Sentinel 8.6 Release Notes

June 2023

Sentinel 8.6 resolves several previous issues and also adds a few new features.

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, our online community that also includes product information, blogs, and links to helpful resources. You can also share your ideas for improving the product in the Ideas Portal.

The documentation for this product is available 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 of the Release Note, HTML version. To download this product, see the Product Download website.

What's New?

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

Introducing OpenSearch

Sentinel now uses OpenSearch and OpenSearch Dashboard for secure, scalable, and distributed indexing of events. It replaces Elasticsearch and Kibana, which were used in the previous releases.

This change has also provided Role-Based Access Control (RBAC) through the security plugins that comes bundled along with OpenSearch and OpenSearch dashboard. Role-Based Access Control (RBAC) and multi-tenancy are supported for the visualization features in the Sentinel. With the RBAC, you can provide the right access to the right users based on their permission level for accessing the visualization features. The multi-tenancy in the visualization provides greater flexibility for tenants by letting them control their dashboards or visualizations. The security plugins provide secure communication between Sentinel and OpenSearch as well as between OpenSearch nodes and out of the box. Node-to-node encryption is also enabled in OpenSearch by default. It prevents potential attackers from intercepting traffic between OpenSearch nodes and keeps the cluster always secure.It helps to reduce the risk from network-based attacks.

Integration With ArcSight Threat Acceleration Program (Basic)

Sentinel is now integrated with ArcSight Threat Acceleration Program (Basic). The basic feed provides threat intelligence, which is automatically incorporated into the threat monitoring content of Sentinel. With this integration, the real-time threat detection capability of Sentinel has been enhanced as it can now detect more threats in real-time by using the centralized event log analysis.

TLS 1.3 Support

Sentinel supports communication through TLS 1.3 in non-FIPS mode.

When Sentinel is configured for FIPS mode, the communication protocol automatically changes to TLS 1.2. This happens due to some limitations of JDK with TLS 1.3.

JDK Upgrade

Sentinel now supports JDK version 1.8_update372.

Library Upgrades

Several packages have been upgraded to address security vulnerabilities. The underlying libraries of CVE-2022-42889 are upgraded, though the security vulnerabilities did not directly affect Sentinel.

RHEL 8.7 Support

This release provides additional support for Red Hat Enterprise Linux version 8.7.

Deprecated Operating System

The support for the following operating systems has been deprecated from this release:

- Red Hat Enterprise Linux version 8.3
- Red Hat Enterprise Linux version 8.4

Deprecated Plugins

The bundling of the following plugins with Sentinel 8.6 has been deprecated and would be available on Marketplace for downloading:

Collectors

- Cisco Network Admission Control
- F5 Firepass
- IBM DB2
- McAfee Network Security Platform
- McAfee Vulnerability Manager
- NetIQ Cloud Manager
- Novell Access Governance Suite
- Novell Cloud Security Service
- Qualys QualysGuard
- Tenable Network Security Nessus
- Tripwire IP360
- BeyondTrust Retina

Connectors

- NetIQ Audit
- Cisco SDEE

Action

- Webroot IP Lookup

Rebranding

Sentinel product and the associated documentation has been rebranded from Microfocus to OpenText.

The Sentinel plugin versions have been upgraded as part of rebranding. However, as there are no feature upgrades for most of these plugins, no release note is available for them.

No Auto-Upgrade for Collector Plugins

Novell/NetIQ collectors would not get auto upgraded on Sentinel upgrade. If you need the latest plugin version, you can download it from Marketplace.

Software Fixes

Sentinel 8.6 includes software fixes that resolve the following issues:

Vulnerability Related to Jetty 9.4.25.v20191220

Issue: There were a couple of vulnerabilities related to Jetty 9.4.25.v20191220 that was affecting Sentinel on port 9443 and 9090.

Fix: The Jetty version has been updated to `jetty 9-15.1.2-26.1`.

Creation of New clientID Fails

Issue: While creating a new ClientID and ClientSecret using a POST call, a failure message as `Authentication token not found` is displayed.

Fix: You can create a new `clientid` and `clientsecret` using a browser-based REST plugin like `Talend API Tester` or `Boomerang SOAP & REST client`.

TLS - SHA1 and CBC Cipher Issues

Issue: Unable to remove the SHA1 and CBC ciphers for GUI access (TLS).

Fix: Weak ciphers TLS - SHA1 and CBC have been disabled.

Issues in Configuring Externally-Signed CA

Issue: There were issues in configuring externally - signed CA as the documentation was incorrect.

Fix: The documentation is updated. For more information see section Importing the Digitally Signed Certificates into Sentinel on Using CA Signed Certificates.

Sentinel Service Takes Long to Start after an Upgrade

Issue: In cases where Sentinel server was deployed in a closed network (with no access to internet), the service was taking upto 20 mins to start after an upgrade..

Fix: The issue is fixed.

VMware ESXi Preview Collector Crashes

Issue: The VMware_ESXi_2011.1r6-201708240457-preview collector parser is unable to check input data and crashes during parsing.

