Micro Focus Security ArcSight Intelligence SaaS

Software Version: 6.4.5

User's Guide

Document Release Date: April 2023
Software Release Date: April 2023

Legal Notices

Micro Focus
The Lawn
22-30 Old Bath Road
Newbury, Berkshire RG14 1QN
UK

https://www.microfocus.com

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://softwaresupport.softwaregrp.com/support-contact-information
Support Web Site	https://softwaresupport.softwaregrp.com/
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/

Contents

Introduction

With the growing number of threats to monitor in the IT ecosystem, IT organizations have a demanding need to continuously think of better and effective ways to secure their enterprise network. In today's world, employees can access their company's data and applications from within the company, home, and even through personal mobile devices regardless of their geographical location. With IT organizations having to manage their assets both on-premises and in the cloud environment, it has become increasingly challenging for IT security teams to detect any malicious activities carried out by internal users intentionally or accidentally, such as data theft, data exfiltration, and account compromise.

While security information and event management (SIEM) solutions such as Micro Focus ArcSight Enterprise Security Manager (ESM) offer security and compliance monitoring solutions that focus mostly on external threats, IT organizations need solutions that also perform in-depth user behavior monitoring that can detect anomalies and potential threats happening within the organization. Most of the data loss and data breach activities are carried out by users with valid credentials.

ArcSight Intelligence SaaS 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. Using your organization's data, Intelligence first establishes the *normal* behavior for your organizational entities and then using advanced analytics, it identifies the *anomalous* behaviors that constitute potential risks such as compromised accounts, insider threats, or other cyber threats.

Intelligence detects potential threats by performing the following:

- Uses unsupervised machine learning techniques to automatically define user profiles and baselines
- Actively monitors account access patterns and actions on the associated entities against defined baselines to detect anomalies
- Applies a risk score for each entity based on the anomalies detected
- Displays anomalies prioritized by the user risk score in a user-centric, interactive dashboard that helps Security Analysts investigate the highest risks first and take necessary actions immediately

Therefore, Intelligence significantly decreases the number of threats that go undetected and increases a Security Analyst's ability to quickly investigate all detected anomalies.

Supported Data Types

This section provides information about each data type supported by Intelligence. The data of the supported data types is ingested and used in Intelligence analytics.

- Access
- Active Directory
- Authentication
- Web Proxy
- EDR

Access data sources: sh (Fileshare), rs (Resource)

The Access data represents events collected from solutions such as Identity and Access Management (IAM), Microsoft SharePoint, Microsoft OneDrive where users access resources such as servers or fileshares.

Examples of access events include:

- A user fails to access a network share object `VPM-CFDB01.data.int`
- A user attempts to access shared drive `Network Shares/HR/HR-Policies/`

Examples of IAM products include: Active Directory

The Intelligence Access data type best supports Windows Security Log (or Active Directory) event data.

The Microsoft Windows Security Log contains records of login/logout activity, as well as other security-related events specified in the system's Audit Policy. A System Administrator must enable the Windows Audit feature to allow events to be recorded in the Security Log.

Mandatory Input Fields

The following fields are required to be present in the Access events for analytics to process the events:

Column Name	Data Type	Required (Y/N)	Description	Example
deviceReceiptTime	Integer	Y	The time at which the event related to the activity was received.	1592839336200 Equivalent GMT - 2020-06-22 15:22:00
destinatonUserName	Varchar	Y	The user involved in authentication.	john.legget

Column Name	Data Type	Required (Y/N)	Description	Example
destinationHostName	Varchar	N	The server handling the authentication.	
filePath	Varchar	N	Path, project, or tag that the resource belongs to.	
fileType	Varchar	N	Type of collection that the resource belongs to, for example, shr	
fileName	Varchar	N	File, ID, or Object that the resource is mapped to.	
externalId	Varchar	N	Usually a Windows event code (for example, **5140**, **4664**, and so on), but Analytics can be configured to accept other values, including **-1**.	4663
categoryOutcome	Varchar	N	An indicator of whether the authentication was successful. Usually either **success** or **failure**, however, Analytics can be configured to accept other values.	failure

Active Directory data sources: ad

The Active Directory data represents events collected from Identity and Access Management (IAM) solutions that identify successful and failed logins to authentication targets. These authentication targets include domain controllers/servers, resources, and file shares.

Examples of authentication events include:

- A user fails to log in to YOURDC.yourcompany.com
- A user attempts to access shared drive DEV_102_share

Examples of IAM products include:

- Active Directory

The Intelligence Active Directory data type best supports Windows Security Log (or Active Directory) event data.

The Microsoft Windows Security Log contains records of login/logout activity, as well as other security-related events specified in the system's Audit Policy. A System Administrator must enable the Windows Audit feature to allow events to be recorded in the Security Log.

