentinel in High Availability

Issue: Distributed search fails if the target Sentinel server in high availability mode fails over to another high availability cluster node than the one that was running Sentinel when it was added as a target. (BUG 816719)

Fix: Distributed search no longer fails if the target Sentinel server is in high availability mode.

1.8.5 Correlation Rules are Auto-Deployed After the Sentinel Upgrade

Issue: When you upgrade Sentinel, correlation rules are auto deployed, which causes the Sentinel service to slow down or stop. (BUG 840964)

Fix: Sentinel no longer auto-deploys correlation rules after the upgrade.

1.8.6 Sentinel becomes Unresponsive While Generating Large Reports

Issue: When you generate reports that include large volume of events (approximately 20 million events), Sentinel becomes unresponsive and displays an error. (BUG 864705)

Fix: Sentinel now generates reports that include large volume of events.

1.8.7 Remote Collector Managers Might Drop Events When Sentinel Restarts

Issue: When the Sentinel server restarts, remote collector managers cache the events until the Sentinel server restarts completely. Remote collector managers might drop some events during the Sentinel shutdown and restart process. (BUG 848516)

Fix: Sentinel now notifies the remote collector managers before initiating the shutdown and restart process. Sentinel delays the shutdown process until all the events received prior to the notification are processed. Remote Collector Managers no longer drop events when Sentinel restarts.

1.8.8 Sentinel Agent Manger Creates Duplicate Installation Directories When Agents Migrated from Security Manager are Upgraded

Issue: If you have migrated Agents (installed on a non-default share) from Security Manager to Sentinel Agent Manager and if you upgrade these migrated Agents, Sentinel Agent Manager creates duplicate installation directories in Agent machines and results in Agent failure. (BUG 851275)

Fix: Sentinel Agent Manager no longer creates duplicate directories for migrated Agents and migrated Agents work properly.

1.8.9 The Sentinel Agent Manager Migration Tool Does Not Populate Orphaned Agents

Issue: The Sentinel Agent Manager Migration tool does not populate orphaned Agents under the **Windows Agent** tab. (BUG 843217)

Fix: The Sentinel Agent Manager Migration tool now populates orphaned Agents under the Windows Agent tab.

1.8.10 Installing Sentinel Agent Manager with the Re-purpose Option Fails

Issue: When installing Sentinel Agent Manager with the re-purpose option, the installation does not proceed and results in an error.(BUG 854969)

Fix: You can now successfully install Sentinel Agent Manager with the re-purpose option.

1.8.11 Cannot Set Background and Text Colors to Events

Issue: You cannot set background and text colors based on filter criteria to events in Sentinel Control Center. (BUG 842620)

Fix: Sentinel now provides Color Filter configuration that enables you to set background and text colors to events in the Sentinel Control Center based on filter criteria.

1.8.12 When a Search Fails because of Many Open Files, the Error Message Does Not Provide the Relevant Information

Issue: When an event search fails because of many open files, the error message does not provide relevant information about the cause of the event search failure. (BUG 861152)

Fix: The event search error message now provides relevant information about the cause of the event search failure.

1.8.13 Sentinel Generates Duplicate Correlated Events from a Single Trigger Event from Remote Systems

Issue: Sentinel generates duplicate correlation events from a single trigger event received from the remote systems. (BUG 854563)

Fix: Sentinel no longer generates duplicate correlated events from a single trigger event received from the remote systems.

1.8.14 Sentinel Does Not Export the Event IDs While Exporting the Search Results

Issue: When you export search results, Sentinel does not export the Event IDs. (BUG 849099)

Fix: Sentinel now exports Event IDs when exporting the search results.

1.8.15 Security Intelligence Dashboard Does Not Launch After Restoring the Backup

Issue: When you back up the Sentinel data by using the -i option, the backup script does not include the authentication details for the appuser and dbuser in the security intelligence database. Therefore, when you restore the backup data, the Sentinel fails to authenticate with the security intelligence database and displays an error. (BUG 853713)

Fix: Sentinel now overwrites the records related to authentication details when you restore the backup. Therefore, security intelligence dashboard now launches successfully.

