Risk Service 2.0
Administration Guide

September 2020

Legal Notice

Contents

About This Book

This guide includes an overview of Risk Service, basic scenarios, and step-by-step guidance for common tasks.

Intended Audience

This book provides information for individuals responsible for configuring and managing Identity and Access Management solution.

For the most recent version of this guide, visit the Risk Service Documentation website (https://www.netiq.com/documentation/risk-service/).

Contact Information

We want to hear your comments and suggestions about documentation. You can use the **comment on this topic** link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

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

1 Introduction to Risk Service

Risk Service evaluates the risk level during each access attempts using the contextual information without influencing the end-user experience. For example, the contextual information can be IP address and device information. This enhances the authentication and access processes, user governance, and prevents fraudulent access to the secured web application or network.

Risk Service uses deterministic, rule-based computation. It enables organizations to find threats quickly with known attack patterns and take appropriate actions. You can integrate your access management solution with Risk Service to assess the risk based on the contextual information associated with an access attempt. You can define an appropriate action for each risk level. For example, granting access or asking for additional authentication.

To enable the unknown threat or anomaly detection, Risk Service integrates with ArcSight Intelligence (formerly Interset) to leverage its User and Entity Behavioral Analytics (UEBA) capability. Using the organization's data, Interset establishes the normal behavior for the organizational entities and then, using advanced analytics and machine learning, identifies the anomalous behaviors that constitute potential risks such as compromised accounts, insider threats, or other unknown cyber threats.

For more information about UEBA and its integration with Risk Service, see the following resources:

- User and Entity Behavioral Analytics
- ArcSight Intelligence
- Enabling Behavioral Analytics Using Interset for Access Manager
- Enabling Behavioral Analytics Using Interset for Advanced Authentication

In this section:

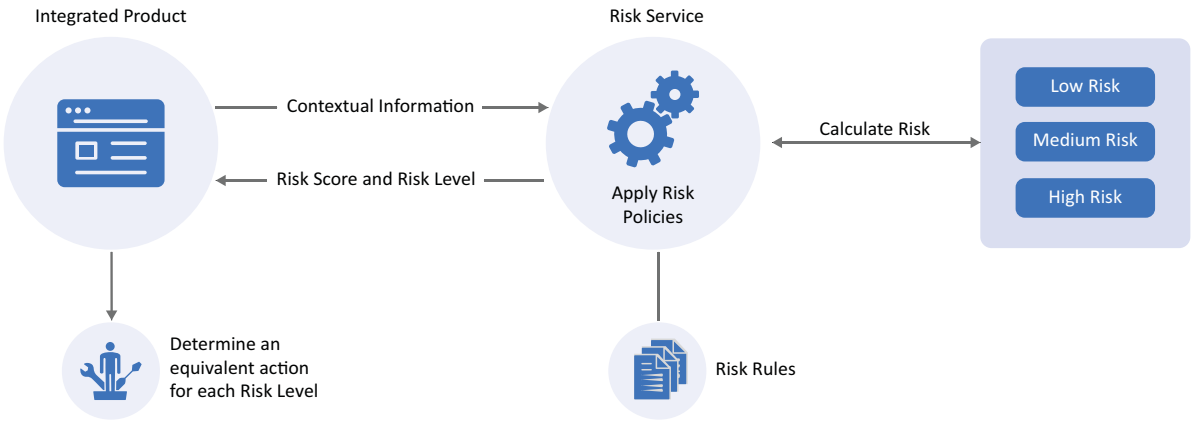
Risk Service Key Terms

Term	Description
Rule	A rule indicates a condition that you want to evaluate the risk associated with each login attempt. For evaluation, a rule is assigned to a risk policy. You can assign a single rule to multiple risk policies. You can combine multiple rules in a risk policy.
Risk Policy	A risk policy is a group of risk rules. Ensure to assign a rule to a risk policy for the evaluation process. You can combine multiple rules in a risk policy.