Mandatory Input Fields

The following fields are required to be present in the Active Directory events for analytics to process the events:

Column Name	Data Type	Required (Y/N)	Description	Example
destinationUserName	Varchar	Y	The user involved in authentication. Primary entity for **ad** data source.	john.legget
categoryOutcome	Varchar	Y	The outcome of the event. One of **success** or **failure**.	success
destinationHostName	Varchar	Y	The target involved in the authentication. Typically the domain controller to which the user is authenticating. The secondary entity for an **ad** data source.	CONTROLLER3.interset.com
externalId	Varchar	Y	Usually a Windows event code (e.g., **4624**, **4771**, etc.), but Analytics can be configured to accept other values, including **-1**.	4624
deviceReceiptTime	Integer	Y	The time at which the event related to the activity was received.	1592839336200 Equivalent GMT -2020-06-22 15:22:00
destinationNTDomain	Varchar	N	The domain that contains the user that is affected by the event.	interset
categoryObject	Varchar	N	The type of the object.	/Host/Operating System

Column Name	Data Type	Required (Y/N)	Description	Example
categoryBehavior	Varchar	N	The action or behavior associated with the event.	Authentication/Verify
deviceCustomString4	Varchar	N	The string that further explains why the user failed to authenticate. Usually a hexadecimal code, but can be any string.	0xc0000064
sourceGeoLocationInfo	Varchar	N	Combination of the latitude and longitude values separated by a comma.	45.1234, -74.4321

Authentication data source: auth

The Authentication data represents events collected from Identity and Access Management (IAM) solutions where users authenticate or attempt to authenticate with an authentication provider.

Examples of authentication events include:

- l a user fails to log onto the server **NFMC.company.com**
- l a user successfully logs into the workstation **WS-1495SM-NA**

Examples of IAM products include:

- Active Directory
- PingFederate
- SecureAuth IDP

The Intelligence authentication data type best supports Windows Security Log (or Active Directory) event data. To ingest data from other authentication data sources, contact Micro Focus Customer Support at https://softwaresupport.softwaregrp.com/.

The Microsoft Windows Security Log contains records of login/logout activity, as well as other security related events specified in the system's Audit Policy. A System Administrator must enable the Windows Audit feature to allow events to be recorded in the Security Log.

Mandatory Input Fields

The following fields are required to be present in the Authentication events for analytics to process the events:

Column Name	Data Type	Required (Y/N)	Description	Example
destinationUserName	Varchar	Y	The user involved in authentication. Primary entity for **auth** data source.	john.legget
categoryOutcome	Varchar	Y	The outcome of the event. One of **success** or **failure**.	success
destinationHostName	Varchar	Y	The target involved in the authentication. Typically the domain controller to which the user is authenticating. The secondary entity for an **auth** data source.	CONTROLLER3.interset.com
externalId	Varchar	Y	A string describing the event type or a type of an authentication action.	4624
deviceReceiptTime	Integer	Y	The time at which the event related to the activity was received.	1592839336200 Equivalent GMT -2020-06-22 15:22:00
destinationNTDomain	Varchar	N	The domain that contains the user that is affected by the event.	interset
categoryObject	Varchar	N	The type of the object.	/Host/Operating System

Column Name	Data Type	Required (Y/N)	Description	Example
categoryBehavior	Varchar	N	The action or behavior associated with the event.	Authentication/Verify
deviceCustomString4	Varchar	N	The string that further explains why the user failed to authenticate. Usually a hexadecimal code, but can be any string.	0xc0000064
sourceGeoLocationInfo	Varchar	N	Combination of the latitude and longitude values separated by a comma.	45.1234, -74.4321

Web Proxy data source: pxy

The Web Proxy data are raw events that capture network traffic, primarily Web surfing, from a collection of human users.

Examples

- A user accessed the Web site **https://yourcompany.com**
- A user received data from a web destination, **vap3iad3.lijit.com**

Examples of Web Proxy products include:

- Microsoft Internet Security and Acceleration Server (ISA)
- Squid
- Blue Coat Secure Web Gateway

Mandatory Input Fields

The following fields are required to be present in the Web Proxy events for analytics to process the events:

Column Name	Data Type	Required (Y/N)	Description	Example
deviceReceiptTime	Integer	Y	The time at which the event related to the activity was received.	1592839336200 Equivalent GMT -2020-06-22 15:22:00
requestMethod	Varchar	Y	The HTTP method of the request.	GET
deviceSeverity	Varchar	Y	The HTTP response status.	400
bytesIn	Integer	Y	Bytes returned to the client in the response.	410235
sourceUserName	Varchar	N	The name associated with the client making the request.	john.legget
destinationHostName	Varchar	N	The host name of the machine the client is trying to connect to.	a-0001.a-msedge.net
bytesOut	Integer	N	The number of bytes the client sent in its request.	690235
requestClientApplication	Varchar	N	The agent string of the Blue Coat devices.	Mozilla/5.0 (Windows NT 5.1; rv:8.0) Gecko/20100101 Firefox/8.0
deviceCustomString1	Varchar	N	The agent string of the Microsoft devices.	Windows Update Agent
deviceVendor	Varchar	N	The device vendor of the client.	Microsoft
deviceProduct	Varchar	N	The device product of the client.	ISA Server

The Endpoint Diagnostics and Response (EDR) data is useful for endpoint, authentication, access and web proxy models, which further process the data.

Administering Intelligence for End Users

There are tasks that you can perform as the Intelligence Administrator to ensure that the Analytics end users have access to the information they need, when they need it.

These tasks include:

- "Managing Bots and Bot-like Users" below
- "Tuning the Analytics" on page 16

User Roles

Two user roles exist in Intelligence SaaS: Admin and User.

