Micro Focus Security
ArcSight Interset Standard Edition

Software Version: 6.1.0

Release Notes

Document Release Date: July 2020

Software Release Date: July 2020

Contents

Introduction

This Guide provides the ArcSight Interset 6.1.0 release notes, which include:

- Supported Software Environments
- What's New
- Unsupported Features
- Known Issues

If you have any questions or concerns about the information presented in this or any other ArcSight Interset 6.1.0 Guides, contact Micro Focus Customer Support at https://softwaresupport.softwaregrp.com/.

System Requirements

This section provides information about system requirements and tuning guidelines for ArcSight Interset.

Important: For information about system requirements for CDF, Transformation Hub, the database, and SmartConnectors, see the specific product documentation in the ArcSight Product Documentation website.

Software Requirements

Software	Version
CDF	2020.05
Transformation Hub	3.3.0
Fusion	1.1.0
Recon (Optional)	1.0.0
Database	Vertica 9.2.1
SmartConnectors	8.0.0

Interset 6.1.0 supports the following Web browsers:

- Microsoft Edge - Latest, Chromium only
- Google Chrome - 74 and above
- Mozilla Firefox - 67 and above

License Requirements

Interset comes with a trial license. Install a valid license before the trial license expires or if the trial license policy has been violated. Purchase the relevant license based on the number of entities you want Interset to analyze. The license policy is violated when the number of entities exceeds the maximum limit. Renew your license before its validity expires or if the license policy has been violated.

Transformation Hub and ArcMC come with a trial license each. For each of these components, install a valid license before the trial license expires.

The database comes with an inbuilt license. The storage capacity for the license is 976 PB. Renew your database license if the storage capacity exceeds 976 PB.

Contact Micro Focus Customer Support at https://softwaresupport.softwaregrp.com/ to procure the licenses.

Hardware Requirements

For information about the hardware requirements for your deployment, see the "Hardware Requirements" section in *Interset 6.1.0 Deployment Guide for CDF.*

Supported Data Sources and SmartConnectors

Interset supports the following Data Sources and SmartConnectors:

Data Sources	Supported Smart Connectors
Access	SmartConnector for Microsoft Windows Event Log - Native Application and System Event Support SmartConnector for Microsoft Windows Event Log - Unified Application and System Event Support
Active Directory	SmartConnector for Microsoft Active Directory Windows Event Log Native
VPN	SmartConnector for Microsoft Network Policy Server File SmartConnector for Pulse Secure Pulse Connect Secure Syslog SmartConnector for Nortel Contivity Switch Syslog
Web Proxy	SmartConnector for Microsoft Forefront Threat Management Gateway File SmartConnector for Squid Web Proxy Server File SmartConnector for Blue Coat Proxy SG Multiple Server File

In addition, a fuller set of SmartConnectors is supported for those sources which provide data of relevance to the Interset analytics models. Micro Focus may need to examine sample logs to optimize analysis of data from this broader set of sources.

Ports Used

In addition to the ports used by CDF, Transformation Hub, and the database, Interset uses the following ports when firewall is enabled. Ensure that the following ports are available:

Ports	Direction	Description
TCP 30820	Inbound	Used for the database to connect to HDFS during Analytics processing
TCP 30070	Inbound	Used for Hadoop Monitoring Dashboard (Optional)
TCP 30010	Inbound	Used for communication between the HDFS NameNode and the HDFS DataNodes

What's New

This section outlines the key features of this release:

- **Installation using Scripts**

  To enable an easier deployment, Interset provides installation scripts that automatically take care of all the prerequisites, software installations, and post-installation configurations. The scripts are applicable only for single-node, new deployments where high availability is not needed. For more information about installing using scripts, see the "Deploy Interset Using Scripts" section in *Interset 6.1.0 Deployment Guide for CDF.*

- **Integration with Recon**
  You can now leverage Recon threat hunting capabilities by integrating Recon with Interset. In addition to exploring events in Interset, you can gain further insight into events and identify hidden security threats through Recon.

- **Support for New Data Types**

  Interset now supports the ingestion and analysis of the following data types:

  - Access
  - VPN

  In addition, Interset also supports the full set of SmartConnectors for those sources which provide data of relevance to the Interset analytics models.

Unsupported Features

The following features are currently not being supported in Interset 6.1.0. These are currently projected for future release versions.

- **Multi Tenancy**
- “**Workflow**”

Important: One Node Cluster has specific configuration parameters required in CDF. For more information about single node setup, contact Micro Focus Customer Support at https://softwaresupport.softwaregrp.com/.

Known Issues

This section includes a summary of the known issues for Interset 6.1.0.

Cannot View the Events That Triggered an Anomaly

In the Interset UI **> Explore** page **> Anomalies & Violation** panel, when you click an anomaly or violation, a dialog box provides context about the anomaly or violation. When you click **View Events** to view the events that triggered the anomaly or violation, you might not see any events. This is a sporadic issue. To resolve the issue, click **View Events** again to view the events.

