Sentinel 7.4 Release Notes

December 2015

Sentinel 7.4 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 **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 website.

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

1 What’s New?

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

1.1 New Certified Platforms

Sentinel is now tested and certified on the following platforms:

- **Operating System:** SUSE Linux Enterprise Server (SLES) 11 Service Pack 4 (64-bit).

  SLES 11 SP4 is certified only on traditional installations.
- **Data Synchronization:** Microsoft SQL Server 2014.

For more information about the certified platforms, see the Technical Information for Sentinel page.

1.2 Additional Permissions to Manage Reports

In addition to the **Manage reports** permission, Sentinel now provides report permissions at a granular level that allow you to provide users permission to specific report operations while restricting other report operations:

- **Import reports:** The **Manage reports** permission now allows users to only create, export, run, and delete reports. To import reports, users must now have the **Import reports** permission.
- **Run reports:** Allows users to only run reports.
- **Share reports:** Allows users to share reports with other roles.

For more information about permissions, see “Configuring Roles and Users” in the *NetIQ Sentinel Administration Guide*.

1.3 Sharing and Restricting Access to Reports

You can now share your reports with other roles and also control who can access the out-of-the-box reports:

- **Sharing reports with other roles:** You can share your reports with other roles without transferring the complete ownership of your reports. When you share your reports with other roles, users in that role will be able to view or run your reports depending on the report permission they have, but they will not be able to delete your reports.
- **Restricting access to out-of-the-box reports:** By default, the out-of-the box reports are visible to all Sentinel users. The report results of these reports may contain sensitive audit data, which you may not want all users to have access to. You can restrict these reports’ visibility only to you, with users in your role, or with users in selected roles as necessary.

  NOTE: Only users in the Administrator role can restrict the visibility of the out-of-the-box reports.

For more information, see “Working with Reports” in the *NetIQ Sentinel User Guide*.

1.4 Escalating Alerts to an Incident

After performing adequate investigation on an alert, you may determine there is a serious problem and the alert needs further investigation by the security analyst. Sentinel now allows you to escalate such alerts to an incident without losing all the work you already did as part of the alert investigation. For more information about escalating alerts to an incident, see “Escalating Alerts to an Incident” in the *NetIQ Sentinel User Guide*.

1.5 Performing Actions on Alert Trigger Events

Sentinel now provides a Search icon in the Alert Details page, which initiates a search for events that triggered the alert. When the events are displayed, you can perform necessary actions on alert trigger events in the similar way you perform on other events in the Search page. For more information about viewing the Alert Details page, see "Viewing Alerts" in the *NetIQ Sentinel User Guide*.

1.6 Sequence Timeout Correlation Rule

Sentinel now provides a new correlation rule type named Sequence Timeout. This rule detects when one or more events do not happen in the specified sequence. The Sequence Timeout rule fires when events that match the first subrule are not followed by events that match the second subrule in a specified time frame. For example, you can create a Sequence Timeout rule to detect a scenario where the server stopped but did not start again within an interval of 5 minutes. For more information about Sequence Timeout rule, see "Sequence Timeout Rule " in the *NetIQ Sentinel User Guide*.

1.7 Enhanced Authentication Mechanism for Collector Manager and Correlation Engine

When installing and configuring the Collector Manager and the Correlation Engine, you no longer need to copy the user credentials from the `activemqusers.properties` file. To enhance the security and for ease of use, Sentinel now allows you to use the `admin` user credentials to configure the Collector Manager and the Correlation Engine. For more information, see "Installing Sentinel" in the *NetIQ Sentinel Installation and Configuration Guide*.

1.8 SSL Connection for Data Synchronization

You can now establish an SSL connection to create a secured, encrypted communication channel between the Sentinel server and external database. For more information, see "Enabling SSL Communication for Data Synchronization" in the *NetIQ Sentinel Administration Guide*.

1.9 Java Upgrade

Sentinel 7.4 now includes Java 8 update 60, which includes fixes for several security vulnerabilities.