Note: The user role is specified when configuring the user for your environment. For any changes to users and roles, Micro Focus Customer Support at https://softwaresupport.softwaregrp.com/

The **Admin** role can perform the following tasks:

- Access the Intelligence UI to view analyzed data
- Access the Anomalies page
- Tune Anomaly weights and importance
- Add comments and notes to anomalies and violations
- Create, add, and delete tags
- Access the Tuning API and Analytics API

The **User** role can perform the following tasks:

- Access the Intelligence UI to view analyzed data
- Add comments and notes to anomalies and violations
- Create, add, and delete tags

Managing Bots and Bot-like Users

Bots are scripts or applications that run automated tasks. If your organization has system bot activity, this activity — because of the exceptional speed with which the activity occurs — will likely generate Risky Hours in your analytics. Intelligence identifies those system users it deems to be bots, and strips them from the **Matrix of Anomalies & Violations**.

By default, Intelligence is configured to not identify bots in analytics and instead consider them as users. You can configure Intelligence to identify bots and remove them from analytics. However, prior to configuring Intelligence for bot identification, ensure that analytics has run at least once.

There is often very real difficulty identifying those system users that are bots and those that are live humans, based on the user activity alone. Your Security team should work with you to identify those system users that are truly bots, and those that are not.

After the true bots are identified, you can configure Intelligence to remove these bots from analytics. Similarly, if bot-like users have been stripped from analytics but are not bots, you can configure Intelligence to ensure that these users remain in analytics.

Note: To manage bots and bot-like users, you must have access to the Tuning API. To request access to the API, contact Micro Focus Customer Support at https://softwaresupport.softwaregrp.com/.

Enabling or Disabling Identification of Bots

By default, Intelligence is configured to not identify bots in analytics and instead consider them as users. You can configure Intelligence to identify bots and remove them from analytics. However, prior to configuring Intelligence for bot identification, ensure that analytics has run at least once.

By default, Intelligence is also configured to not delete the previous analytics results of entities identified as bots for the current analytics run. Therefore, there is no change in the entities identified as bots for the current analytics run. You can configure Intelligence to delete the previous analytics results of entities identified as bots for the current analytics run. This ensures that entities identified as bots earlier are not automatically considered as bots for the current analytics run.

To enable or disable identification of bots:

1. In a web browser, log in to Intelligence with an Admin role.
2. Click  , point to **API Documentation >**, then select **Tuning API** in the drop-down list to open the API in Swagger.
3. Expand the **Parameters** section.
4. Click the row where **PUT /{tid}/parameters/{name}** is displayed.
5. Click **Try it Out!**.
6. Under **Parameters**, specify the tenant ID for **tid** and specify **BOT_CLASSIFIER_ENABLED** as the parameter name for **name**. The **BOT_CLASSIFIER_ENABLED** parameter is used for enabling or disabling bot identification. By default, the value of this parameter is 0, indicating that bot identification is disabled. A value of 1 indicates enabling bot identification.
7. In the text box provided for the **body** parameter, specify the tenant ID, the parameter name, and a value of 1 to enable the parameter or 0 to disable the parameter.
8. Click **Execute**.
9. Repeat steps 5 to 8 for the **BOT_CLEANER_ENABLED** parameter. The **BOT_CLEANER_ENABLED** parameter is used for retaining or deleting the previous analytics results of

entities identified as bots for the current analytics run. By default, the value of this parameter is 0, indicating that the previous analytics results of entities identified as bots are not deleted for the current analytics run. A value of 1 indicates the previous analytics results of entities identified as bots are deleted for the current analytics run.

Tagging Entities as Bots or Bot-like Users as Users

You can tag an entity currently shown as a user in analytics as a bot. Similarly, you can tag an entity currently shown as a bot in the PDF report as a user. The changes will reflect in the next analytics run.

To tag entities as bots or bot-like users as users:

Important: You can tag entities as bots or bot-like users as users only if bot identification is enabled prior to analytics run.

1. In a web browser, log in to Intelligence with an Admin role.
2. Click  , point to **API Documentation >**, then select **Tuning API** in the drop-down list to open the API in Swagger.
3. Expand the **Entity Tags** section.
4. Click the row where **PUT /{tid}/entity_tags/{ds}/{did}/{type}/{identifier}/{tag}** is displayed.
5. Click **Try it Out!**
6. Under **Parameters**, do the following:
   - For the **tid** parameter, specify the tenant ID.
   - For the **ds** parameter, specify the data type.
   - For the **did** parameter, specify the data identifier.
   - For the **type** parameter, specify the tag type.
   - For the **identifier** parameter, specify the tag key.
   - For the **tag** parameter, specify the tag value.
7. In the text box provided for the **body** parameter, specify the value for the desired fields.
8. Click **Execute** to enable the new entity tag. The changes will reflect in the next analytics run.

Tuning the Analytics

After you have had the opportunity to explore the Intelligence Analytics and investigate the leads identified in the Intelligence Dashboard, you may want to fine-tune the importance applied by the Analytics to the events in your source data.

For example, perhaps due to the nature of your business, your employees have never — not once — accessed the corporate information systems outside of the standard 9:00 am to 5:00 pm work hours. In this scenario, should an employee one day access your corporate information system outside of the standard work hours, the potential for that access to be a risk to your organization could be much more significant than it would be in an organization in which employees routinely access the corporate systems at any hour. As a result, you might want to increase the importance of the group of anomalies in the anomaly family, **User worked in an unusual hour**. When you increase the importance of this anomaly family, anomalies of this type that are identified in the Analytics will have a higher risk score than they would have using the default importance level.

You fine-tune the importance of individual anomalies, or grouped anomaly families, on the **Anomalies** page of the Intelligence user interface.

