Sentinel 7.4 Service Pack 2 Release Notes

June 2016

Sentinel 7.4 SP2 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 website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click the comment icon on 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 website.

For the latest version of this release notes, see *Sentinel 7.4 Service Pack 2 Release Notes*.

- Section 1, “What’s New?,” on page 1
- Section 2, “System Requirements,” on page 6
- Section 3, “Upgrading to Sentinel 7.4 SP2,” on page 6
- Section 4, “Known Issues,” on page 7
- Section 5, “Contact Information,” on page 19
- Section 6, “Legal Notice,” on page 19

1 What’s New?

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

- Section 1.1, “Java Upgrade,” on page 1
- Section 1.2, “Security Vulnerability Fix,” on page 1
- Section 1.3, “Enhancements,” on page 2
- Section 1.4, “Software Fixes,” on page 3

1.1 Java Upgrade

Sentinel 7.4 SP2 includes Java 8 update 77, which includes fixes for several security vulnerabilities and also improves Sentinel performance.

1.2 Security Vulnerability Fix

Sentinel 7.4 SP2 resolves the Authentication Bypass and Arbitrary File Upload (CVE-2016-1605) security vulnerability. This vulnerability (ZDI-CAN-3717) was discovered by rgod working with Trend Micro’s Zero Day Initiative.

1.3 Enhancements

- Section 1.3.1, “Addition of Fields to Sentinel Event Schema,” on page 2
- Section 1.3.2, “Visualization Enhancements in Event View Charts,” on page 2
- Section 1.3.3, “Ability to Clone Event Views,” on page 2
- Section 1.3.4, “Usability Improvements in the Sentinel Navigation Panel,” on page 2
- Section 1.3.5, “Enhancement to Collector Manager and Correlation Engine Installation Permissions,” on page 3

1.3.1 Addition of Fields to Sentinel Event Schema

The Sentinel event schema now includes the following two event fields:

- SourceInterface
- TargetInterface

These fields are used for interface names that are usually a part of the events generated by event sources such as network devices. Firewalls, switches, and routers are among the few types of event sources that have the interface names in the events generated by them.

You can now perform operations using the information in these fields. For example, you can apply correlation rules based on the values of these fields. (Bug 974187)

1.3.2 Visualization Enhancements in Event View Charts

Sometimes, the size of stacks in stacked charts in event views are too small and it might be difficult to visualize the information. Sentinel now displays a secondary chart when you click on any of the stacks in stacked charts. The secondary chart renders a pie chart for the selected time slot and helps in better visualization of events. (Bug 948046)

1.3.3 Ability to Clone Event Views

You can now clone an existing event view. You can also edit all the event view configuration fields in the cloned event view and save it. (Bug 948036)

1.3.4 Usability Improvements in the Sentinel Navigation Panel

Sentinel 7.4 SP2 includes the following usability improvements in the navigation panel:

- All the categories in the **Reports and Searches** panel are now collapsed by default. This helps you avoid scrolling through long lists in all the categories, and you can expand only the category you want to work with. (Bug 949072)
- There are now **Expand All** and **Collapse All** buttons under the **Reports and Searches** panel. You can easily navigate through and manage large lists of reports and their category groupings using these buttons. (Bug 949142)

1.3.5 Enhancement to Collector Manager and Correlation Engine Installation Permissions

Any user in the Administrator role can now install Collector Manager and Correlation Engine.

Previously, only the `admin` user had permissions to install Collector Manager and Correlation Engine. It means that the person installing Collector Manager and Correlation Engine had to be given access to the `admin` user credentials, and this could lead to nonobservance of security practices of the organization. Now you can use the credentials of any user in the Administrator role to install Collector Manager and Correlation Engine. `(Bug 952168)`

1.4 Software Fixes

Sentinel 7.4 SP2 includes software fixes that resolve several issues.

For the list of software fixes and enhancements in previous releases, see the specific release notes.