NOTE: The corresponding Java security vulnerability fixes are available in NetIQ Change Guardian 4.2 and later. Therefore, to receive events from Change Guardian, you must install Change Guardian 4.2 and later. If you already have a Change Guardian server sending events to Sentinel, before you upgrade to Sentinel 7.4, you must first upgrade the Change Guardian server, agents, and the Policy Editor to version 4.2 to ensure Sentinel continues to receive events from Change Guardian post-upgrade.

1.10 PostgreSQL Upgrade

Sentinel 7.4 now includes PostgreSQL 9.4.1, which includes fixes for several security vulnerabilities.

1.11 Latest Plug-ins

Sentinel 7.4 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 7.4, you can visit the Sentinel Plug-ins Website, review the revision history of the latest Collectors and Connectors in the specific documentation, and then determine which plug-ins to download and install.

1.12 Software Fixes

Sentinel 7.4 includes software fixes that resolve several issues.

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

1.12.1 Sentinel Logs Exceptions If You Click Save Multiple Times While Creating a User

Issue: If you click **Save** multiple times while creating a new user, Sentinel tries to create multiple users for the same user entry and logs exceptions. (BUG 944475)

Fix: After you click **Save**, Sentinel disables it till the new user record is saved. Also, Sentinel allows the creation of only one user entry at a time. These ensure that multiple entries for the same user cannot be saved.

1.12.2 Incorrect Data in the ObserverEventTime Event Field

Issue: Sentinel Agent Manager Connector displays incorrect data in the `ObserverEventTime` event field when Sentinel Agent Manager is set to default system locale. Hence, the date and time values vary according to the system language. (BUG 929551)

Fix: Regardless of the system language in Sentinel Agent Manager, the Sentinel Agent Manager Connector now displays correct data in the `ObserverEventTime` event field.

1.12.3 Security Vulnerability in the Sentinel Web Interface

Issue: The Sentinel Web interface allows potential attackers to include content that can cause Clickjacking. (BUG 949924)

Fix: The Sentinel Web interface now does not allow inclusion of any external content.

1.12.4 Customized Correlated Event Fields Are Lost When You Associate or Disassociate an Action with the Correlation Rule

Issue: Customized correlated event fields are lost when you associate or disassociate an action (any action other than `Create alert`) with the correlation rule. (BUG 949389)

Fix: Customized correlated event fields are no longer lost when you associate or disassociate an action with the correlation rule.

1.12.5 Unable to Install the Collector Manager If the Password Contains Special Characters

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

Fix: The Collector Manager installation process is now modified. You no longer need to specify the Collector Manager user credentials. You must now specify the `admin` user password, which accepts special characters. For more information, see the "Installing Collector Managers and Correlation Engines" section in *NetIQ Sentinel Installation and Configuration Guide* > *Installing Sentinel*.

1.12.6 Unwanted Security Manager Databases Associated with Sentinel Agent Manager After Migrating from Security Manager to Sentinel Agent Manager

Issue: After you migrate from NetIQ Security Manager to Sentinel Agent Manager, some Security Manager databases still exist. These databases need to be de-associated in Sentinel Agent Manager. (BUG 920939)

Fix: Security Manager databases are now de-associated in Sentinel Agent Manager after the migration is complete.

1.12.7 Cannot Install Sentinel after Uninstalling It

Issue: Sentinel installation fails if you install Sentinel after uninstalling it. (BUG 924567)

Fix: The Sentinel installation process is updated to resolve this issue. You can now install Sentinel after uninstalling it.

1.12.8 Event Field Names Do Not Display Correctly for Event Fields That Use Customer Variables

Issue: In search results, Sentinel displays short names for event fields that use customer variables instead of event fields' display names. (BUG 950361)

Fix: Sentinel now displays the full name for event fields in search results.

1.12.9 Real-time Event Views Are Unusable When There Are a Large Number of Values for the “Other” Series Item

Issue: When there are a large number of values for the `Other` series item, real-time event views become unusable because the right perspective of the data is lost. `(BUG 948003)`

Fix: The `Other` series item is disabled by default. If you want to use the `Other` series item, click **Other** in event views to enable it.

1.12.10 Sentinel Does Not Display Event Views with Area Charts Clearly

Issue: The Area type charts in event views are not clearly visible when the EPS is high. `(BUG 947891)`

Fix: Sentinel now displays event views in Stacked Area charts.

