NetIQ

Release Notes

Sentinel 8.5 Release Notes

August 2021

Sentinel 8.5 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 in the HTML version of the documentation posted at the Sentinel Documentation page. To download this product, see the Product Download website.

- “What’s New?” on page 1
- “System Requirements” on page 3
- “License and Purchasing Information” on page 3
- “Installing Sentinel 8.5” on page 4
- “Upgrading to Sentinel 8.5” on page 4
- “Known Issues” on page 4
- “Contacting Micro Focus” on page 11
- “Legal Notice” on page 11

What’s New?

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

- “ArcSight Intelligence Integration with Sentinel” on page 2
- “MITRE ATT&CK” on page 2
- “JDK Upgrade” on page 2
- “Storing Raw Events from Connector” on page 2
- “TLS Support” on page 3
- “Operating System (OS) Versions” on page 3
- “Software Fixes” on page 3

ArcSight Intelligence Integration with Sentinel

With this release, Sentinel provides its customers a way to integrate with exciting analytics technologies of ArcSight Intelligence. Hence, Sentinel users can get risk score almost in real-time and use it for their further analysis in their own correlation rule, etc. This enables Sentinel to get much threat hunting experience.

ArcSight Intelligence is a user and entity behavioral analytics solution that uses data science and advanced analytics to identify the top risky entities and behaviors occurring in your organization. Intelligence first establishes the normal behavior for your organizational entities and then uses advanced analytics, to identify the anomalous behaviors by any entities and provides an appropriate risk score to each such entities.

Sentinel provides a way to Integrate with ArcSight Intelligence 6.3. This integration facilitates users of the Sentinel to send their data to the ArcSight Intelligence for analysis and also, provides a way to receive entities risk score details from the Intelligence. This makes Sentinel detect any riskier users and entities in the organization that might compromise the entire system and creates a potential threat.

MITRE ATT&CK

MITRE ATT&CK helps cybersecurity teams assess the effectiveness of their Security Operations Center (SOC) processes and defensive measures to identify areas for improvement. MITRE ATT&CK is a globally accessible knowledge base of cybersecurity adversary tactics and techniques based on real-world observations. The MITRE ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

From this release of Sentinel, administrators can map correlation rules with MITRE ATT&CK ID. MITRE ATT&CK stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). The MITRE ATT&CK Framework is a common industry language of threat actor Tactics and Techniques based on real-world observations.

Sentinel administrators can now map their own out-of-the-box or custom correlation rule directly with the MITRE ATT&CK ID. Hence, providing a lot of data analysis at their fingertips thereby giving them a power of visualization of what are the rules get fired or what all Tactics and MITRE Techniques are being exploited by their customers. Sentinel is providing them a certain set of tool-sets by which they can immediately get a view of their network and what is the most important attacks they need to prevent.

If a correlation rule mapped with a MITRE ATT&CK ID is triggered, the triggered events will have MITRE ATT&CK ID and MITRE ATT&CK Name. These events are analyzed through a widget that is available in a default security health dashboard. The top ten MITRE ATT&CK Name appears in this dashboard in a Time Range of 1 day and Display Interval of 1 hour.

JDK Upgrade

In order to avoid security vulnerabilities (CVE-2021-2161, CVE-2021-2163, CVE-2021-2341, CVE-2021-2432, CVE-2021-2369, CVE-2021-2388) and to make use of the security features of new JDK standards, JDK is upgraded from 1.8.0_update242 to 1.8.0_update302

Storing Raw Events from Connector

Sentinel Syslog connector, from the version 2021.1r1, will enable storing of the raw events coming through the ArcSight Smart Connectors. These are the untouched, unprocessed events that are directly generated by the end device. This setting can be enabled by checking the **Preserve Raw Event** option in the corresponding Smart Connector.

TLS Support

Support of TLS 1.0 and TLS 1.1 has been removed.

Operating System (OS) Versions

Traditional installation: Sentinel is now certified on the following new platform as well:

- Red Hat Enterprise Linux (RHEL) 8.3

Deprecated OS: Following OS are now deprecated since RHEL and SLES removed support for these OS:

- RHEL 7.6 and 7.7
- SLES 15 SP1

Software Fixes

Sentinel 8.5 includes software fixes that resolve the following issues:

- "Converting to FIPs on the Sentinel Server Changes the Protocol from TLS 1.2 to TLS 1.1" on page 3
- "Sentinel REST Calls Failing After Upgrading Sentinel Java Client" on page 3
- "Error when Generating a New Report" on page 3

Converting to FIPs on the Sentinel Server Changes the Protocol from TLS 1.2 to TLS 1.1

Issue: When converting to FIPS on the Sentinel server, the protocol changes from TLS 1.2 to TLS 1.1 and this causes termination of the connection between SAM and Sentinel server. However, customer must use TLS 1.2

Fix: Now when converting to FIPS, TLS version is not getting changed from 1.2 to 1.1

Sentinel REST Calls Failing After Upgrading Sentinel Java Client

Issue: After upgrading Sentinel Java Client from 8.1 to 8.2, REST calls failing.

Fix: Now after upgrading Sentinel Java Client from 8.1 to 8.2, REST calls not failing.

Error when Generating a New Report

Issue: Error when generating a new report. The main issue of the error can be, keystore is tampered or the password is incorrect.

Fix: Not getting an error when generating a new report.

System Requirements

For more information about 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 8.5

For information about installing Sentinel 8.5, 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 8.5

You can upgrade to Sentinel 8.5 from any prior versions of Sentinel (from Sentinel 8.2 and later).

