Micro Focus Security
ArcSight Intelligence

Software Version: 2022.1.1

ArcSight Intelligence SaaS 2022.1.1 Administrator's and User's Guide

Document Release Date: 1/28/2022
Software Release Date: 1/28/2022

Legal Notices

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

https://www.microfocus.com/en-us/legal

Copyright Notice

Trademark Notices

Documentation Updates

The title page of this document home page of this Help 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

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 2022.1.1 Administrator's and User's Guide (Intelligence 2022.1.1)

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 cyberressuport@microfocus.com.

We appreciate your feedback!

Support

Contact Information

Email	cyberressuport@microfocus.com
Support Web Site	https://support.cyberreshelp.com

Contents

Copyright Notice 3

Trademark Notices 3

Documentation Updates 3

Send Documentation Feedback 4

Support 4

Contents 5

Introduction 7

Supported Environments 7

Intended Audience 7

About ArcSight Intelligence 8

Administering ArcSight Intelligence for End Users 9

Modifying ArcSight Intelligence Analytics Configuration 9

User Roles 9

Enabling Windowed Analytics 10

Managing Bots and Bot-like Users 10

Tuning the Analytics 11

DID-Separation Configuration 13

For CrowdStrike 13

Other Users 13

Understanding Users and Other Entities in ArcSight Intelligence 14

Entities, Behaviors, and Risk Accumulation 14

Behaviors 14

Accumulating Risk 15

Understanding the ArcSight Intelligence Dashboard 16

Exploring the Overall Risk Page 16

Exploring the Entities Page 17

Manage User-Defined Tags for Entities 18

Exploring the Explore Page 19

Matrix of Anomalies & Violations 20

Contribution to Risk by Threat 21

Top Risky Panel 21

Anomalies & Violations Panel 22

Entity Details Panel 22

Create User-defined Tags for an Entity 23

Apply Filters to Entity and Anomaly Data 23

Apply Anomaly and Violation Flags 24

Add Comments to an Anomaly or Violation 26

Authentications Panel 26

Most Accessed Panel 27

Top Users To Trigger Violations Panel 27

Exploring Raw Events 27

Viewing Reports 29

CSV Reports 29

PDF Reports 29

Advanced Features 30

Introduction

This guide describes how to administer and use ArcSight Intelligence SaaS 2022.1.1. It also provides an overview of the ArcSight Intelligence cluster requirements, dependencies, components, and best practices.

ArcSight Intelligence uses data science and advanced analytics to identify the top risky entities and behaviors occurring in your organization. Using your organization's data, ArcSight Intelligence establishes the *normal* behavior for your organizational entities and then, using advanced analytics, identifies the *anomalous* behaviors that constitute potential risks such as compromised accounts, insider threats, or other cyber threats.

ArcSight Intelligence's innovative user experience, true machine learning, and big data platform easily identify and prioritize high risk anomalies, allowing your security practitioners to explore the underlying raw event data instantly. In addition, the ArcSight Intelligence analytical models apply risk scores to individual users to provide security teams with relevant, prioritized information quickly enough to stop the activity before data loss occurs.

Supported Environments

ArcSight Intelligence SaaS supports the following Web browsers:

- Google Chrome
- Mozilla Firefox
- Microsoft Edge

Intended Audience

This guide assumes that you are an experienced system administrator with sound Linux skills and are familiar with your organization's server environment, security infrastructure, and data sources. You should also be familiar with the business needs of your organization.

About ArcSight Intelligence

With increasing threats to the IT ecosystem, IT organizations need to continuously find better and effective ways to monitor and secure their enterprise networks. In today’s world, employees can access company data and applications from within the company, home, and even using personal mobile devices regardless of geographic location. With IT organizations managing their assets both on-premises and in the cloud, it is increasingly challenging for IT security teams to detect malicious activities by internal users, intentional or accidental, such as data theft, data exfiltration, and account compromise.