[FT-20305]

Cannot View the Events for Anomalies Related to Travel

In the Interset UI **> Explore** page **> Anomalies & Violation** panel, when you click an anomaly related to travel and view the events that triggered it by using any of the following methods, you might not see any events.

- Click **View Events** to view the events that triggered the anomaly.
- Click **View Events**, then click **Explore Raw Events** to explore raw events in the Event Viewer.

This happens if the latitude and longitude data from the SmartConnectors have values that are more than four decimal points.

For example, longitude value = 100.992541

This does not have an impact on Interset Analytics and hence, anomalies are generated. However, the events contributing to the anomalies are not displayed.

To avoid this situation, ensure that the latitude and longitude data have values up to four decimal points when they are sent by the SmartConnectors to Transformation Hub.

For example, longitude value = 100.9925

[FT-20867]

Cannot Explore Raw Events for the Anomaly Types 282, 286, and 287 of the Active Directory Server Data.

In the Interset UI **> Explore** page, when you filter anomalies with 282, 286, or 287, anomalies are displayed in the **Anomalies & Violation** panel based on the filter you provided. When you click an anomaly, a dialog box provides context about the anomaly or violation. When you click **View Events > Explore Raw Events**, you cannot see any events.

As a workaround, perform the following steps:

1. Launch a terminal session and log in to any of the Kubernetes nodes.
2. Execute the following command to retrieve the nginx configmap name:

   ```
   export NS=$(kubectl get namespaces |grep arcsight|cut -d ' ' -f1); kubectl -n $NS   get configmap   |grep nginx
   ```

   The nginx-load-balancer-conf configmap is displayed.

3. Execute the following command to modify the nginx-load-balancer-conf configmap:

   ```
   export NS=$(kubectl get namespaces |grep arcsight|cut -d ' ' -f1); kubectl -n $NS   edit configmap nginx-load-balancer-conf
   ```

4. In the **Data** section in the configmap, add the **http2-max-field-size** field if it is not already added and set the value of the **http2-max-field-size** field to 16k.
5. Save the configmap.
6. Execute the following command to retrieve the nginx ingress pod name:

   ```
   export NS=$(kubectl get namespaces |grep arcsight|cut -d ' ' -f1); kubectl -n $NS get pods |grep ingress
   ```

7. Execute the following command to restart the nginx ingress pod:

   ```
   kubectl delete pod <nginx-ingress-controller-xxx> -n namespace
   ```

[FT-20865]

Filtering Using the Hand Icon in the Matrix of Anomalies & Violations Does Not Update the Top Risky Users Accordingly

In the Interset UI **> Explore** page **> Matrix of Anomalies & Violations**, when you click the hand icon, then click and drag the cursor across the matrix to see the risky users and anomalies or violations for a specific time interval, the users in the **Top Risky Users** panel are not updated accordingly.

For example, if there are no risky users and the associated anomalies or violations in the selected time interval (for example, between 4:30 pm and 4:35 pm on a day), the **Top Risky Users** panel still displays users.

This is a known issue and will be addressed in a later version.

[FT-20451]

Events in Recon For Historical Data

When you ingest historical data in the database and Analytics is run for it, the anomalies are displayed in the Interset dashboard. In Recon, you cannot see or explore the events that triggered the anomalies when the database receives historical events that were generated more than 7 days ago.

For example, if the database receives historical events on 9th July and the events were generated on 1st July, the events are not visible in Recon.

[FT-20973]

Mismatch Between the Anomaly Expected Highest Value and the Visualization Expected Highest Value

In the Interset UI **> Explore** page **> Anomalies & Violation** panel, when you click an anomaly or violation, a dialog box provides context about the anomaly or violation. The **Expected highest for <user_name>** value in the visualization does not match the value in the anomaly or violation.

For example, an anomaly is " It was slightly unusual that <user_name> logged in to Interset 12 times in an hour; <user_name> typically logs in at most 6 times in an hour." and the **Expected highest for <user_name>** value in the visualization is 4. In this example, the expected highest value for the user is 6 and the value in the visualization is 4. There is a mismatch between the values.

This is a known issue and will be addressed in a later version.

[FT-20947]

CSV Reports Do Not Have Timestamps in the Date and Time Format

The CSV Reports have timestamps in the Unix Epoch format instead of the date and time format. This is a known issue and will be addressed in a later version. [FT-20978]

Malware Scan Might Report a False Positive

When scanning the cdf-2020.05.00100-2.3.0.7.zip file or an installer *.tar file that contains this file, certain malware detection programs might report a false positive in a subroutine called updateRoleId. This subroutine is within /cdf/images/cdf-master-images.tgz file.