To tune Analytics:

1. In a web browser, log in to Intelligence with an Admin role.
2. Click **Settings**  , then select **Anomalies** in the drop-down list.
   The **Anomalies** page opens, listing all of the anomalies triggered on your source data by the models. Each anomaly appears with the following information: the model **ID**, as well as the model **Data Type**, **Threat Type**, and **Family Type**.
3. To change the importance of an anomaly **Family Type**, do the following:
   - At the top of the **Anomalies** page, click in the **Type to filter by tag or keyword** field.
     A new dialog box opens, displaying the **Data Type**, **Threat Type**, and **Family Type** for the anomalies identified.
4. Select a **Data Type**, **Threat Type**, or **Family Type.**
   Following the example discussed above, under **Family Type**, you would select the **User worked in an unusual hour** anomaly family type.

   The anomalies of that type triggered by the Analytics are now isolated in the **Anomalies** page.
5. Select an anomaly, and then click **Tuning**.
6. In the **Anomaly Tuning** dialog box, click one of the available values on the horizontal rule.

Continuing with the example above, you would click the **High** value on the horizontal rule to increase the importance of these anomalies to the highest amount available.

Important: The **Default Weight** of the anomaly is indicated at the top of the **Anomaly Tuning** dialog box, with a lock symbol. Intelligence strongly recommends that you avoid changing any anomaly weight unless instructed to do so by Micro Focus Customer Support.

7. Click **Apply**.
8. Repeat Steps 5 through 7 for the remaining anomalies.

The next time Analytics is run, the new **Importance** value will be applied to the anomalies.

Tip: To return the anomaly importance to the default setting at any time, select the anomaly, click **Tuning**, and then in the **Anomaly Tuning** dialog box, click **Reset to Default**.

Understanding Users and Other Entities in Intelligence

Intelligence uses advanced analytical models to measure behavior and to quantify risks. These models range from cluster models, which group together users and assets based on specific behavioral vectors, to volumetric anomaly models, rare activity models, and other higher-order models. Many different behavioral vectors are tracked and measured, which reduces the ability for malicious users or compromised accounts to "fake" normal behavior.

The Intelligence models are true advanced behavioral models: they don't rely on binary rules or arbitrary thresholds. Rather, these models measure the probability that an observed action is truly anomalous and represents a true potential risk. Using this type of approach leads to a continuous, prioritized list of risks, and helps improve the efficiency of IT security teams and their tools.

The use of Intelligence machine learning models means that you are not required to perform any additional configuration for the analytical models to execute. Through observation, Intelligence learns what constitutes normal behavior for the entities within your organization, and immediately begins to quantify abnormal behavior. There are no thresholds to set, no rules to author, and no configurations to undertake.

Intelligence displays the results of Intelligence Analytics in an interface that provides at-a-glance actionable information on current risk, and flexible multi-entity historical data exploration.

Users and Other Entities

Entities are the foundation of Intelligence Analytics. Entities are the objects involved in behaviors. For example, if a user Philip accesses Fileshare A, then the event contains, at minimum, one behavior, and two entities. Philip's account and Fileshare A are the two entities, and the access is the behavior.

Behaviors

Behaviors are often thought of as single events. In the previous example, the access can be captured in one single event. If that event happens to be a malicious action, finding that one malicious event is virtually impossible. This is because there can be billions of these events, and the overwhelming majority of events are perfectly legitimate and normal behaviors.

Accumulating Risk

As behaviors occur, Intelligence processes these events and calculates that which is normal from dozens of behavioral perspectives. For example, Intelligence will count how many times Philip accesses Fileshare A each hour, how often his authentication attempts fail on Fileshare A, at what time of day, or which day of week he is normally active, etc.

These metrics are all calculated using unsupervised machine learning. This means that the system identifies what is normal, rather than organizational security practitioners setting thresholds which may be reasonable for some, but completely inappropriate for others.

As new observed behaviors occur, Intelligence determines whether the behaviors are normal, or unusual. When unusual, Intelligence calculates how unusual the behavior is. The more unusual the behavior, the higher the significance of the anomaly. When anomalies are identified, these anomalies influence the risk score of the entities that are involved in the behavior. The more an entity is involved in significant anomalies, the higher that entity's risk score. For example, if Philip accesses Fileshare A 100 times in an hour, and accesses 100 other fileshares that he's never accessed before, his risk score will spike, because the behavior simulates internal recon or lateral movement. In addition, because Fileshare A was involved in a significant set of anomalies, its risk score will also spike.

This comprehensive reporting allows practitioners to explore the anomalies from different perspectives. In cases where multiple user accounts are accessing Fileshare A in an abnormal manner, the user behavior may not appear abnormal and therefore the risk scores may not

spike significantly, however, Fileshare A would have a significant spike in its risk score, providing a signal to security practitioners that Fileshare A requires attention.

As entities are involved in risky behaviors, their risk scores increase. The riskier the entity's behavior the more the risk increases. When the entity is not engaging in any activity, the risk score decays downward towards zero; as a result, when the entity goes a long time without registering any suspicious activities, its risk score will trend toward zero.