Most security information and event management (SIEM) solutions, such as Micro Focus ArcSight Enterprise Security Manager (ESM), offer security and compliance monitoring solutions that focus primarily on external threats. However, IT organizations need solutions that also perform in-depth user behavior monitoring to detect anomalies and potential threats within the organization. Users with valid credentials carry out most data loss and data breach activities.

ArcSight Intelligence is a user and entity behavioral analytics solution that uses data science and advanced analytics to identify your organization's top risky entities and behaviors. Using your organization's data, ArcSight Intelligence first establishes the *normal* behavior for your organizational entities. Then, using advanced analytics, identifies the *anomalous* behaviors that constitute potential risks, such as compromised accounts, insider threats, or other cyber threats.

ArcSight Intelligence detects, analyzes, and identifies potential threats by:

- Using unsupervised machine learning techniques to define user profiles and baselines automatically
- Actively monitoring account access patterns and actions on the associated entities against defined baselines to detect anomalies
- Applying risk scores for each entity based on the anomalies detected
- Displaying 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

As a result, ArcSight Intelligence significantly decreases the number of undetected threats and increases a Security Analyst's ability to investigate the detected anomalies quickly and efficiently.

Administering ArcSight Intelligence for End Users

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

These tasks include:

- Modifying ArcSight Intelligence Analytics Configuration
- Enabling Windowed Analytics
- Managing Bots and Bot-like Users
- Tuning the Analytics
- DID-Separation Configuration

Modifying ArcSight Intelligence Analytics Configuration

ArcSight Intelligence runs Analytics according to the Analytics configuration properties set during deployment. However, the Analytics configurations, such as enabling Analytics to run on newly ingested data and scheduling when Analytics is run can be modified. Analytics can also be run on demand. For more information on modifying the ArcSight Intelligence Analytics Configuration and running Analytics on demand, contact Micro Focus ArcSight Intelligence support.

User Roles

Two user roles exist in Arcsight 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, contact Micro Focus Customer Support at cyberressupport@microfocus.com.

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

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

Enabling Windowed Analytics

By default, ArcSight Intelligence is configured to run Analytics in batch mode. When new data is ingested, Analytics is run on both the new and the existing data. Although this process is beneficial when you first deploy ArcSight Intelligence (for testing and validation purposes), running Analytics on the entirety of your data on an ongoing basis unnecessarily uses system resources. Instead, Windowed Analytics can be enabled.

> **Note:** For ArcSight Intelligence SaaS environments Windowed Analytics can only be enabled by a member of the support team. For assistance, contact Micro Focus Customer Support at cyberressupport@microfocus.com.

When Windowed Analytics is enabled, ArcSight Intelligence runs Analytics only on newly ingested data as determined by the date of the last Analytics run and the timestamp of the data. ArcSight Intelligence identifies the data it has already analyzed, and then runs Analytics only on the new data. These results are then aggregated with the existing results to produce updated, current Analytics results for the entire data set.

Windowed Analytics has a positive impact on performance and stability because it allows the system to analyze and aggregate smaller, more consistently sized quantities of data than batch mode, particularly as the total amount of data in your system continues to grow.

Managing Bots and Bot-like Users

Internet bots, or web robots, are software applications that run automated tasks. If your organization has system bot activity, this activity — because of the exceptional speed with which the activity occurs — can generate Risky Hours in your Analytics. identifies those system users it deems to be bots, and strips them from the **Matrix of Anomalies & Violations**.

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

To manage bots and bot-like users:

1. Click **Settings** ⚙, then select **Tuning API** from the drop-down list to open the API in Swagger.

3. Expand the **Entity Tags** section.

4. Click the **PUT /interset/tuning/{tid}/entity_tags/{ds}/{did}/{type}/{identifier}/{tag}** row.

5. Click **Try it out!** to enable the new entity tag.

6. Under **Parameters**, provide 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**, specify **users**.
   - For the **identifier**, specify the username, or ID, for the user
   - For the **tag**, do one of the following
     - If the entity is currently a user shown in the Analytics and you want to tag this entity as a bot, type **FORCEBOT**.
     - If the entity is currently shown as a bot in the PDF Report and you want to tag this entity as a user, type **NOTBOT**.