Term	Description
Risk Score	The value that is returned when the rule condition is not met. By default, a user's risk score increases by 100 for each failed rule condition. The higher the score, the higher is the risk. In the advanced mode, you can fine-tune the risk assessment by changing the risk score of a rule from 100 to another value. This helps you alter the weightage of that rule compared to other rules in the policy.
Is/Is Not condition	When you configure a rule and select a parameter for assessment, you can determine how the conditions must match for each of the sub-parameters. For example, if you configure a rule to assess the IP address of a user, you can configure whether the IP address must be specific, be in a range, or be in a particular subnet. If you want to assess whether the IP address of a user is within a range of 10.10.10.1 to 10.10.10.10, you can specify the `Is` condition in the rule configuration. This indicates that when the rule is evaluated, only IP addresses in the range of 10.10.10.1 to 10.10.10.10 will be considered as a valid IP addresses. During the rule evaluation, if you want a rule to be passed when it does not meet a specific criteria, select `Is Not` in the rule configuration screen. For example, if you want to stop all login attempts from a particular IP address, configure the rule using the `Is Not` condition.
Risk Level	A risk level indicates the status of each login attempt that the risk service returns after comparing the parameters associated with each attempt against the defined rules in a policy. You can configure the risk level based on the number of rules that failed during evaluation. The available risk levels are low, medium, and high. For example, define a policy with three rules and set the risk level as follows: ◆ **Low**: if one rule fails in the evaluation process ◆ **Medium**: if two rules fail in the evaluation process ◆ **High**: if all the configured rules fail For each risk level, you can define a subsequent action.
Action If Condition Succeeds	When a policy contains more than one rule, you can make a specific rule as a decisive rule and define an action if that rule condition succeeds. Actions available are: ◆ **Allow Access** ◆ **Deny Access** ◆ **Proceed with next rule** For example, a policy contains IP Address Rule and User Last Login Rule. You want the policy to evaluate the IP address Rule first. If the rule meets the condition, allow access without validating another rule in the policy. To promote the IP Address Rule as the decisive rule, select the IP Address Rule, click the Rule Action icon, and select **Allow Access**. Risk Service executes the IP Address Rule first. If the rule meets the defined condition, the User Last Login Rule is not executed.