1.8.16 Log In to Sentinel Fails if the User Name Has Duplicate Entries in the Database

Issue: If a user name has duplicate entries in the database (Users Table), the **Users** tab in the Sentinel Web Console displays an error. The user name with the duplicate entries is not able to log in to the Sentinel Web Console. (BUG 799946)

Fix: While creating a new user, Sentinel now examines whether the user name already exists in the database and does not create duplicate entries. For the existing duplicate users, you must manually delete the entries from the Users table in the database. For information about deleting the existing duplicate users in the database, contact NetIQ Technical Support.

1.8.17 If the Appuser Password is More Than 47 Characters, Sentinel Web Console Does Not Launch

Issue: If the appuser password is more than 47 characters, the Sentinel Web Console does not launch and displays the error HTTP ERROR: 503.(BUG 817663)

Fix: Sentinel Web Console now launches successfully with the appuser password of more than 47 characters.

1.8.18 The ModifyEventSourceServer Audit Event Does Not Provide Relevant Information

Issue: The ModifyEventSourceServer audit event is generated every five minutes and does not provide relevant information about the modification to the Event Source Server. (BUG 827633)

Fix: The ModifyEventSourceServer audit event now provides relevant information about the modifications to the Event Source server. You can configure the time interval for generating the ModifyEventSourceServer audit event in the **Queue Management** tab. For more information about configuring time interval in the **Queue Management** tab, see the "Managing the Queue" section in the Connector for Agent Manager guide in the Sentinel Plug-ins Web site.

1.8.19 The iTRAC Database Table Does Not Display Entries After Sentinel Upgrade

Issue: After you upgrade Sentinel, the iTRAC database tables (usertable and usergrouptable) do not display any entries. This might result in loss of user information in Sentinel. (BUG 841604)

Fix: The iTRAC database tables now displays entries after you upgrade Sentinel.

1.8.20 Remote Code Execution Vulnerability

Issue: An attacker might execute an arbitrary code in the system installed with Agent Manager using a vulnerable method, which can result in directory traversal. This vulnerability requires user interaction. (BUG 878834)

Fix: The Agent Manager no longer uses the vulnerable method. Therefore, Agent Manager is no longer vulnerable to remote code execution.

1.8.21 Cannot Back Up the Sentinel Server if Sentinel was Installed on a Custom Port

Issue: When you perform a full server backup on Sentinel installations that use a custom port, the backup operation fails. (BUG 844062)

Fix: You can now perform a full back up and restore on Sentinel servers that use a custom port.

1.8.22 Cannot Import an Older Version of Sentinel Plug-In

Issue: When you try to install an older version of a plug-in by placing the older plug-in in the `/var/opt/novell/sentinel/data/updates/pending` directory, Sentinel does not import the old plug-in. By default, Sentinel only imports a plug-in if the pending directory contains a newer version of the plug-in than the one currently installed. (BUG 853506)

Fix: For the very rare case where you must install an older plug-in as part of a testing scenario, Sentinel can now support this option by using a customizable configuration parameter. To import an old plug-in, set the following property in the `configuration.properties` file to true and then restart the Sentinel server:

```
plugins.import.oldplugin = true
```

[Return to Top]

1.8.23 MongoDB Does Not Start if There Are Duplicate Users in the Database

Issue: MongoDB does not start if there are duplicate user names in the database. This issue might occur if you had done a full backup and restore of security intelligence data any time on your Sentinel server, before upgrading to Sentinel 7.1.1 and later. (BUG 856174)

Fix: When you upgrade Sentinel, the installer first checks for duplicate users and then proceeds with the upgrade.

2 System Requirements

You can upgrade to Sentinel 7.2 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 Installing Sentinel 7.2

For information about installing Sentinel 7.2, see the *NetIQ Sentinel Installation and Configuration Guide*.

[Return to Top]

4 Upgrading to Sentinel 7.2

Download the Sentinel installer from the NetIQ Download Web site. For information about upgrading to Sentinel 7.2, 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]

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.

For the list of known issues in the supported SLES 11 Service Pack, see the SUSE Release Notes.

For the list of known issues in previous releases, see the Sentinel 7.1 Documentation Web site.

5.1 Connection Problems between Clients and Sentinel Running in FIPS Mode

Issue: Sentinel 7.2 includes Oracle Java 1.7 update 51, 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.

5.2 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**.

5.3 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.

5.4 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: Append the default port number to the URL when accessing Sentinel baselining in the following instances:

- Sentinel has been configured to listen on the default port, 443.
- Sentinel is listening on a non-default port but port forwarding is enabled, which routes traffic from the default port to the port on which Sentinel is listening.