7. In the text box provided for the body parameter, specify the value for the desired field.

8. Click **Execute** to enable the new entity tag.

> **Note:** To ensure that the user **indentifier** is accurate, get this ID from the **Explore** page (if currently a user shown in the Analytics) or from the PDF Report (if currently reported as a bot).

Tuning the Analytics

After you have had the opportunity to explore the Analytics and investigate the leads identified in the 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 user interface.

To tune Analytics:

1. In a Web browser, log in to as a user with an Admin role.
2. Click **Settings** ⚙, then select **Anomalies** from 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**, 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. strongly recommends that you avoid changing any anomaly weight unless instructed to do so by Micro Focus support representative.
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**.

DID-Separation Configuration

DID separation configuration can be customized for your cluster, but please follow the guidelines below to do so:

For CrowdStrike

1. For regular CrowdStrike data with no customization, use the default CrowdStrike DID configurations.
2. Make sure that you are using the appropriate DID-separation configuration that is included with the version of normalizer/analytics.

Other Users

For any customization please contact Micro Focus support representative for further help.

Understanding Users and Other Entities in ArcSight Intelligence

ArcSight 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 ArcSight Intelligence models are true advanced behavioral models: they do not 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. This approach leads to a continuous, prioritized list of risks, and helps improve the efficiency of IT security teams and their tools.

Using ArcSight Intelligence machine learning models means that additional configuration is not required for the analytical models to execute. Through observation, ArcSight Intelligence learns what constitutes normal behavior for the entities in your organization, and immediately begins to quantify abnormal behavior. There are no thresholds to set, no rules to author, and no configurations to undertake.

ArcSight Intelligence displays the results of ArcSight Intelligence Analytics in an interface that provides actionable information on current risk along with flexible multi-entity historical data exploration.

Entities, Behaviors, and Risk Accumulation

Entities are the foundation of ArcSight 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.

As behaviors occur, ArcSight Intelligence processes these events and calculates that which is normal from dozens of behavioral perspectives. For example, ArcSight 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.

Accumulating Risk

As new observed behaviors occur, ArcSight Intelligence determines if the behaviors are normal or unusual. When unusual, ArcSight 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.

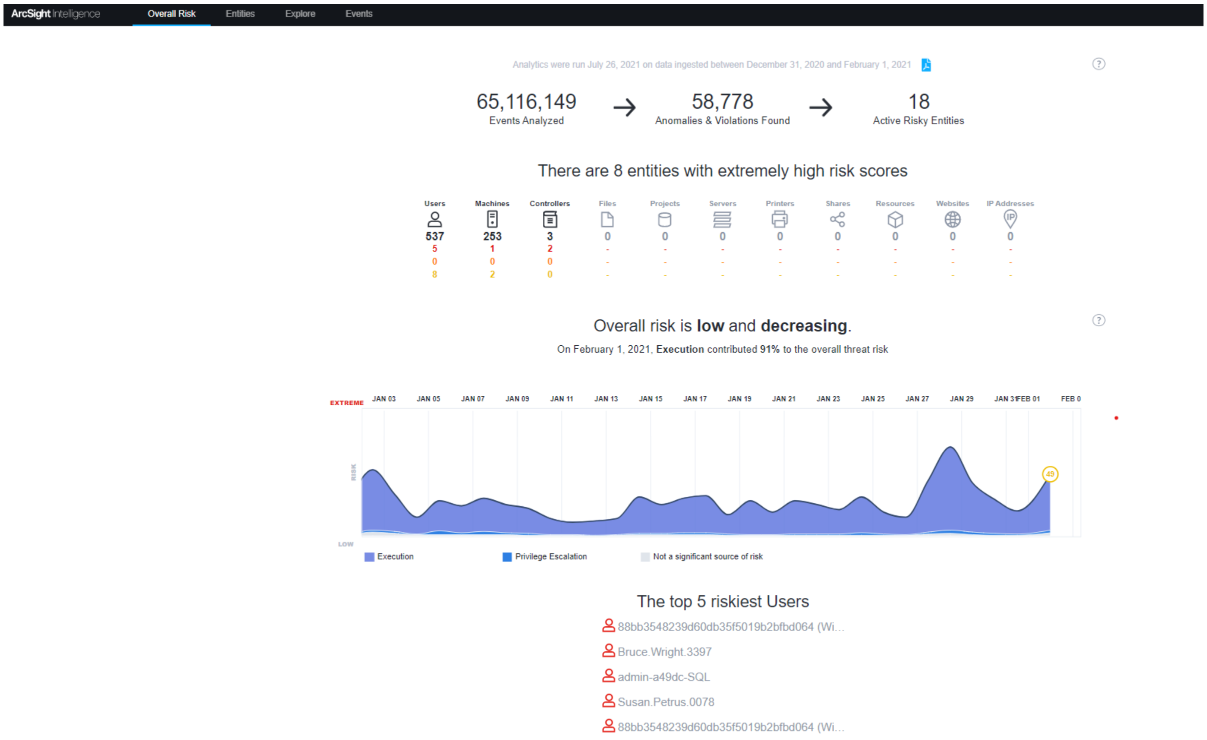
Understanding the ArcSight Intelligence Dashboard

