Sentinel 8.6.1 Release Notes

November 2023

Sentinel 8.6.1 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:

JDK Upgrade

Sentinel now supports JDK version 1.8_update382.

Support of rcsentinel is removed

The command line utility 'rcsentinel' for managing and configuring Sentinel services is no longer supported.

Example: The command line utility for restarting sentinel services is now ‘systemctl restart sentinel.service or <sentinel_install_directory>/opt/novell/sentinel/bin/server.sh restart’ instead of ‘rcsentinel restart’.

Operating System Support

This release provides additional support for following operating systems:

- Red Hat Enterprise Linux Server (RHEL) 9.2 64-bit
- Red Hat Enterprise Linux Server (RHEL) 9.1 64-bit
- Red Hat Enterprise Linux Server (RHEL) 9.0 64-bit
- Red Hat Enterprise Linux Server (RHEL) 8.8 64-bit
- SUSE Linux Enterprise Server (SLES) 15 SP5 64-bit

Deprecated Operating System

The support for SUSE Linux Enterprise Server 15 SP3 64-bit and RHEL 8.5 operating systems has been deprecated from this release.

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 8.6.1

For information about installing Sentinel 8.6.1, 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 8.6.1

If you are upgrading to Sentinel 8.6.1, see section Upgrading Sentinel from *Sentinel Installation and Configuration Guide*.

You can directly upgrade to Sentinel version 8.6.1 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 8.6.1

If you are upgrading to Sentinel 8.6.1 from any version prior 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.

Software Fix

Sentinel 8.6.1 includes software fixes that resolve the following issues:

Lucene Search fails to retrieve any events

Issue: The Lucene Regex Parsing in Sentinel does not support capital letters.

Fix: Lucene search is now supported with capital and camel case characters.

ISO Appliance Installation Failure

Issue: Installation of the ISO appliance failed with Hyper-V 2016 environment.

Fix: Appliance on Hyper-V environment is now supported with VHD format.

Vulnerability Fix of ActiceMQ

Issue: The Java OpenWire protocol marshaller exhibits a vulnerability that exposes a risk of RCE attack. This flaw potentially allows a remote attacker with network access to exploit a Java-based OpenWire broker or client.

Fix: Upgrade both brokers and clients to version 5.16.7 to address and fix this vulnerability.

Known Issues

Opentext 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, SCC 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.

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.

Error displayed on Passive node after failover on OS: SLES 15 SP5

Issue: Insufficient prvileges (4): call=39, status='complete' error is displayed on Passive node after failover on OS: SLES 15 SP5.

Workaround: Ensure consistent Userid (UID) and Groupid (GID) values for the 'novell' user and 'novell' group across all cluster nodes, and set ownership of the '/var/opt/novell/sentinel' path to 'novell:novell'

The terminal error 'gfxterm' is not found

Issue: The terminal error 'gfxterm' isn't found is displayed during the installation of the Hyper-V Appliance.

Workaround: Please disregard this message, as it does not impact any functionality.

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