- Section 1.4.1, “Cannot Manage Some Alerts in the Alerts Dashboard,” on page 3
- Section 1.4.2, “Sentinel Writes a Warning Message in Logs Repeatedly,” on page 4
- Section 1.4.3, “Report Generation Fails If the Remote Sentinel Server Events Contain Special Characters,” on page 4
- Section 1.4.4, “Firewall Turns ON After Running the report_dev_setup.sh Script,” on page 4
- Section 1.4.5, “Warning Displayed in the Sentinel Web Interface When You Add a Sentinel Log Manager Server as Data Source,” on page 4
- Section 1.4.6, “Non-Administrator Users with the Right Permissions Cannot Assign Alerts,” on page 4
- Section 1.4.7, “Event Fields Copied from the Trigger Event Overwrite Customized Event Fields,” on page 4
- Section 1.4.8, “Sentinel Web Interface Stops When You Select Event Sources for Event Criteria,” on page 5
- Section 1.4.9, “Administrator User Cannot Edit User Event Views,” on page 5
- Section 1.4.10, “Collector Manager Generates Unnecessary Keystores When You Import the Root Certificate,” on page 5
- Section 1.4.11, “The simple_event_restore Option in the backup_util.sh Script does not Restore Data,” on page 5
- Section 1.4.12, “Sentinel Link Event Sources Do Not Communicate with Sentinel Intermittently,” on page 5
- Section 1.4.13, “Real-Time Views Do Not Display Any Data for Tenants That Have the Underscore Character in Their Names,” on page 5
- Section 1.4.14, “Cannot Use Sorting in Incident View Manager in Sentinel Control Center,” on page 5
- Section 1.4.15, “Reports are Empty When the Last Day of the Time Range Does Not Contain Events Searched For By That Report,” on page 6
- Section 1.4.16, “Cannot Start Sentinel Control Center,” on page 6

1.4.1 Cannot Manage Some Alerts in the Alerts Dashboard

Issue: You cannot close, assign, or edit some alerts in the Alerts Dashboard, and hence Sentinel displays them continuously. This is a sporadic issue. `(Bug 932378)`

Fix: You can now manage such alerts.

1.4.2 Sentinel Writes a Warning Message in Logs Repeatedly

Issue: Sentinel writes the following warning message in log files every three minutes:

```
<timestamp> | INFO | jvm 1 | XML configuration warning in file:/etc/opt/novell/
sentinel/sm-bridge/attributeValuesEtl.xml(38:7): The content of element type "etl"
must match "(description?,properties?,connection*,(script*,query*)*)"
```

However, there is no impact on Sentinel functionality and performance because of this message. (Bug 963803)

Fix: Sentinel no longer writes the warning message to the logs.

1.4.3 Report Generation Fails If the Remote Sentinel Server Events Contain Special Characters

Issue: In distributed reporting, report generation fails if events from remote Sentinel servers contain special characters. (Bug 974900)

Fix: Sentinel now encodes remote Sentinel server events that contain special characters.

1.4.4 Firewall Turns ON After Running the report_dev_setup.sh Script

Issue: The firewall turns ON when you run the `report_dev_setup.sh` script. This might cause errors in communication through some Sentinel ports. (Bug 820239)

Fix: Sentinel now retains the status of the firewall after running the `report_dev_setup.sh` script.

1.4.5 Warning Displayed in the Sentinel Web Interface When You Add a Sentinel Log Manager Server as Data Source

Issue: The Sentinel Web interface displays the following warning when you add a Sentinel Log Manager server as a data source for data federation:

```
Target <IP address> does not support Operation EPS
```

However, there is no impact because of this warning. The Sentinel Log Manager server gets added as a data source successfully. (Bug 961319)

Fix: Sentinel no longer displays this warning when you add a Sentinel Log Manager server as a data source.

1.4.6 Non-Administrator Users with the Right Permissions Cannot Assign Alerts

Issue: Sentinel displays an error when non-administrator users with the **Allow users to manage alerts** permission try to assign alerts. (Bug 971694)

Fix: Users with the **Allow users to manage alerts** permission can now assign alerts.

1.4.7 Event Fields Copied from the Trigger Event Overwrite Customized Event Fields

Issue: Event fields copied from the trigger event always overwrite customized event fields even when they are removed from the correlation rule configuration. (Bug 969898)

Fix: Sentinel now copies the event fields correctly, as per the selection.

1.4.8 Sentinel Web Interface Stops When You Select Event Sources for Event Criteria

Issue: The Sentinel Web interface stops and does not respond when there are more than 500 event sources, and you try selecting event sources for event criteria. (Bug 966320)

Fix: The Sentinel Web interface now responds correctly even when there are a large number of event sources.

1.4.9 Administrator User Cannot Edit User Event Views

Issue: The Administrator user cannot edit or delete event views of other users. (Bug 949148)

Fix: The Administrator user now has privileges to edit or delete event views of other users.

1.4.10 Collector Manager Generates Unnecessary Keystores When You Import the Root Certificate

Issue: Collector Manager generates some additional, unnecessary keystores when you run the `ssl_certs.sh` script to import the root certificate. (Bug 974491)

Fix: Collector Manager now creates only the required keystores when you import the root certificate.