There is no workaround needed. We validated that the code is not malware. We have verified that the package was built and compiled in a secure and trusted fashion. In an upcoming release, we will modify the packaging to avoid this false positive.

Known Issues in CDF

For known issues related to CDF, see Transformation Hub Release Notes in the ArcSight Product Documentation website.

Changing a BOT User to a NOTBOT User Has No Effect on Inactive Projects

When anomalies are identified because few users access a specific project, and one or more of the users are flagged as bots, changing the BOT users to NOTBOT users – and therefore increasing the number of non-bot users accessing the project – will not impact the project's identification as 'inactive'. Anomalies will therefore continue to be identified when the project is accessed, even though more non-bot users are now regularly accessing the project.

This issue has no workaround. [FT-8934]

Bad Message 413 reason: Request Entity Too Large

While logging to the Interset UI, a bad message **413** is encountered. To resolve this issue, clear the cookies for the site and log in again. [FT-20164]

Daylight Savings Time

During the weeks immediately following Daylight Savings Time (DST) clock changes, you may observe an increase in reported Normal Working Hours anomalies. These anomalies, which are due to automatic software clock changes, will usually have risk scores of zero (0), and are reflective of the perceived Normal Working Hours pattern shift. [FT-8601]

Swagger User Interface Might Display an Alert Icon Even When Properly Authenticated

When an Interset Administrator logs into the Swagger user interface, they might see an alert icon on certain functions. This alert does not impact the API and can be ignored. [FT-10243]

Repartition Percentage Threshold

In the **CDF Management Portal > Configure/Deploy** page **> Interset**, when you specify a value for the **Repartition Percentage Threshold** field, the installer does not validate the value. However, Interset Analytics fails if the value is not set between 0.7 and 1.0 as stated in the tooltip.

To avoid this situation, ensure that you set a value between 0.7 and 1.0.

[FT-20011]

Prefix Filtering Does Not Work in CDF for Event Viewer

When searching for a prefix string in Event Viewer, the result of the query is of all the occurrences of the string. This is a known issue and will be addressed in a later version.

[FT-20239]

Changing the HDFS NameNode Does Not Terminate the Previous Instance of the HDFS NameNode Container

In the **CDF Management Portal > Configure/Deploy** page **> Interset**, when you change the value of the **HDFS NameNode** field to deploy the HDFS NameNode container on another worker node, the older instance of the HDFS NameNode container goes into a pending state instead of being terminated.

As a workaround, you need to perform the following steps after changing the value in the field.

1. In the CDF Management Portal, click **Cluster > Nodes**.
2. Click the [-] icon for the **interset-namenode:yes** label present on the worker node.
3. From **Predefined Labels**, drag and drop the **interset-namenode:yes** label to the worker node to which you want to add it. Ensure the worker node matches the new value you specified in the **HDFS NameNode** field.
4. Configure the database with HDFS. For more information, see the "Configure the Database with HDFS" section in *Interset 6.1.0 Deployment Guide for CDF.*
5. Restart the HDFS DataNodes. Do the following:
    a. Launch a terminal session and log in to a worker node where an HDFS DataNode is deployed.
    b. Execute the following commands:

```
NAMESPACE=$(kubectl get namespaces | grep arcsight-installer | awk '{ print $1}')
```

```
kubectl get pods -n $NAMESPACE | grep -e 'hdfs\|interset-analytics' | awk '{print $1}' | xargs kubectl
delete pod -n $NAMESPACE --force --grace-period=0
```

[FT-20019]

Certificate Warnings in Logstash Logs

When you view the Logstash logs, you may come across the following warnings:

- ** WARNING ** Detected UNSAFE options in elasticsearch output configuration!
- ** WARNING ** You have enabled encryption but disabled certificate verification.
- ** WARNING **To make sure your data is secure change :ssl_certificate_vertification to true

Though these warnings are displayed, there is no impact in the functionality. Hence, you can ignore these warnings.

[FT-20038]

Swagger UI Session Expires After 120 seconds of Inactivity

When using the Swagger UI and trying an API request for a particular operation, a successful result returns a code of 200. If the Swagger UI is not used for 120 seconds or more (inactive screen), and the same API request when re-tried, results in returning an error code of **401**.

To get the correct result, the workaround for this issue is to go back to the Interset UI. Refresh the Interset UI and then use the Swagger UI. The reason for the issue is due to token expiry after 120 seconds. This will be addressed in a later version.

[FT-20234]

Cannot Save Searches in Event Viewer

When exploring events in the Event Viewer, you cannot save the search query that you build. Ideally, when you **Type to filter raw events**, a custom built query can be saved using the **Save** option at the bottom left. This functionality is not working currently.

There is a workaround to the issue which involves modification of the **investigator.yml**. Contact Micro Focus Customer Support at https://softwaresupport.softwaregrp.com/ to resolve the issue. This will be addressed in a later version.

[FT-20299]