Understanding the Intelligence Dashboard

The Intelligence Dashboard is a user-centric, interactive dashboard that provides information on the top risky entities and behaviors occurring in your organization. It displays the Intelligence Analytics results, allows you to visually explore the results and the underlying raw data, and take appropriate actions immediately. With the help of the **Overall Risk** page, you can view the overall risk status of your organization. With the help of the **Entities** page, you can explore the risky entities grouped by their type. With the help of the **Explore** page, you can determine the types of risky activities occurring within your organization. With the help of the Event Viewer, you can explore the events that contributed to the risky activities.

Viewing the Overall Risk Details

When you first log in to Intelligence, you are taken to the **Overall Risk** page. This page allows you to see, at a glance, the overall risk status of your organization. For example, in the following screen shot you immediately see:

- Over 1 million events were analyzed
- About 145 thousand anomalies and violations were found
- 9 active risky entities were identified
- The overall risk is high and increasing
- The threat of Credential Access is contributing 25% to the overall risk
- The various streams of the graph indicate the potential threat types involved
- The types of entities involved and their risk counts
- The top five risky users

When you click an entity type, the **Entities** page opens, where additional information for the selected entity type is displayed.

When you click one of the **Top 5 Riskiest Users**, the **Explore** page opens, with the selected user's name applied to the **anomalies and violations** filter.

Exploring the Entities Page

The **Entities** page provides the entity risk scores, sorts the entities and their risk scores in descending order, and then also provides the trending information, the entity name, the potential threat type, and the most relevant anomaly identified by Intelligence. Potential threat types are determined by the most relevant risky activity in the system.

At the top of the **Entities** page, you can use the different entity tabs to explore the riskiest entities grouped by their type, such as **Users**, **Projects** or **Controllers**, for example. Tabs in bold text represent entities that are present in the data. Typically, you will explore your list of users first.

Note: You may see a difference between the number of entities that exist in your data, and the number of entities that appear in the Intelligence Analytics user interface. This is because:

- The entities that appear in the **Entities** page include only
  - Those entities with a current risk score greater than zero (0); and
  - Those entities that have a current risk score of zero (0), but for which anomalies were identified during the selected time period.
- Entities identified as BOTs do not appear in the user interface.

Potential threat types are determined by the riskiest activity identified by Intelligence for that entity. For example, if the riskiest alert results from behaviors in which a user account is accessing unusual locations or assets, the potential threat type will appear as **Potential Lateral Movement**, and a summarized description of the anomaly will be shown on the right of the page. This provides immediate context for security practitioners, and enables them to more quickly determine whether further investigation is required.

User-Defined Tags

On the **Entities** page, you can associate **User-defined tags** with individual entities or many entities at the same time. You can also create new tags and delete tags you don't need any more.

Important: Do not use **bot**, **forcebot**, or **notbot** as names for a **User-defined tag**.

To manage tags:

1. Choose one or more entities from the **Top Risky Entities** list by selecting the checkbox(es) in the left-most column.

2. Click the **Tag Management** icon ( ).
   The **Tag Management** dialog shows the tags associated with the selected entities. Tags that have checkmarks are associated with all the selected entities. Tags with a stroke through the middle of the checkbox are associated with one or more (but not all) of the selected entities. Tags with no checkmarks are not associated with any of the selected entities.
3. Do one of the following:
   - To associate tags with the selected entities, select the checkbox next to one or more tags and click **Apply**.
   - To remove the association between a tag and the selected entities, clear the checkbox next to the tag and click **Apply**. The **Total entities tagged** field is updated to show the number of entities associated with the tag.
   - To create a new tag, click **Create a new tag?**. Enter the new name in the **tag-name** field, and click **Create**. The new tag is created and associated with the selected entities.
   - To rename a tag, select the tag by clicking its name, then click the **tag-name** field and type the new name. Click **Save Changes** to save the new name.
   - To delete a tag, select the tag by clicking its name, then click **Delete**. Click **Yes** to confirm the deletion.

Exploring the Explore Page

When you select an entity, the **Explore** page opens, where the entity's name is filtered. Here, all **Anomalies & Violations** associated with that entity are shown within the established time range. To find or filter another entity, use the search filter at the top of the **Explore** page.

The **Explore** page information allows you to use to determine the types of risky activities that are occurring within your organization. The **Explore** page features the **Matrix of Anomalies & Violations**, the **Contribution to Risky by Threat** graph, and the **Top Risky Users** and **Anomalies & Violations** panels, which are displayed by default.

- Most Accessed Panel
- Top Risky Panel
- Top Users to Trigger Violations Panel

Matrix of Anomalies & Violations

The **Matrix of Anomalies & Violations** is a visual representation of the **Anomalies & Violations** in your data set, displayed as squares, color-coded to reflect their severity.

You can change the time window for the **Matrix of Anomalies & Violations** to reflect a time period of specific interest. You can choose the following time periods: **24 Hours**, **7 Days**, **30 Days**, **Year**, or you can set the time period to include **All Data**. To zoom in on a specific area of the matrix, click the **+** icon and then click and drag your cursor across the area of the matrix where you want to zoom in. To zoom out, click the **-** icon, or select one of the predefined time windows. To pan across the time window, click and drag your cursor across the matrix (zoom must not be enabled). As you zoom or pan, all aspects of the user interface update dynamically and accordingly.

You can use the slider to the left of the matrix to filter alerts based on their risk level. This enables you to reduce the number of alerts displayed in a gradual manner, and as appropriate. You can also click one of the **Risk** squares below the graph to set the slider filter to that risk level. For example, if you wanted to view **Medium Risk** and above, you would click the yellow **Medium Risk** square. This would filter out all low risk alerts, as shown in the example below.