The ArcSight 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 ArcSight 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.

- Exploring the Overall Risk Page
- Exploring the Entities Page
- Exploring the Explore Page
- Exploring Raw Events

Exploring the Overall Risk Page

When you first log in to ArcSight Intelligence, the **Overall Risk** page is displayed. This page summarizes the overall risk status of your organization. For example, in the following screen shot you immediately see that:



Analytics were run July 26, 2021 on data ingested between December 31, 2020 and February 1, 2021

65,116,149 Events Analyzed → 58,778 Anomalies & Violations Found → 18 Active Risky Entities

There are 8 entities with extremely high risk scores

Users	Machines	Controllers	Files	Projects	Servers	Printers	Shares	Resources	Websites	IP Addresses
537	253	3	0	0	0	0	0	0	0	0
5	1	2	-	-	-	-	-	-	-	-
0	0	0	-	-	-	-	-	-	-	-
8	2	0	-	-	-	-	-	-	-	-

Overall risk is **low** and **decreasing**.

On February 1, 2021, **Execution** contributed **91%** to the overall threat risk

The top 5 riskiest Users

- 88bb3548239d60db35f5019b2bfbd064 (Wi...
- Bruce.Wright.3397
- admin-a49dc-SQL
- Susan.Petrus.0078
- 88bb3548239d60db35f5019b2bfbd064 (Wi...

- Over 65 million events were analyzed
- About 59 thousand anomalies and violations were found
- 18 active risky entities were identified
- The overall risk is low and increasing decreasing
- The stream 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 provides the trending information, the entity name, the potential threat type, and the most relevant anomaly identified by ArcSight Intelligence. Potential threat types are determined by the most relevant risky activity in the system.

At the top of the **Entities** page, you can click on the different entity icons to filter the riskiest entities grouped by type, such as **Users**, **Projects** or **Controllers**. Icons in black represent entities that are present in the data. Icons in gray represent any entities that are not currently present in the data. A blue icon indicates that the entities are filtered by the selected entity type. Typically, you explore the Users entity 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 ArcSight 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 ArcSight 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 appears as **Potential Lateral Movement**, and a summarized description of the anomaly is 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.

From the Entities page, you can:

- Filter the entity data. See Apply Filters to Entity and Anomaly Data
- Associate user-defined tags to the entities. See Manage User-Defined Tags for Entities

To explore a risky entity in further detail, click the anomaly or violation to open the Explore page, which is filtered by the selected entity and threat.

Manage User-Defined Tags for Entities

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

You can access the Explore page two ways; by selecting the **Explore** menu option, or by selecting an entity on the **Overall Risk** or **Entities** pages.