Fix: Sentinel schema Source Port and Target Port data types have been updated.

Issues with the Correlation Test Rule Functionality

Issue: The test rule option was not loading as required.

Fix: The issue is fixed and the test rule feature works seamlessly.

Data loss Issues as Sentinel Installs SSPR Collector Plugin Automatically on Update

Issue: NetIQ Self Service Password Reset Collector is getting upgraded on Sentinel upgrade.

Fix: The Collector is removed from the upgrade list, so now it will not get upgraded on Sentinel upgrade.

Syslog TLS Client Disconnects If Sentinel Server Certificate is Not Validated

Issue: Syslog Connector was not showing the Source IP information when the connection is disconnected.

Fix: The exception, which is thrown at the time of disconnection contains Source IP details in it.

System Requirements

For information related to hardware requirements, supported operating systems, and browsers, see the Sentinel System Requirements.

License and Purchasing Information

To purchase an enterprise license or upgrade your existing license, call 1-800-529-3400, email info@microfocus.com or visit https://www.microfocus.com/en-us/products/netiq-sentinel/contact.

Installing Sentinel 8.6

For information about installing Sentinel 8.6, see the *Sentinel Installation and Configuration Guide*.

NOTE: All the hosts used for the Sentinel server and its components must be set up in two way DNS resolvable environment (Hostname to IP and IP to Hostname).

Upgrading to Sentinel 8.6

You can directly upgrade to Sentinel version 8.6 from version 8.3.1.0 and later. However, if you have a deployment of Sentinel version older than 8.3.1.0, then you must first upgrade to Sentinel 8.3.1.0 and then to Sentinel 8.6.

If you are upgrading to Sentinel 8.6, the existing Elasticsearch data will not be automatically moved to OpenSearch. You must forward the data using the data uploader tool to OpenSearch. For more information, see Migrating Data.

If you wish to save any custom dashboards and visualizations that you might have created in Kibana on or before Sentinel 8.5.1.1, export them from Kibana and then import them back to Opensearch Dashboards after the upgrade. For more information on exporting the data from Kibana, see Exporting Data from Kibana Dashboard to Opensearch Dashboard and for more details on importing the data to Opensearch Dashboard, see Importing Data from Kibana Dashboard to Opensearch Dashboard.

For Traditional upgrade, see Upgrading Sentinel Traditional Installation in Sentinel Installation and Configuration Guide.

Known Issues

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

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

Sentinel Control Center (SCC) is not Launching

Issue: After converting to FIPS mode, in a specific case, SSC does not launch on executing `launcher_controlcenter.exe`. It waits for a single sign-on authentication page and displays the message `Lost Connection`.

Workaround: Reboot the system.

Unable to View Storage Capacity Forecasting Chart

Issue: The **Storage Capacity Forecasting** chart at **Sentinel Main** > **Storage** > **Health**, is not available. This is because Zulu OpenJDK does not include the necessary fonts.

Workaround: Use the following commands to install the fonts:

- yum install fontconfig
- yum install dejavu

Cannot Copy the Alert Links of All the Alerts in an Alert View in Mozilla Firefox and Microsoft Edge

Issue: The **Select All *<number of alerts>* Alerts** > **Copy Alert Link** option does not work in Firefox and Edge.

Workaround: Perform the following steps:

1. Manually select all the alerts on each page of the alert view using the check box that allows you to select all the alerts.
2. Click **Copy Alert Link**.
3. Paste it in the desired application.

Login Screen is Not Displayed When Sentinel, Collector Manager, and Correlation Engine are Installed as an OVF Appliance Image

Issue: The installer halts at the installation in progress screen and does not display the login screen even though the installation is complete.

Workaround: Reboot the virtual machine and launch Sentinel, Collector Manager, or Correlation Engine.

Sentinel 8.6 Appliance in Microsoft Hyper-V Server 2016 Does Not Start When You Reboot

Issue: When Sentinel is deployed as appliance on Hyper-V Server 2016, Sentinel appliance does not start when you reboot it and displays the following message:

```
A start job is running for dev-disk-by\..
```

This issue occurs because the operating system modifies the disk UUID during installation. Therefore, during reboot it cannot find the disk.

Workaround: Manually modify the disk UUID. For more information, see Knowledge Base Article 7023143.

Installation of Collector Manager and Correlation Engine Appliance Fails in Languages Other than English in MFA Mode

Issue: Installation of Collector Manager and Correlation Engine appliance fails in MFA mode if the operating system language is other than English.

Workaround: Install Collector Manager and Correlation Engine appliances in English. After the installation is complete, change the language as needed.

Usability Issues in the Appliance Installation Screens

Issue: The **Next** and **Back** buttons in the appliance installation screens do not appear or are disabled in some cases, such as the following:

- When you click **Back** from the Sentinel precheck screen to edit or review the information in the Sentinel Server Appliance Network Settings screen, there is no **Next** button to proceed with the installation. The **Configure** button allows you to only edit the specified information.
- If you have specified incorrect network settings, the Sentinel Precheck screen indicates that you cannot proceed with the installation due to incorrect network information. There is no **Back** button to go to the previous screen to modify the network settings.