1.4.11 The simple_event_restore Option in the backup_util.sh Script does not Restore Data

Issue: The `simple_event_restore` option in the `backup_util.sh` script does not restore event data and raw data. (Bug 891920)

Fix: The `simple_event_restore` option in the `backup_util.sh` script now restores all the data.

1.4.12 Sentinel Link Event Sources Do Not Communicate with Sentinel Intermittently

Issue: Sentinel Link event sources sometimes stop sending events to Sentinel because of a memory dump issue in the Collector Manager. (Bug 949047)

Fix: Sentinel 7.4 SP2 optimizes memory utilization and the memory dump issue no longer occurs.

1.4.13 Real-Time Views Do Not Display Any Data for Tenants That Have the Underscore Character in Their Names

Issue: Real-time views such as event views or NetFlow views do not display any data for tenants that contain underscore characters in their names. Sentinel replaces the underscore character in tenant names with a space, and hence those tenant names are not recognized. (Bug 977641)

Fix: Sentinel no longer replaces the underscore character in tenant names with a space. So, real-time views display data correctly for tenants that contain underscore characters in their names.

1.4.14 Cannot Use Sorting in Incident View Manager in Sentinel Control Center

Issue: In Sentinel Control Center, the Incidents View window stops responding and Sentinel displays an error if you have used more than one level of sorting while creating or editing the incident view in Incident View Manager. (Bug 974940)

Fix: The Incidents View window now displays correctly even if you have used the sorting feature while creating or editing the incident view in Incident View Manager.

1.4.15 Reports are Empty When the Last Day of the Time Range Does Not Contain Events Searched For By That Report

Issue: If you have specified a time range for a report and no events are generated on the last day of that time range, Sentinel displays an empty report. Events generated on other days of the time range are not displayed in the report. (Bug 976446)

Fix: Sentinel now displays reports correctly for all time ranges.

1.4.16 Cannot Start Sentinel Control Center

Issue: Sentinel Control Center does not start and displays the following error:

```
Application Blocked by Java security
```

This issue occurs because the certificate used to sign Sentinel Control Center jars is expired. (Bug 983294)

Fix: Sentinel Control Center jars are now signed with the renewed certificate.

2 System Requirements

For information about hardware requirements, supported operating systems, and browsers, see the Technical Information for Sentinel page.

3 Upgrading to Sentinel 7.4 SP2

You can upgrade to Sentinel 7.4 SP2 from Sentinel 7.2 or later.

NOTE: If you are upgrading the Sentinel appliance from Sentinel 7.1 SP2 or an earlier version, you must first upgrade to version 7.4, and then to version 7.4 SP2. Please contact Technical Support to obtain the Sentinel 7.4 appliance updates.

Sentinel 7.4 and later versions are compatible with Change Guardian 4.2 and later. If you have a Change Guardian server sending events to Sentinel, before you upgrade Sentinel, you must first upgrade the Change Guardian Server, agents, and the Policy Editor to version 4.2 to ensure that Sentinel continues to receive events from Change Guardian after the upgrade.

Download the Sentinel installer from the NetIQ Download website. For information about upgrading to Sentinel 7.4 SP2, see “Upgrading Sentinel” in the *NetIQ Sentinel Installation and Configuration Guide*.

- Section 3.1, “Upgrading the Sentinel Appliance,” on page 7
- Section 3.2, “Post-Upgrade Configuration,” on page 7

3.1 Upgrading the Sentinel Appliance

You can upgrade the appliance using WebYaST only on Sentinel 7.3 SP2 or later and if you manually upgraded the NetIQ Change Guardian RPM as mentioned in "Upgrading NetIQ Change Guardian RPM" in the *Sentinel 7.3.2 Release Notes*.

To upgrade the appliance from versions prior to Sentinel 7.3 SP2, use the zypper command line utility because user interaction is required to complete the upgrade. WebYaST is not capable of facilitating the required user interaction. For more information about upgrading the appliance using zypper, see "Upgrading the Appliance by Using zypper" in the *NetIQ Sentinel Installation and Configuration Guide*.

(Bug 956278)

3.2 Post-Upgrade Configuration

If you are upgrading from Sentinel 7.2 SP2 or an older version, perform the following:

- Assign the **Allow users to manage alerts** permission to the Search Proxy User role manually, because the upgrade clears this permission. This permission is necessary for the role to perform remote alert search.

  For more information, see "Configuring Roles and Users" in the *NetIQ Sentinel Administration Guide*.
- For consistency with newer versions of Sentinel and Sentinel documentation, rename the Search Proxy User role to Data Proxy User after the upgrade.