When you access the Explore page from the Explore menu, you view all anomalies and violations for all the entities in you environment for the selected date and time range.

When you click on an entity, the Explore page displays, where the entity's name is filtered and all the anomalies and violations associated with the selected 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. If you click on a specific entity, the **Entity Details** Panel is displayed on the left side of the Explore page.

For more details on each page element, see the following sections:

- Matrix of Anomalies & Violations
- Contribution to Risk by Threat
- Top Risky Panel
- Anomalies & Violations Panel
- Entity Details Panel

From the Explore page, you can perform the following actions to better track and filter anomalies and violations:

- Apply Filters to Entity and Anomaly Data
- Apply Anomaly and Violation Flags
- Add Comments to an Anomaly or Violation

You can also view additional panels on the Explore page:

- Authentications Panel
- Most Accessed Panel
- Top Users To Trigger Violations Panel

To add these panels to the Explore page, click the **+** icon on the left side of the page and select the panel that you want to display. To remove a panel, select the **x** icon on the panel.

Matrix of Anomalies & Violations

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

You can perform the following actions from the **Matrix of Anomalies & Violations**:

- Set the time window to reflect a time period of specific interest. Choose the one of following time periods: **24 Hours**, **7 Days**, **30 Days**, **Year**, or set the time period to include **All Data**.
- To zoom in or out, or pan across 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.
- Filter the anomalies and violations:
    - Use the slider to the left of the matrix to filter based on risk level to reduce the number of alerts displayed. You can also click the **Risk** squares in the legend below the graph to set the slider filter to that risk level. For example, if you want to view **Medium Risk** and above, click the yellow **Medium Risk** square. This filters out all low risk alerts, as shown in the example below.
    - Use the search filter labeled **Type to filter anomalies and violations...** located above the Matrix of Anomalies & Violations to choose a filter from the dropdown menu, or search for filters by typing a filter name. Depending on your data set, you can apply filters on many aspects of your data, including **Users**, **Entity Types**, **Projects**, **Controllers**, and **User-defined tags**. See Apply Filters to Entity and Anomaly Data.
    - Select an entity in the **Anomalies & Violations** panel to filter the alerts In the **Matrix of Anomalies & Violations** timeline.

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

The **Contribution to Risk by Threat** graph organizes and displays potential threat types by their percentage of overall risk. This graph is hidden by default. To reveal/hide the **Contribution to Risk by Threat** graph, click the **Contribution to Risk by Threat** heading.

You can filter the graph by threat type by selecting the threat type name or square in the graph legend. 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. Filtering the **Contribution to Risk by Threat** graph, also filters the information displayed in the **Matrix of Anomalies & Violations** and in the **Anomalies & Violations** 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 ArcSight 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.

Anomalies & Violations Panel

The **Anomalies & Violations** panel displays triggered activities in the form of a list. Each anomaly and violation has a time stamp, risk color, description, potential threat type, and associated entities attached to it.

If an anomaly or violation has already been viewed, a Viewed by flag 👁 is visible beside the item in the list. When you hover your cursor over this flag, the username of the threat hunter who has already seen or investigated the anomaly details is displayed.

> **Tip:** You can filter anomalies and violations by the Viewed by flag on the Explore page to see all of the items viewed by either yourself or another threat hunter.

The **Anomalies & Violations** list can be sorted by **Time** (default) or by **Risk**. 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 remove 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 events that triggered the **Anomaly** or **Violation**. For more information on exploring raw events, see Exploring Raw Events.

Entity Details Panel

When you select an entity, the **Entity Details** panel opens. This panel contains additional information on the selected entity. If you select a **User** entity, for example, the **Entity Details** panel displays 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.

From the Entity Details panel, you can do the following:

- Download a PDF report on the entity. Click the PDF icon beside the entity name to generate the report.
- Create and apply user-defined tags. See Create User-defined Tags for an Entity.
- Add notes about the entity.

Create User-defined Tags for an Entity

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.

Apply 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**, 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.