Workaround: Restart the appliance installation.

Collector Manager Runs Out of Memory if Time Synchronization is Enabled in Open-vm-tools

Issue: If you manually install and enable time synchronization in open-vm-tools, they periodically synchronize time between the Sentinel appliance (guest) and the VMware ESX server (host). These time synchronizations can result in moving the guest clock either behind or ahead of the ESX server time. Until the time is synchronized between the Sentinel appliance (guest) and the ESX server (host), Sentinel does not process events. As a result, a large number of events are queued up in the Collector Manager, which may eventually drop events once it reaches its threshold. To avoid this issue, Sentinel disables time synchronization by default in the open-vm-tools version available in Sentinel.

Workaround: Disable time synchronization. For more information about disabling time synchronization, see Disabling Time Synchronization.

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

Issue: When FIPS 140-2 mode is enabled in Sentinel, using Windows authentication for Agent Manager causes synchronization with the Agent Manager database to fail.

Workaround: Use SQL authentication for Agent Manager.

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
```

Workaround: The error can be safely ignored. Although the installer displays the error, the Sentinel High Availability configuration works as expected in non-FIPS 140-2 mode.

Keytool Command Displays a Warning

Issue: While using Keytool command, the following warning is displayed:

```
The JKS keystore uses a proprietary format. It is recommended to migrate to
PKCS12which is an
industry standard format using "keytool -importkeystore -srckeystore
 /<sentinel_installation_path>/etc/opt/novell/sentinel/config/
.webserverkeystore.jks -destkeystore
 /<sentinel_installation_path>/etc/opt/novell/sentinel/config/
.webserverkeystore.jks -deststoretype pkcs12".
```

Workaround: The warning is expected and you can safely ignore it. Although the warning is displayed, Keytool command works as expected.

Sentinel Does Not Process Threat Intelligence Feeds In FIPS Mode

Issue: In FIPS mode, when processing out-of-the-box threat Intelligence feeds from URLs, Sentinel displays the following error: `Received fatal alert: protocol_version`. This issue occurs because the out-of-the-box threat feeds now support only TLS 1.2, which does not work in FIPS mode.

Workaround: Perform the following:

1. Click **Sentinel Main** > **Integration** > **Threat Intelligence Sources**.
2. Edit each URL to change the protocol from `http` to `https`.

Logging Out From Sentinel Main Does Not Log You Out of Dashboards And Vice Versa in Multi-factor Authentication mode

Issue: In multi-factor authentication mode, if you log out of **Sentinel Main** you do not get logged out of Sentinel dashboards and vice versa. This is due to an issue in the Advanced Authentication Framework.

Workaround: Refresh the screen to view the login screen.

When you Open Sentinel Appliance Management Console an Error Message is Displayed

Issue: After upgrading to Sentinel, when you try to open Sentinel Appliance Management Console of the CE (Correlation Engine) or CM (Collector Manager) of HA (High Availability) servers, an error message `Error 404 - Not found` is displayed.

Workaround: For more information, refer to Micro Focus Knowledge Base document.

When you Launch the Visualization Dashboard as a Tenant User, an Error Message is Displayed

Issue: When a non-default tenant user launches the visualization dashboard, an error message **Forbidden** is displayed. This error message is displayed, whenever the dashboard is launched by the non-default tenant user who has **View-only** permission for the **Management** option and there is no user with **Edit** permission for the **Management** option under that tenant.

Workaround: Ignore the error message as there is no functionality impact.

In RHEL, RCM and RCE are not Connecting to the Server When CRL is Enabled

Issue: Remote Collector Manager (RCM) and Remote Correlation Engine (RCE) not able to connect to the server when CRL is enabled, in RHEL.

Workaround: Upgrade the **cURL version** on the machine to 7.60 or above.

RCM is not Forwarding the Events to the Sentinel Server When Event Visualization, FIPS, and CRL are Enabled

Issue: In the fresh installation of distributed setup, after enabling the Event Visualization, the FIPS, and the CRL services, the Remote Collector Manager (RCM) is not forwarding the events to the Sentinel Server.

Workaround: If either the Event Visualization and FIPS or the Event Visualization and CRL are enabled, then RCM forwards the events to the Sentinel server.

Incident Reports are Failing with Exceptions After Upgrading the Operating System

Issue: When you upgrade the Operating System, incident reports fail with exceptions.

Exception is Logged while Trying to Re-index for the First Time

Issue: An exception is being logged when the re-index operation runs for the first time.

Plugin Issues

The Java 8 update included in Sentinel might impact the following plug-ins:

- SAP (XAL) Connector
- Remedy Integrator

Contacting Open Text

For specific product issues, contact Open Text Support Open Text Support (https://www.microfocus.com/support-and-services/).

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos: Customer Support (https://www.microfocus.com/support-and-services/).
- The Community pages: Open Text Community (https://www.microfocus.com/communities/).

Legal Notice