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.

The Java 8 update and the security vulnerability fixes included in Sentinel 7.3 SP1 and later might impact the following plug-ins:

- Cisco SDEE Connector
- SAP (XAL) Connector
- Remedy Integrator

For any issues with these plug-ins, NetIQ will prioritize and fix the issues according to standard defect-handling policies. For more information about support polices, see Support Policies.

- Section 4.1, "Cannot Receive Events from NetIQ eDirectory," on page 9
- Section 4.2, "Warning Displayed When Upgrading Sentinel Appliance to Version 7.4 SP1 and Later," on page 9
- Section 4.3, "Cannot Create Reports by Using Sentinel SDK," on page 9
- Section 4.4, "Synchronization Needs to be Started Manually in Sentinel High Availability When You Modify Configuration Files in the Active Node," on page 9
- Section 4.5, "Cannot Receive Events from Sentinel UNIX Agent 7.4 After Upgrading Sentinel to Version 7.3 SP1 and Later," on page 10
- Section 4.6, "Error When Configuring the NFS Storage After Upgrading Sentinel Appliance to Version 7.3 SP1 and Later," on page 11

- Section 4.7, “Exception in the Sentinel Server Log When You Upgrade Sentinel Versions Prior to 7.3 SP1 to Versions 7.3 SP1 and Later,” on page 11
- Section 4.8, “Cannot Receive Events from Secure Configuration Manager After Upgrading Sentinel to Version 7.3 SP1 and Later,” on page 11
- Section 4.9, “Cannot View Alerts with IPv6 Data in Alert Views,” on page 11
- Section 4.10, “Bar Mitzvah Security Vulnerability in Sentinel Link Connector,” on page 12
- Section 4.11, “The Agent Manager Connector Does Not Set the Connection Mode Property in Events If the Associated Collector Supports Multiple Connection Modes,” on page 12
- Section 4.12, “Sentinel Agent Manager Does Not Consider the RawDataTapFileSize Configuration,” on page 12
- Section 4.13, “Tips Table Search Does Not Return the Complete List of Alert Fields in Upgraded Sentinel Installations,” on page 12
- Section 4.14, “Data Synchronization Fails While Synchronizing IPv6 Addresses in Human Readable Format,” on page 12
- Section 4.15, “Event Search Does Not Respond if You Do Not Have Any Event Viewing Permissions,” on page 13
- Section 4.16, “The Event fields Panel is Missing in the Schedule Page When Editing Some Saved Searches,” on page 13
- Section 4.17, “Sentinel Does Not Return Any Correlated Events When You Search for Events for the Deployed Rule with the Default Fire Count Search,” on page 13
- Section 4.18, “New Incoming Alerts Incorrectly Appear to be Selected When You Modify Existing Alerts,” on page 13
- Section 4.19, “Loading Historical Security Intelligence Data Takes a Long Time,” on page 13
- Section 4.20, “Security Intelligence Dashboard Displays Invalid Baseline Duration When Regenerating a Baseline,” on page 14
- Section 4.21, “Sentinel Server Shuts Down When Running a Search If There Are Large Number of Events in a Single Partition,” on page 14
- Section 4.22, “Error While Using the report_dev_setup.sh Script to Configure Sentinel Ports for Firewall Exceptions on Upgraded Sentinel Appliance Installations,” on page 14
- Section 4.23, “Sentinel Generic Collector Performance Degrades When Generic Hostname Resolution Service Collector is Enabled,” on page 15
- Section 4.24, “Sentinel Cannot Access Security Intelligence, Netflow, and Alert Data in FIPS 140-2 Mode,” on page 15
- Section 4.25, “Security Intelligence Database and Alert Dashboard Occasionally Do Not Work in Upgraded Custom Installations of FIPS 140-2 Enabled Sentinel,” on page 15
- Section 4.26, “Sentinel Does Not Configure the Sentinel Appliance Network Interface By Default,” on page 16
- Section 4.27, “The Web Browser Displays an Error When Exporting Search Results in Sentinel,” on page 16
- Section 4.28, “Sentinel Services Might Not Start Automatically After the Installation,” on page 17
- Section 4.29, “Cannot Enable Kerberos Authentication in Sentinel Appliance Installations,” on page 17
- Section 4.30, “Unable to View More Than One Report Result at a Time,” on page 17
- Section 4.31, “Agent Manager Requires SQL Authentication When FIPS 140-2 Mode is Enabled,” on page 17