IMPORTANT: Upgrading to Sentinel 8.5.0.0 from Sentinel 8.4.0.1 is not supported. However, you can upgrade to Sentinel 8.5.0.1

IMPORTANT: Because of the latest JDK upgrade, for configuring LDAPS and SDK, the user needs to use hostname instead of IP address, and also it must be resolvable.

IMPORTANT: There is a change in the upgrade procedure of Traditional and Appliance installation. Please refer to Settings in Elasticsearch for Secure Cluster Communication and follow the steps. This is only applicable if you are upgrading Sentinel to the latest versions from 8.3.1 and prior.

IMPORTANT: You can perform an offline update by downloading Offline Patch ISO for each appliance. For more information, see Performing Offline Updates.

WARNING: If you are upgrading from versions prior to Sentinel 8.3, you must manually assign the **Send events and attachments** permission to non-administrator users who send events or attachments to Sentinel. Unless you assign this permission, Sentinel will no longer receive events and attachments from Change Guardian and Secure Configuration Manager.

For Traditional installation, refer to Upgrading the Operating System section 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, please contact Technical Support.

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

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

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.

Unable to View Storage Capacity Forecasting Chart

Issue: In **Sentinel Main** > **Storage** > **Health**, the **Storage Capacity Forecasting** chart 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

Error When Launching a Kibana Dashboard After Upgrading Sentinel

Issue: Launching a Kibana dashboard displays the following message: `No default index pattern. You must select or create one to continue.`

Workaround: To set a Kibana index pattern as the default index pattern:

1. Select any of the following:
   - alerts.alerts
   - security.events.normalized_*
2. Click **Set as Default**.

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.

Installing Sentinel, Collector Manager, and Correlation Engine as an OVF Appliance Image Does Not Display the Login Screen

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

Issue: In 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.

Error When Upgrading to Sentinel 8.2 HA Appliance

Issue: When you upgrade to Sentinel 8.2 HA appliance, Sentinel displays the following error:

```
Installation of novell-SentinelSI-db-8.2.0.0-<version> failed:
with --nodeps --force) Error: Subprocess failed. Error: RPM failed: Command exited
with status 1.
Abort, retry, ignore? [a/r/i] (a):
```

Workaround: Before you respond to the above prompt, perform the following:

1. Start another session using PuTTY or similar software to the host where you are running the upgrade.
2. Add the following entry in the `/etc/csync2/csync2.cfg` file:

   ```
   /etc/opt/novell/sentinel/config/configuration.properties
   ```
3. Remove the `sentinel` folder from `/var/opt/novell`:

   ```
   rm -rf /var/opt/novell/sentinel
   ```
4. Return to the session where you had initiated the upgrade and enter `r` to proceed with the upgrade.

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 is expected and you can safely ignore it. Although the installer displays the error, the Sentinel High Availability configuration works successfully 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: Until a fix is available in the Advanced Authentication Framework, refresh the screen to view the login screen.

The Kibana Custom Dashboard is not Displayed After Upgrading to Sentinel 8.3.1

Issue: The Kibana custom dashboard is not displayed when you upgrade from Sentinel 8.3 or earlier to Sentinel 8.3.1.

Workaround: Ensure that you re-create the custom dashboard after upgrading Sentinel.

When you Launch Kibana the Conflict Error Message is Displayed

Issue: After installing or upgrading Sentinel and when you launch Kibana for the first time, the conflict error message is displayed.

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

When you Reboot OS Redhat 8.1 and 8.2, Sentinel is not Started Automatically

Issue: After installing Sentinel on OS Redhat 8.1 and 8.2, Sentinel (Server, RCM, or RCE) is not started automatically after reboot.

Workaround: Change the SELINUX value to **SELINUX=disabled** in the file `/etc/selinux/config`.

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

Issue: After upgrading to Sentinel 8.3, 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.

Users with Hide Management Permission of Visualization, Still Can See the Management Tab in the Kibana Page

Issue: After upgrading to Sentinel 8.4, users with hide management permission of visualization still can see the Management tab on the Kibana page, but cannot access the features of the Management tab.

When Admin Changes User Role of Alerts, Immediately Changes are not Updated in the Kibana Page

Issue: Existing users unable to see any alerts on the Kibana page immediately, although permission is updated by the admin to see the alerts.

Workaround: You need to logout and login again when the user permission is updated.

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 OS from any Older Version to Latest Version

Issue: When you are upgrading the Operating System, from an older version to the latest version, 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 while Running `convert_to_fips.sh` in Sentinel 8.5 RCM/RCE Appliance Build

Issue: When the system administrator runs `convert_to_fips.sh` in Sentinel 8.5 RCM/RCE appliance build, after providing correct credentials of the users in a continuous loop, the following error message is displayed:

```
ERROR: Failed to connect to <Sentinel server IP>:
Failed to retrieve token for communication channel.
```

Workaround: Perform the following steps:

1. Exit from the script execution.
2. Go to <Sentinel RCM/RCE installation>/etc/opt/novell/sentinel/config/configuration.properties
3. Set the value of `rest.endpoint.port` to corresponding webserver port.

   For example, `rest.endpoint.port=8443`
4. Rerun the `convert_to_fips.sh`

Contacting Micro Focus

For specific product issues, contact Micro Focus Support at https://www.microfocus.com/support-and-services/.

Additional technical information or advice is available from several sources:

- Product documentation, Knowledge Base articles, and videos: https://www.microfocus.com/support-and-services/
- The Micro Focus Community pages: https://www.microfocus.com/communities/

Legal Notice

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see http://www.microfocus.com/about/legal/ (http://www.microfocus.com/about/legal/).