Apply Anomaly and Violation Flags

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

⚠ 🔥 📍 ☆ 💼 ✓

These flags have no established definitions; as a result, your organization can determine the appropriate meaning for each of the symbols 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:

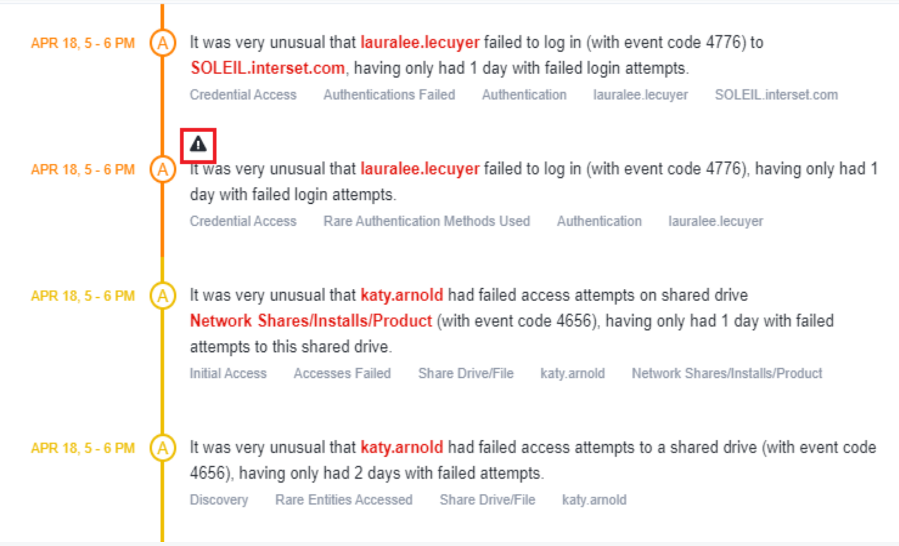
1. In the **Anomalies & Violations** panel, click in an anomaly for which you want to set a flag.
   The anomaly opens, displaying the flags in the upper left corner.

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.



APR 18, 5 - 6 PM A It was very unusual that lauralee.lecuyer failed to log in (with event code 4776) to SOLEIL.interset.com, having only had 1 day with failed login attempts.
Credential Access Authentications Failed Authentication lauralee.lecuyer SOLEIL.interset.com

⚠

APR 18, 5 - 6 PM A It was very unusual that lauralee.lecuyer failed to log in (with event code 4776), having only had 1 day with failed login attempts.
Credential Access Rare Authentication Methods Used Authentication lauralee.lecuyer

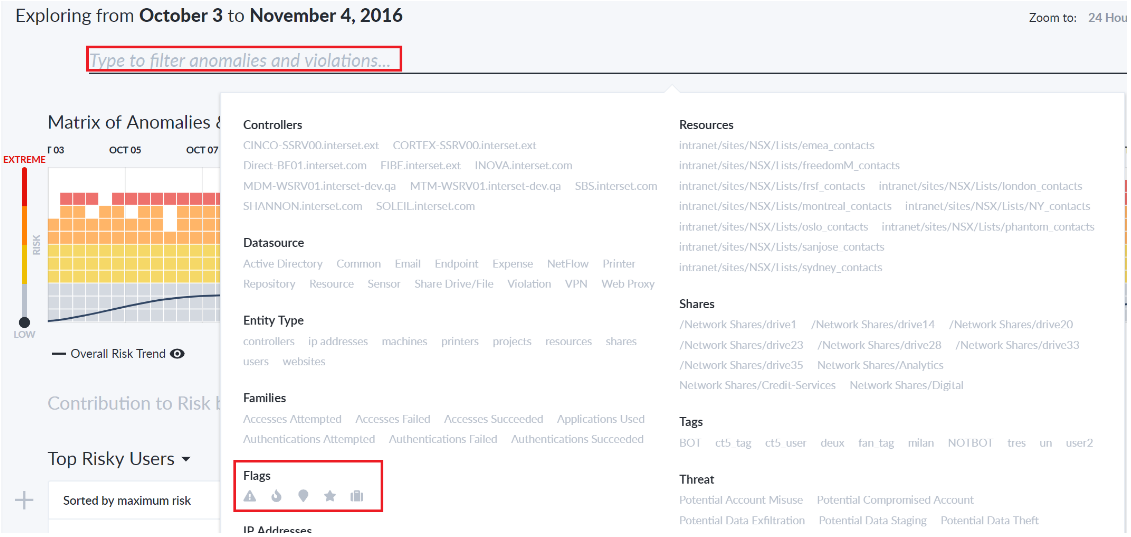
APR 18, 5 - 6 PM A It was very unusual that katy.arnold had failed access attempts on shared drive Network Shares/Installs/Product (with event code 4656), having only had 1 day with failed attempts to this shared drive.
Initial Access Accesses Failed Share Drive/File katy.arnold Network Shares/Installs/Product