- Section 4.32, “Sentinel High Availability Installation in FIPS 140-2 Mode Displays an Error,” on page 17
- Section 4.33, “Sentinel High Availability Installation in Non-FIPS 140-2 Mode Displays an Error,” on page 18
- Section 4.34, “Appliance Update From Versions Prior to Sentinel 7.2 Fails in WebYaST,” on page 18
- Section 4.35, “Error While Installing Correlation Rules,” on page 18
- Section 4.36, “Sentinel Link Action Displays Incorrect Message,” on page 18
- Section 4.37, “Dashboard and Anomaly Definitions with Identical Names,” on page 18
- Section 4.38, “Active Search Jobs Duration and Accessed Columns Inaccuracies,” on page 19
- Section 4.39, “IssueSAMLToken Audit Event Displays Incorrect Information in the Security Intelligence Dashboard,” on page 19
- Section 4.40, “Sentinel Agent Manager Does Not Capture the Windows Insertion String Fields With Null Values,” on page 19

4.1 Cannot Receive Events from NetIQ eDirectory

Issue: NetIQ eDirectory Instrumentation cannot connect to Audit Connector through Platform Agent. Hence, Sentinel cannot receive events from eDirectory. This issue occurs because eDirectory Instrumentation uses MD5 RSA certificate algorithm, which has been deprecated in Java 8 update 77 that is used in Sentinel 7.4 SP2. `(Bug 985312)`

Workaround: To enable eDirectory Instrumentation to use a custom certificate, perform the steps mentioned in NetIQ Knowledgebase Article 7017764.

4.2 Warning Displayed When Upgrading Sentinel Appliance to Version 7.4 SP1 and Later

Issue: Sentinel displays the following warning when upgrading the appliance to version 7.4 SP1 and later:

```
Failed to set encrypted password

(Bug 967764)
```

Workaround: Ignore the warning. There is no impact to the upgrade.

4.3 Cannot Create Reports by Using Sentinel SDK

Issue: You cannot create reports by using Sentinel SDK. `(Bug 966406)`

Workaround: To create reports by using Sentinel SDK, perform the steps mentioned in NetIQ Knowledgebase Article 7017293.

4.4 Synchronization Needs to be Started Manually in Sentinel High Availability When You Modify Configuration Files in the Active Node

Issue: In Sentinel High Availability (HA), when you customize Sentinel by updating configuration files or by making changes in the Sentinel Web interface in the active node, the changes are not reflected in the passive node. Synchronization needs to be started manually.

For example, you must start synchronization manually in the following scenarios:

- When you change the communication protocol to SSL, by updating the `/etc/opt/novell/sentinel/config/databasePlatforms.xml` file for the following property:

  ```
  ssl=require
  ```

- When Sentinel is in FIPS mode, the synchronization to convert all the passive nodes to FIPS mode is not performed completely. When failover occurs in such scenario, the Sentinel Web interface does not launch.
- When you change the LDAP configuration in the active node, it is not synchronized to the passive nodes. Because of this, you will not be able to authenticate LDAP accounts in the passive nodes.

(Bug 956702 and Bug 954472)

Workaround: When you modify a configuration file, or when files are modified because of the changes you made in the Sentinel Web interface, add that file or directory for synchronization manually, by performing the following steps:

1. Log in as the `root` user on the active node.
2. Add the file or directory for synchronization, by adding the following line in the `/etc/csync2/csync2.cfg` file:

   ```
   include <file name or directory>;
   ```

   For example:

   - Add the following line if you have changed the communication protocol to SSL in the `/etc/opt/novell/sentinel/config/databasePlatforms.xml` file:

     ```
     include /etc/opt/novell/sentinel/config/databasePlatforms.xml;
     ```

   - Add the following line if you want to synchronize passive nodes to FIPS mode:

     ```
     include /etc/opt/novell/sentinel/config/nonfips_backup;
     ```

   - Add the following line if you have updated the LDAP configuration:

     ```
     include /etc/opt/novell/sentinel/config/auth.login;
     ```

3. Start the synchronization manually by running the following command:

   ```
   csync2 -x -v
   ```

   This will synchronize the updates onto all the passive nodes.

4.5 Cannot Receive Events from Sentinel UNIX Agent 7.4 After Upgrading Sentinel to Version 7.3 SP1 and Later

Issue: The security vulnerability fixes included in Sentinel 7.3 SP1 involved changes to the communication mechanism for a secured connection. These changes are not compatible with Sentinel UNIX Agent 7.4. Therefore, Sentinel cannot receive events from Sentinel UNIX Agent 7.4. (Bug 953990)

Workaround: There is no workaround at this time. This issue will be resolved when a compatible version of Sentinel UNIX Agent is made available.