In the **Matrix of Anomalies & Violations** timeline, you can filter the analytics on the associated entities displayed in **Anomalies & Violations**.

Periods of Risky Activity features an **Overall Risk Trend** which displays a baseline within the graph. When you add an entity filter to the **Periods of Risky Activity** graph, a new **Risk Trend** line based on that entity is created. This custom **Risk Trend** displays a baseline based on that entity's activity. You can have multiple **Risk Trends** displayed at once. You can also hide and show the **Risk Trends** by selecting the name of the **Risk Trend**.

Contribution to Risk by Threat

In **Matrix of Anomalies & Violations** is the **Contribution to Risk by Threat** graph. This graph organizes and displays potential threat types by their percentage of the overall risks. You can filter the graph by threat type by selecting the threat type name or square in the graph. For example, if you wanted to highlight the percentage that **Potential Internal Recon** represents in the graph, you would select the **Potential Internal Recon** name or square underneath the graph. To reveal/hide the **Contribution to Risk by Threat** graph, click the **Contribution to Risk by Threat** heading.

Applying Filters to Entity and Anomaly Data

At the top of the **Entities** and **Explore** pages is a field where you can select filters to apply to the data that is displayed.

- On the **Entities** page, the filter field is labeled **Type to filter entities by name, tag, or type...**
- On the **Explore** page, the filter field is labeled **Type to filter anomalies and violations...**

From the filter field you can choose a filter from the dropdown menu, or you can search for filters by typing the filter name. Depending on your data set, you can apply filters on many aspects of your data, including **Users**, **Entity Types**, **Projects**, **Controllers**, **Flags**, and **User-defined tags**.

When you select filters, the filters appear in a list under the filter field:

- On the **Entities** page, the filter list is labeled **Showing entities matching:**
- On the **Explore** page, the filter list is labeled **Showing anomalies and violations matching:**

To disable a filter:

- In the filter list, hover your cursor over the filter name and then click the checkbox on the left. The filter is still displayed but is no longer applied to the data. Repeat this process to enable a disabled filter.

To remove a filter from the filter list:

- In the filter list, hover your cursor over the filter name and click the **X** on the right. The filter is removed from the list, but is still available to use if you select it again.

Anomalies & Violations Panel

The **Anomalies & Violations** panel displays triggered activities in the form of a list. Each **Anomaly** or **Violation** has a time stamp, risk color, description, potential threat type, Viewed by flag, and associated entities attached to it. The **Anomalies & Violations** list can be sorted by **Time** (default) or by **Risk**.

The Viewed by flag on an anomaly displays the username of the threat hunter who has already seen or investigated the anomaly details.
On the **Explore** page, in the filter field labeled as **Type to filter anomalies and violations...**, you can filter all the viewed anomalies and violations by selecting the Viewed by flag from the dropdown menu.

To sort the list:

- At the top left of the **Anomalies & Violations** panel, click the dropdown menu and then select **Sort by time** or **Sort by risk**.

To apply filters based on an **Anomaly** or **Violation**:

- Below the description of the **Anomalies** or **Violation**, click the tags you wish to apply to the filter.

To disable a filter:

- At the top left of the page, under **Type to filter anomalies and violations...**, hover your cursor over the filter name and then click the checkbox on the left. Repeat this process to enable a disabled filter.

To delete a filter:

- At the top left of the page, under **Type to filter anomalies and violations...**, hover your cursor over the filter name and click the **X** on the right.

When you click in an **Anomaly** or **Violation** box, a visualization is provided to enhance context and includes a description of the activity. From here you can choose to explore the raw events that triggered the **Anomaly** or **Violation**, For more information on exploring raw events, see the **Exploring Raw Events** section.

To download a CSV report, click the **Events** option and then, click on the CSV symbol next to the date, this will automatically download the CSV report.

Anomaly and Violation Flags

Intelligence provides five (5) possible flags that you can use to characterize, or mark individual anomalies and violations within the Analytics. These five flags are represented by the following symbols:

These five flags, or symbols, have no established definitions; as a result, your organization can determine the appropriate meaning for each symbol within the context of the anomalies and violations that you want to highlight in your data.

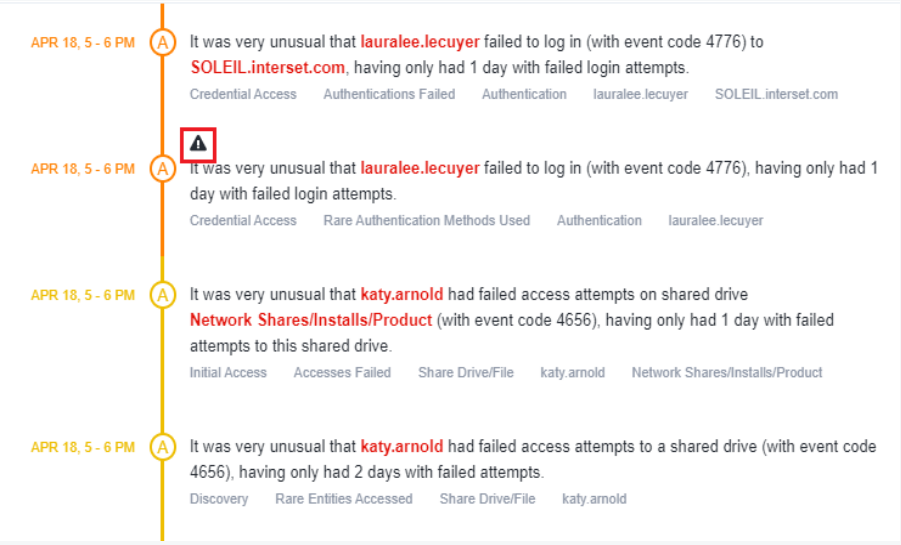
For example, you may decide to use one of these symbols to identify anomalies and violations resulting from failed access or log in attempts. You choose which of the flags you will use for this purpose and then, in the **Anomalies & Violations** panel, you mark the individual anomalies accordingly. When you have finished marking the anomalies and violations, you have only to select the flag as a filter to produce a list of all failed access and log in attempts.