5.5 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 might take a few minutes.

5.6 Sentinel Web Console Might Not Launch After Enabling the FIPS Mode

Issue: If Sentinel is in FIPS mode, the Sentinel Web console does not launch in Internet Explorer (with TLS version set only to 1.2) and logs an exception in the server logs. In Chrome, the Sentinel Web console launches but logs an exception. (BUG 867675)

Workaround: To launch Sentinel Web Console in FIPS mode in Internet Explorer:

1. Downgrade the Java version on the Sentinel server to Java 7 update 45

   For more information, see the instructions in TID 7014980 in the NetIQ Support Knowledge Base.
2. In the Internet Explorer, click **Tools** > **Internet Options**.
3. In **Internet Options**, click the **Advanced** tab.
4. In the security section, select either **Use TLS 1.0** or **Use TLS 1.1**.

NOTE: Changing the value of the TLS to 1.0 or 1.1 might decrease your security level.

5.7 Sentinel Control Center Takes a Long Time to Launch After the Java Upgrade

Issue: If you work in a managed network or do not have access to the Internet and if you upgrade to Java 7 update 25, Sentinel Control Center (SCC) takes a long time to launch because of the changes in the certificate revocation process in Java. Since there is no access to the revocation services of the Certificate Authorities (CA). There is a delay in the launch of SCC. For more information about this issue, see TID 7014806 in the NetIQ Support Knowledge Base. (BUG 828340)

Workaround: To avoid the delay in the launching of SCC, in the **Control Panel** > **Java Control Panel** > **Advanced**, in the **Perform certificate checks on** section, select **Do not check**.

NOTE: Disabling certificate revocation checking might decrease your security level.

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

Issue: The message queuing service (mqsvc.exe) utilizes a large 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.

5.9 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.

5.10 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 that this time.

5.11 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*.

5.12 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.

5.13 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.

5.14 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
```

5.15 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.

5.16 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.

5.17 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.

5.18 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.

5.19 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.

5.20 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.

5.21 Sentinel High Availability Installation Does Not Check for the Required NSS Packages

Issue: When you perform a silent installation of Sentinel in High Availability mode and when FIPS mode is enabled, the installer does not check for the required NSS packages. (BUG 815941)

Workaround: Ensure that the required NSS packages are available on the system before you start the installation.

5.22 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.

5.23 Appliance Update Fails in WebYaST

Issue: WebYaST is unable to update the appliance 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 Sentinel Appliance Versions 7.0.1 or Earlier in the *NetIQ Sentinel Installation and Configuration Guide*.

5.24 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.

5.25 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.

5.26 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.

5.27 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.

5.28 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]

5.29 Sentinel Control Center does Not Launch if the Client Computer has Java 7 Update 51 Installed

Issue: If you have Java 7 update 51 installed on the client computer, Sentinel Control Center does not launch. (BUG 862771)

Workaround: Upgrade to Sentinel 7.1.1.2 or add the Sentinel Web Console URL to the Java security Exception site list. To upgrade to Sentinel 7.1.1.2, see Sentinel 7.1.1.2 readme.

To edit the Java security Exception site list:

1. In **Control Panel** > **Java** > **Security**, click **Edit Site List**.
2. In the **Exception Site List** window, click **Add** and specify the Sentinel Web Console URL in the exception list field.
3. Click **OK**.

5.30 Unable to Delete Renamed Dashboards After Upgrading the Xen Appliance

Issue: After you upgrade the Xen appliance to Sentinel 7.1, if you rename a dashboard and then delete the renamed dashboard, Sentinel displays an error. However, Sentinel deletes the dashboard successfully. (BUG 816542)

Workaround: There is no workaround at the time of this release.

5.31 The Help Menu Displays the HTTP 404 Error

Issue: The **Help** menu in Event Source Management and the Sentinel Web console displays the `HTTP 404 Error` and does not launch the Sentinel documentation Web site. `(BUG 814138)`

Workaround: To view the latest Sentinel documentation, see the Sentinel 7.1 Documentation Web site.

5.32 Solution Manager Does Not Install Correlation Rules with the Same Name

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.

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 Qmunity, our community Web site that offers product forums, product notifications, blogs, and product user groups.

[Return to Top]

7 Legal Notice

[Return to Top]