4.6 Error When Configuring the NFS Storage After Upgrading Sentinel Appliance to Version 7.3 SP1 and Later

Issue: Sentinel displays an error when you try to configure NFS as secondary storage location after you Sentinel appliance to version 7.3 SP1 and later. (Bug 934851)

Workaround: After upgrading the Sentinel appliance, restart the SLES operating system using the following command:

```
init 6
```

4.7 Exception in the Sentinel Server Log When You Upgrade Sentinel Versions Prior to 7.3 SP1 to Versions 7.3 SP1 and Later

Issue: When you upgrade Sentinel from version 7.3 to version 7.3 SP1 and start the Sentinel server, you might see the following exception in the server log:

```
Invalid length of data object ......
```

(Bug 933640)

Workaround: Ignore the exception. There is no impact to Sentinel performance because of this exception.

4.8 Cannot Receive Events from Secure Configuration Manager After Upgrading Sentinel to Version 7.3 SP1 and Later

Issue: Sentinel uses the Diffie-Hellman protocol to communicate with Secure Configuration Manager. As part of fixing the Logjam vulnerability, the certificate key size for the Diffie-Hellman protocol in Sentinel has been increased to 2048. However, Secure Configuration Manager uses the default certificate key size; that is, 1024. Because of this mismatch, Secure Configuration Manager can no longer communicate with Sentinel. (Bug 935987)

Workaround: Upgrade Secure Configuration Manager to version 6.1. For more information, see the *NetIQ Secure Configuration Manager 6.1 Release Notes*.

Or

Perform the following steps:

WARNING: Performing this workaround overrides the fix for the Logjam vulnerability specified in "Security Vulnerability Fixes" in the *Sentinel 7.3.1 Release Notes*.

---

1. Log in as the `novell` user and open the `/etc/opt/novell/sentinel/config/configuration.properties` file.
2. Comment out the following line following line by prefixing `#`:

   ```
   jdk.tls.ephemeralDHKeySize=2048
   ```
3. Restart Sentinel.

4.9 Cannot View Alerts with IPv6 Data in Alert Views

Issue: Sentinel alert views and alert dashboards do not display alerts that have IPv6 addresses in IP address fields. (Bug 924874)

Workaround: To view alerts with IPv6 addresses in Sentinel, perform the steps mentioned in NetIQ Knowledgebase Article 7016555.

4.10 Bar Mitzvah Security Vulnerability in Sentinel Link Connector

Issue: The Bar Mitzvah security vulnerability exists in Sentinel Link Connector. Sentinel Link Connector uses the RC4 algorithm in SSL and TSL protocols, which might allow plaintext recovery attacks against the initial bytes of a stream. For more information, see CVE-2015-2808. (Bug 933741)

Workaround: The Sentinel Link Connector version 2011.1r4 resolves this issue. Until it is officially released on the Sentinel Plug-ins website, you can download the Connector from the Previews section.

4.11 The Agent Manager Connector Does Not Set the Connection Mode Property in Events If the Associated Collector Supports Multiple Connection Modes

Issue: The Agent Manager Connector version 2011.1r3 does not set the CONNECTION_MODE property in the events if the Collector parsing the events supports multiple connection modes. (Bug 880564)

Workaround: The Agent Manager Connector version 2011.1r5 and later resolve this issue. Until it is officially released on the Sentinel Plug-ins website, you can download the Connector from the Previews section.

4.12 Sentinel Agent Manager Does Not Consider the RawDataTapFileSize Configuration

Issue: Sentinel Agent Manager ignores the value specified in `RawDataTapFileSize` attribute in the `SMServiceHost.exe.config` file for the raw data file size configuration, and stops writing to the raw data file when the file size reaches 10 MB. (Bug 867954)

Workaround: Manually copy the content of the raw data file into another file and clear it when the file size reaches 10 MB, so that Sentinel Agent Manager can write new data into it.

4.13 Tips Table Search Does Not Return the Complete List of Alert Fields in Upgraded Sentinel Installations

Issue: In upgraded installations of Sentinel, when you search for alert attributes in the Tips table in the Web interface, the search does not return the complete list of alert fields. However, alert fields display correctly in the Tips table if you clear the search. (Bug 914755)

Workaround: There is no workaround at this time.