To create flags:

1. In the **Anomalies & Violations** panel, click in an anomaly for which you want to set a flag. The anomaly opens, displaying the flags in the upper left corner.
2. Click on a flag symbol to enable it for the anomaly.

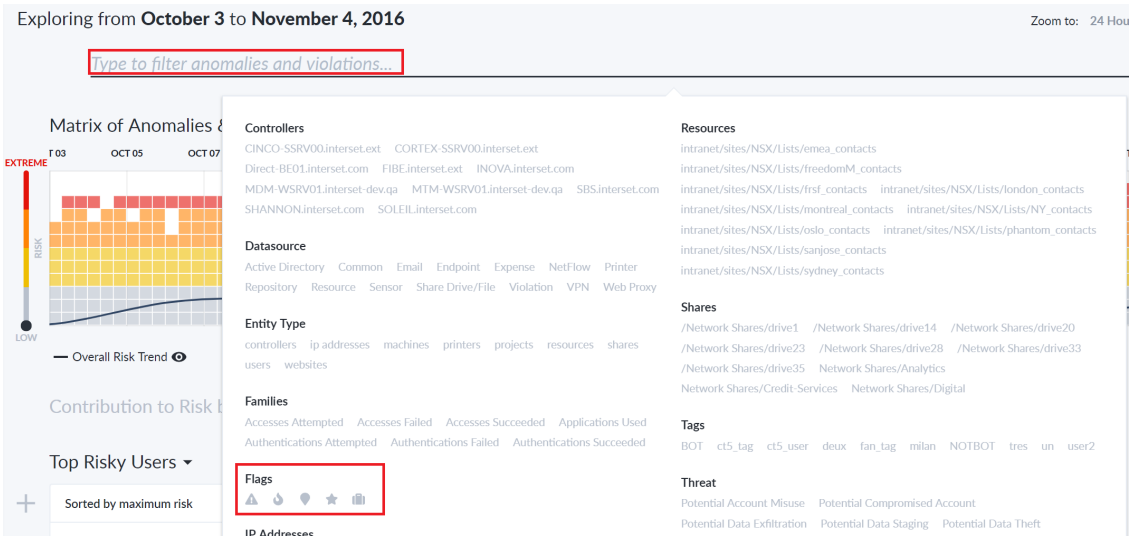
Tips:

- When a flag is enabled for an anomaly or violation, the symbol changes from light to dark.
- When you close the anomaly and return to the list of anomalies and violations, the enabled flag appears within the anomaly and provides a visual cue.

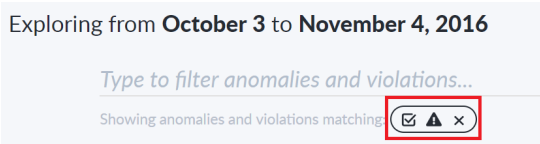


- When you hover over the flag, the date and time it was created, and the account that created it, are displayed.

3. To view all the anomalies and violations flagged with a specific symbol, click in the **Type to filter anomalies and violations** field.
4. In the filter drop-down menu, under **Flags**, select the flag on which you want to filter the anomalies and violations.



The Explore page now displays only the anomalies and violations that match the defined filter, which is displayed directly below the **Type to filter anomalies and violations** field.



Tips:

- To return to the unfiltered view of anomalies and violations, click the **X** beside the filter.
- To remove a flag from an anomaly or violation, open the individual anomaly or violation, and then click the flag to disable it.

Adding Comments to an Anomaly or Violation

Based on your investigation of an anomaly or a violation, you may want to add your observations so that other members of your team can leverage the information you have gathered so far. You can add a comment by clicking on an item in the Anomalies & Violations panel, and typing in the **Notes** field.

Entity Details Panel

When you select an entity, an **Entity Details** panel containing additional information on the entity you clicked opens. If you selected a **User** entity, for example, the **Entity Details** panel might display information regarding the **Most Recent Risk Score**, **Maximum Risk** score within the time frame, Read-only tags, User-defined tags, Typical working hours, and Typical weekly activity. To download a PDF report on the entity, click the PDF icon beside the entity name.

From the **Entity Details** you can create and apply **User-defined tags**.

Important: Do not use **bot**, **forcebot**, or **notbot** as names for a **User-defined tag**.

To create a tag:

1. On the right side of **User-defined tags**, click the icon. A **+** appears below the **User-defined tags** section.
2. Click the **+**.
3. In the dialog box, enter the name of the tag you want to create.
4. On the right side of **User-defined tags**, click **done** to save the tag.