APR 18, 5 - 6 PM A It was very unusual that katy.arnold had failed access attempts to a shared drive (with event code 4656), having only had 2 days with failed attempts.
Discovery Rare Entities Accessed Share Drive/File katy.arnold

- 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.



Exploring from **October 3** to **November 4, 2016**

Zoom to: 24 Hou

Type to filter anomalies and violations...

Controllers
CINCO-SSRV00.interset.ext CORTEX-SSRV00.interset.ext Direct-BE01.interset.com FIBE.interset.ext INOVA.interset.com MDM-WSRV01.interset-dev.qa MTM-WSRV01.interset-dev.qa SBS.interset.com SHANNON.interset.com SOLEIL.interset.com

Datasource
Active Directory Common Email Endpoint Expense NetFlow Printer Repository Resource Sensor Share Drive/File Violation VPN Web Proxy

Entity Type
controllers ip addresses machines printers projects resources shares users websites

Families
Accesses Attempted Accesses Failed Accesses Succeeded Applications Used Authentications Attempted Authentications Failed Authentications Succeeded

Flags
⚠ 🔥 ● ★ 💼

IP Addresses

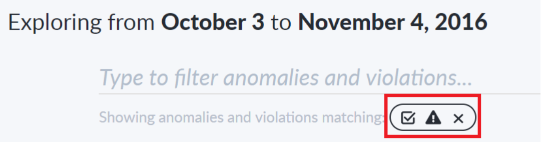
Resources
intranet/sites/NSX/Lists/emea_contacts
intranet/sites/NSX/Lists/freedomM_contacts
intranet/sites/NSX/Lists/frsf_contacts intranet/sites/NSX/Lists/london_contacts
intranet/sites/NSX/Lists/montreal_contacts intranet/sites/NSX/Lists/NY_contacts
intranet/sites/NSX/Lists/oslo_contacts intranet/sites/NSX/Lists/phantom_contacts
intranet/sites/NSX/Lists/sanjose_contacts
intranet/sites/NSX/Lists/sydney_contacts

Shares
/Network Shares/drive1 /Network Shares/drive14 /Network Shares/drive20 /Network Shares/drive23 /Network Shares/drive28 /Network Shares/drive33 /Network Shares/drive35 Network Shares/Analytics Network Shares/Credit-Services Network Shares/Digital

Tags
BOT ct5_tag ct5_user deux fan_tag milan NOTBOT tres un user2

Threat
Potential Account Misuse Potential Compromised Account Potential Data Exfiltration Potential Data Staging Potential Data Theft

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.



Exploring from **October 3** to **November 4, 2016**

Type to filter anomalies and violations...

Showing anomalies and violations matching ☑ ⚠ ×

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.

Add 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.

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; either Machines or Application.

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 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 **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 on **Type to filter raw events** to create queries through the **Query Editor** . To enable saving of queries, contact Micro Focus Customer Support at cyberressuport@microfocus.com, as this involves modifications to investigator.yml.

Viewing Reports

You can view reports that provide you with further insight into risky entities and their behaviors. With the help of reports, you can investigate the ArcSight 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 **Overall 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 ArcSight 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.