1.12.11 Sentinel Does Not Display the Number of Dashboards Available

Issue: In the Navigation panel, Sentinel does not display the number of dashboards available. `(BUG 948081)`

Fix: Sentinel now displays the number of dashboards available.

1.12.12 Charts in Event Views Do Not Display Correctly If Legend Names are Too Long and Take Up Huge Space

Issue: If the names of legends are too long, they take up a huge space and the chart does not display correctly. `(BUG 949310)`

Fix: Sentinel now truncates legend names to 24 characters when they are too long.

1.12.13 Orphan File Descriptors Are Created When EPSHistory REST API is Used

Issue: When you call EPSHistory REST API, a new file descriptor for reading `eps.data` is created and is never closed. This generates orphaned file descriptors. `(BUG 947974)`

Fix: Sentinel now closes file descriptors correctly.

2 System Requirements

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

3 Installing Sentinel 7.4

For information about installing Sentinel 7.4, see the *NetIQ Sentinel Installation and Configuration Guide*.

4 Upgrading to Sentinel 7.4

You can upgrade to Sentinel 7.4 from Sentinel 7.0 or later.

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

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

4.1 Upgrading Sentinel Appliance

You can upgrade the appliance using WebYaST only on Sentinel versions 7.3.2 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*.

Appliance upgrades from versions prior to Sentinel 7.3.2 must be done using 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 information about upgrading the appliance by using zypper, see "Upgrading the Appliance by Using zypper" in the *NetIQ Sentinel Installation and Configuration Guide*.

(BUG 956278)

4.2 Post Upgrade Configuration

If you are upgrading Sentinel 7.2.2 or an older version, perform the following actions:

- After the upgrade, the Search Proxy User role will not have the **Allow users to manage alerts** permission. This permission is necessary for the role to perform remote alert search. Assign the **Allow users to manage alerts** permission to the Search Proxy User role manually.

  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.

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.

The Java 8 update and the security vulnerability fixes included in Sentinel 7.3.1 and later may impact the following plug-ins:

- Cisco SDEE Connector
- SAP 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.

5.1 Sentinel Displays an Error When You Run the configure.sh Script in Custom Installations

Issue: When you run the `configure.sh` script in custom installations of Collector Managers or Correlation Engines, Sentinel displays the following error:

```
Error getting the client keystore file.
Refer to /two/var/opt/novell/sentinel/log/install.log for detailed error messages.

(BUG 956466)
```

Workaround: Ignore the error. The configuration proceeds as expected.

5.2 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.

5.3 Cannot Receive Events from Sentinel UNIX Agent 7.4 After Upgrading Sentinel to Version 7.3.1 and Later

Issue: The security vulnerability fixes included in Sentinel 7.3.1 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.

5.4 Error When Configuring the NFS Storage After Upgrading Sentinel Appliance to Version 7.3.1 and Later

Issue: Sentinel displays an error when you try to configure NFS as secondary storage location after you Sentinel appliance to version 7.3.1 and later. (BUG 934851)

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

```
init 6
```

5.5 Exception in the Sentinel Server Log When You Upgrade Sentinel Versions Prior to 7.3.1 to Versions 7.3.1 and Later

Issue: When you upgrade Sentinel from version 7.3 to version 7.3.1 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.

5.6 Cannot Receive Events from Secure Configuration Manager After Upgrading Sentinel to Version 7.3.1 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: Until a fix is available from Secure Configuration Manager, you can 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.

5.7 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.

5.8 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 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.

5.9 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.

5.10 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.

5.11 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.

5.12 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.

5.13 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)**.

5.14 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.

5.15 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.

5.16 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.

5.17 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.

5.18 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.

5.19 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*.

5.20 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.

5.21 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.

5.22 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.

5.23 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*.

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

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

Workaround: To configure the network Interface:

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

5.25 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.

5.26 Sentinel Services Might Not Start Automatically After the Installation

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

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

```
rcsentinel start
```

5.27 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.

5.28 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.

5.29 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.

5.30 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.

5.31 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.

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

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

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

5.33 Error While Installing Correlation Rules

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

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

5.34 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.

5.35 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.

5.36 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.

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

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

Workaround: There is no workaround at this time.

5.38 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.

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 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.

7 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/.