To delete a tag:

1. On the right side of **User-defined tags**, click the icon.
2. Click a tag to highlight it.
3. Press your **Delete** or **Backspace** key to delete the tag.
4. On the right side of **User-defined tags**, click **done** to save your changes.

Note: If you use the same tag for multiple entity types, the results of filtering may also return entities that are associated with entities of that tag. For example, filtering on a tag of "Boston" which has been applied to users and controllers located in Boston may return users outside of Boston that have interacted with the controllers with that tag.

Authentications Panel

The **Authentications** panel displays the total number of successful and failed authentication attempts, sorted by entities with the most failed attempts in descending order.

To add the **Authentications** panel:

- Click the **+** symbol and then select **Authentications**.

To remove the panel:

- Click the **X** symbol at the top right of the panel.

Most Accessed Panel

On the **Explore** page, you can view the **Most Accessed** entities of your whole dataset, or of specific entities.

To add a **Most Accessed** panel:

- At the bottom of the page beside the leftmost tab, click the **+** symbol, select **Most Accessed** and then select a filter.

Each **Most Accessed** filter displays a list of entities that have been interacted with, sorted in descending order. You can further explore the **Most Accessed** entities by selecting an entity to open the **Entity Details** panel.

To remove the panel:

- Click the **X** symbol at the top right of the panel.

Top Risky Panel

On the **Explore** page, the **Top Risky** panel provides a list of the top risky entities by type, displaying the **Top Risky Users** by default. You can change the filter to display a different entity type by clicking **Top Risky Users**, selecting **Top Risky**, and then selecting an entity type. The **Top Risky** list is sorted by maximum risk.

Note: You may see a difference between the number of entities that exist in your data, and the number of entities that appear in the Intelligence Analytics user interface. This is because:

- Only entities with anomalies appear in the Top Risky list; entities without identified anomalies within the selected time range are filtered out. In addition, entities identified as BOTs do not appear in the user interface.
- When you select the all data timeframe, all entities that have ever had at least one identified anomaly will be shown.

To view anomalies information for a particular user in the **Top Risky Panel**, apply the user tag to the filter. Do one of the following to apply filters based on a risky user:

- Hover your cursor over the user tag and press **ctrl + tab**.
- Right-click the user tag and select **Open Link in New Tab**.

To add a new **Top Risky** panel:

- At the bottom of the page beside the leftmost panel, click the **+** symbol, select **Top Risky** and then select an entity type.

You can further explore the **Top Risky** entities by clicking an entity box to open the **Entity Details** panel.

To remove the panel:

- Click the **X** symbol at the top right of the panel.

Top Users To Trigger Violations Panel

On the **Explore** page, you can view the **Top Users To Trigger Violations**. This panel provides a table list of the top users who have triggered Workflow violations, sorted in descending order.

To add the **Top Users To Trigger Violations** panel:

- At the bottom of the page beside the leftmost panel, click the **+** symbol and then select **Top Users To Trigger Violations**.

To remove the panel:

- Click the **X** symbol at the top right of the panel.

Exploring Raw Events

When you click an item in the **Anomalies & Violations** panel, a dialog box appears that provides additional context about the anomaly or violation. To see the events that triggered the risky activity, in the top right of the dialog box, click **View Events** -> **Explore Raw Events**. This launches a pre-populated query in Event Viewer, where you can further explore the events.

Event Viewer provides security practitioners with a quick way to explore the context around the raw events that triggered the anomaly. This can include expanding the time range, changing filter options, or any other grid oriented data.

Note: When Using the **Event** option to explore raw events through the **Event Viewer**, you can build your own custom query and save it. Click **Type to filter raw events** to create queries through the **Query Editor**. You can also edit an existing query and save it. You can either click **SAVE** or use the **Ctrl/command + s** keyboard shortcut to save your query. To enable saving of queries, contact Micro Focus Customer Support at https://softwaresupport.softwaregrp.com/, as this involves modifications to investigator.yml.

Exporting Intelligence Reports

You can export reports that provide you with further insight into risky entities and their behaviors. With the help of reports, you can investigate the Intelligence Analytics results and take appropriate action immediately.

- CSV Reports
- PDF Reports

CSV Reports

CSV reports provide you with the raw data of the **Anomalies & Violations**. A CSV Report can provide you with further insight on how an entity is behaving. For example, a user entity CSV Report may contain information regarding country of origin, actions taken, username and object type. To download a CSV report, click on the **Events** option and then, click on the **CSV symbol** next to the date, this will automatically download the CSV Report. The CSV Report can contain up to 10,000 records.

PDF Reports

After an investigation has sufficient evidence to warrant an escalation, information can be exported to a PDF format so that incident response can begin immediately. To generate a PDF report for your organizational risk, on the **Entity Risk** page, next to the date at the top of the page, click the PDF icon. To generate a report for a user entity, from the **Explore** page, click a user entity name to open the **Entity Details** panel, and then click the PDF icon beside the entity name to download a PDF report. With this report, you can quickly share the findings of the investigation without having to manually create any additional documents. The report helps provide an understanding of what constitutes a risky and an abnormal behavior for any entity.

Advanced Features

In the Intelligence user interface, you can take advantage of a number of advanced features that allow you to manage the security of your organization more effectively. For example, you can work with a user with Admin role to manage bots and bot-like users. For more information, see Managing Bots and Bot-like Users.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on ArcSight Intelligence SaaS 6.4.5 User's Guide

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to Documentation-Feedback@microfocus.com.

We appreciate your feedback!