4.14 Data Synchronization Fails While Synchronizing IPv6 Addresses in Human Readable Format

Issue: Data synchronization fails when you try to synchronize IPv6 address fields in a human readable format to external databases. For information about configuring Sentinel to populate the IP address fields in human readable dot notation format, see "Creating a Data Synchronization Policy" in the *NetIQ Sentinel Administration Guide*. (Bug 913014)

Workaround: To fix this issue, manually change the maximum size of the IP address fields to at least 46 characters in the target database, and re-synchronize the database.

4.15 Event Search Does Not Respond if You Do Not Have Any Event Viewing Permissions

Issue: If run an event search when your role's security filter is blank and your role does not have event viewing permissions, the search does not complete. The search does not display any error message about the invalid event viewing permissions. (Bug 908666)

Workaround: Update the role with one of the following options:

1. Specify a criteria in the **Only events matching the criteria** field. If users in the role should not see any events, you can enter **NOT sev:[0 TO 5]**.
2. Select **View system events**.
3. Select **View all event data (including raw data and NetFlow data)**.

4.16 The Event fields Panel is Missing in the Schedule Page When Editing Some Saved Searches

Issue: When editing a saved search upgraded from Sentinel 7.2 to a later version, the **Event fields** panel, used to specify output fields in the search report CSV, is missing in the schedule page. (Bug 900293)

Workaround: After upgrading Sentinel, recreate and reschedule the search to view the **Event fields** panel in the schedule page.

4.17 Sentinel Does Not Return Any Correlated Events When You Search for Events for the Deployed Rule with the Default Fire Count Search

Issue: Sentinel does not return any correlated events when you search for all correlated events that were generated after the rule was deployed or enabled, by clicking the icon next to **Fire count** in the **Activity statistics** panel in the Correlation Summary page for the rule. (Bug 912820)

Workaround: Change the value in the **From** field in the Event Search page to a time earlier than the populated time in the field and click **Search** again.

4.18 New Incoming Alerts Incorrectly Appear to be Selected When You Modify Existing Alerts

Issue: When you click **Select All** in alerts views to select alerts, deselect few alerts, and modify them, new incoming alerts are also selected in the refreshed alert views. This results in wrong count of alerts selected for modification, and also it appears as if you are modifying new incoming alerts too. However, only the originally selected alerts are modified. (Bug 904830)

Workaround: No new alerts will appear in the alert view if you create the alert view with a custom time range.

4.19 Loading Historical Security Intelligence Data Takes a Long Time

Issue: Historical Security Intelligence (SI) data takes a long time to load in Sentinel systems that have a high Events Per Second (EPS) load. (Bug 908599)

Workaround: If you are creating a security intelligence dashboard with historical data, plan to deploy the dashboard when the load on your system is lower, if possible. There is no other workaround at this time.

4.20 Security Intelligence Dashboard Displays Invalid Baseline Duration When Regenerating a Baseline

Issue: During Security Intelligence baseline regeneration, the start and finish dates for the baseline are incorrect and display 1/1/1970. (Bug 912009)

Workaround: The correct dates are updated after the baseline regeneration is complete.

4.21 Sentinel Server Shuts Down When Running a Search If There Are Large Number of Events in a Single Partition

Issue: Sentinel server shuts down when you run a search if there are a large number of events indexed in a single partition. (Bug 913599)

Workaround: Create retention policies in such a way that there are at least two partitions open in a day. Having more than one partition open helps reduce the number of events indexed in partitions.

You can create retention policies that filter events based on the `estzhour` field, which tracks the hour of the day. Therefore, you can create one retention policy with `estzhour:[0 TO 11]` as the filter and another retention policy with `estzhour:[12 TO 23]` as the filter.

For more information, see "Configuring Data Retention Policies" in the *NetIQ Sentinel Administration Guide*.

4.22 Error While Using the report_dev_setup.sh Script to Configure Sentinel Ports for Firewall Exceptions on Upgraded Sentinel Appliance Installations

Issue: Sentinel displays an error when you use the `report_dev_setup.sh` script to configure Sentinel ports for firewall exceptions. (Bug 914874)

Workaround: Configure Sentinel ports for firewall exceptions through the following steps:

1. Open the `/etc/sysconfig/SuSEfirewall2` file.
2. Change the following line:

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590"
   ```

   to

   ```
   FW_SERVICES_EXT_TCP=" 443 8443 4984 22 61616 10013 289 1289 1468 1443
   40000:41000 1290 1099 2000 1024 1590 5432"
   ```
3. Restart Sentinel.

4.23 Sentinel Generic Collector Performance Degrades When Generic Hostname Resolution Service Collector is Enabled

Issue: Sentinel Generic Collector performance degrades when Generic Hostname Resolution Service Collector is enabled on Microsoft Active Directory and Windows Collector. EPS decreases by 50% when remote Collector Managers send events. (Bug 906715)

Workaround: There is no workaround at this time.

4.24 Sentinel Cannot Access Security Intelligence, Netflow, and Alert Data in FIPS 140-2 Mode

Issue: When you install Sentinel in FIPS 140-2 mode, connector to Security Intelligence database fails to start, and Sentinel cannot access Security Intelligence, Netflow, and alert data. (Bug 915241)

Workaround: Restart Sentinel after installing and configuring in FIPS 140-2 mode.

4.25 Security Intelligence Database and Alert Dashboard Occasionally Do Not Work in Upgraded Custom Installations of FIPS 140-2 Enabled Sentinel

Issue: When you upgrade Sentinel from a custom installation of Sentinel that was installed by a non-root user and was configured in FIPS 140-2 mode, Security Intelligence database and Alert Dashboard occasionally do not start. (Bug 916285)

Workaround: Perform the following steps:

1. Go to `<custom installation directory>/opt/novell/sentinel/bin` to know the Sentinel Indexing Service.
2. Run the following command:

   ```
   ./si_db.sh status
   ```

   Verify whether the following output displayed:

   ```
   Connection between alert store and indexing service is running.
   Security Intelligence database is running.
   Indexing service is running.
   ```

   If any of the above mentioned three services are not running, perform the following steps.
3. Run the following command to stop Sentinel:

   ```
   rcsentinel stop
   ```
4. Log in to the Sentinel server as the `novell` user.
5. Run the following command:

   ```
   <custom installation directory>/opt/novell/sentinel/bin/si_db.sh startnoauth
   ```
6. Run the following commands to add dbauser and appuser users:

   ```
   cd <custom installation directory>/opt/novell/sentinel/3rdparty/mongodb/bin
   ./mongo
   use admin
   db.addUser ("dbauser", "novell")
   use analytics
   ```

```
db.addUser ("appuser", "novell")
exit
```

7 Stop the MongoDB database:

```
<custom installation directory>/opt/novell/sentinel/bin/si_db.sh stop
```

8 Perform the following steps to add encrypted password fields:

8a Run the following command to get the encrypted password for the `novell` user:

```
<custom installation directory>/opt/novell/sentinel/bin/encryptpwd -e novell
```

Encrypted password is displayed. For example:

```
bVWOzu6okMmMCkgM0aHeQ==
```

8b In the `configuration.properties` file, update the `baselining.sidb.password` and `baselining.sidb.dbpassword` properties with the encrypted

password. for example:

```
baselining.sidb.password=9bVWOzu6okMmMCkgM0aHeQ==
baselining.sidb.dbpassword=9bVWOzu6okMmMCkgM0aHeQ==
```

9 Exit from the `novell` user account and start Sentinel as the `root` user using the following command:

```
rcsentinel start
```

NOTE: Run the `configure.sh` script to reset the password whenever needed. For more information about running the `configure.sh` script, see "Modifying the Configuration after Installation" in the *NetIQ Sentinel Installation and Configuration Guide*.

4.26 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**.

4.27 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.

4.28 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
```

4.29 Cannot Enable Kerberos Authentication in Sentinel Appliance Installations

Issue: In Sentinel appliance installations, 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.

4.30 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.

4.31 Agent Manager Requires SQL Authentication When FIPS 140-2 Mode is Enabled

Issue: When FIPS 140-2 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 140-2 mode is enabled in your Sentinel environment.

4.32 Sentinel High Availability Installation in FIPS 140-2 Mode Displays an Error

Issue: If FIPS 140-2 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 140-2 mode.

4.33 Sentinel High Availability Installation in Non-FIPS 140-2 Mode Displays an Error

Issue: The Sentinel High Availability installation in non-FIPS 140-2 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 140-2 mode.

4.34 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*.

4.35 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.

4.36 Sentinel Link Action Displays Incorrect Message

Issue: When you execute a Sentinel Link action from the Web interface 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.

4.37 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.

4.38 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.

4.39 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.

4.40 Sentinel Agent Manager Does Not Capture the Windows Insertion String Fields With Null Values

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

Workaround: There is no workaround at this time.

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 website.

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

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.

6 Legal Notice

For information about NetIQ legal notices, disclaimers, warranties, export and other use restrictions, U.S. Government restricted rights, patent policy, and FIPS compliance, see http://www.netiq.com/company/legal/.