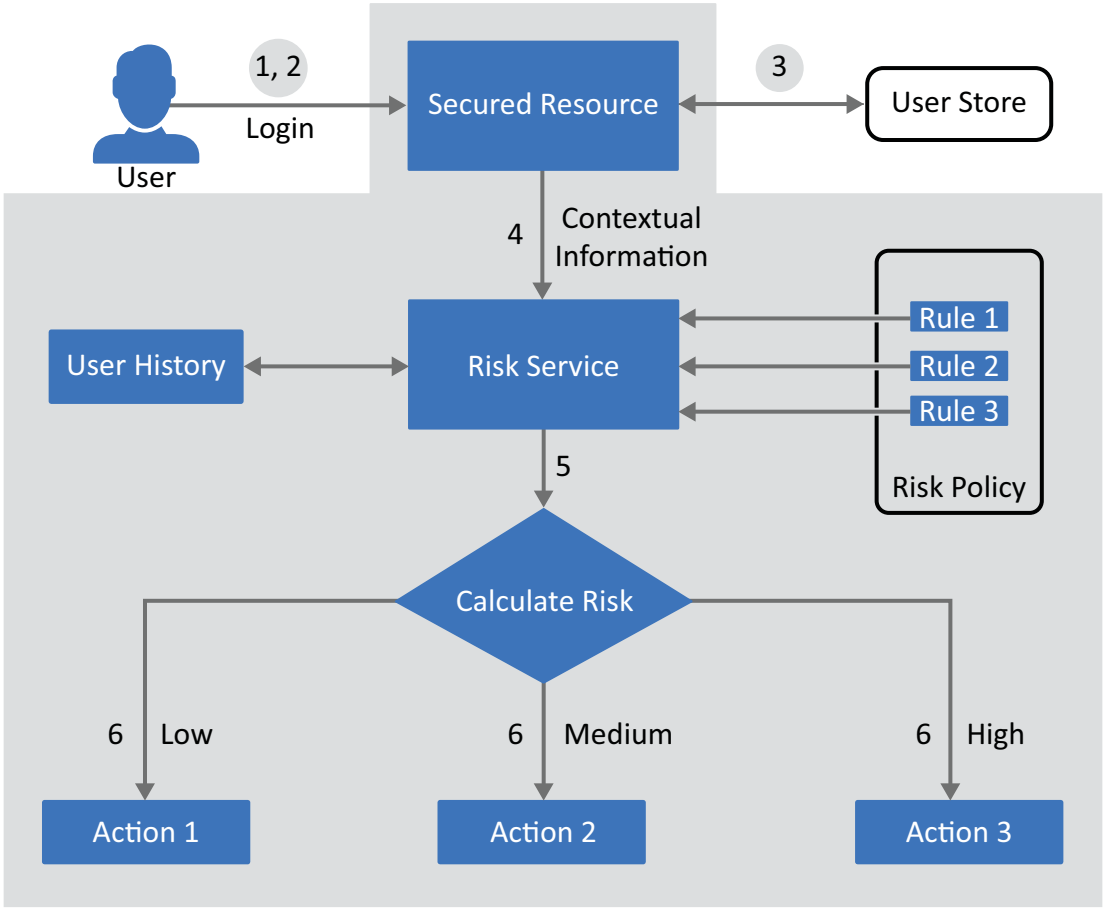
How It Works

The following illustration depicts the Risk Service process:



For information about Risk Rules, see Table 2-1, “Risk Rules,” on page 13.

The following diagram illustrates the basic flow of authentication using Risk Service:



1. A user tries to log in to a web application.
2. The user specifies login credentials.
3. The integrated access management solution identifies the user.

4. The integrated access management solution provides the contextual data to Risk Service.
5. Risk Service calculates the risk level based on the defined set of rules and returns one of the following risk levels:
    - Low
    - Medium
    - High
6. The administrator configures appropriate action (authentication chains) based on the risk level.

Benefits of Risk Service

Risk Service enables you to accomplish the following goals:

- Enhance the security of a web application or network by reducing and preventing fraudulent access.
- Assess the risk level based on different parameters and users' behavioral patterns (for example, browser type, time of login).
- Improve user experience. Users need to provide additional details for authentication only when the associated risk prevails.

2 Configuring Risk Service

2.1 Configuring a Risk Policy

A risk policy includes one or more risk rules. Risk Service uses a risk policy to evaluate the risk based on the rules assigned to that policy. A rule contains a condition for which you want to evaluate the risk associated with each login attempt.

Before configuring a risk policy, determine the following details:

- The web application or network you want to secure.
- The parameters you want to assess during a login attempt.
- (Advanced setting) The risk score for each parameter.
- Whether you want to record the details of the risk assessment.
- Identify the database to store details of the risk assessment.

Steps to Configure a Risk Policy

1. Click the **Create a Risk Policy** icon.
2. Specify the following details:
   - **Policy Name**: Specify a name for the policy.
   - **Policy Description**: Describe the purpose of this policy.
3. Assign risk rules.

   You can select a rule from the existing list or create a new rule. You can assign multiple rules to a policy. The rules are executed in the top to bottom sequence. You can drag and drop to change the priority and sequence of rules.

   3a Click the **Add Rule** icon.

   3b Click one of the following options:
   - Click **Add New Rule** to create a new rule. For details, see Configuring Risk Rules.
   - Click **Add Existing Rule** to select one or more rules from the **Rule Selection** window.

   3c (Optional) You can configure a specific rule as a decisive rule and define an action if that rule condition is met.

Click the **Rule Actions** (⋮) icon of the rule and configure the action. You can configure one of the following actions for a rule:

- **Allow Access**: If the rule succeeds, the risk level is Low, other rules in the policy are not executed.
- **Deny Access**: If the rule fails, the risk level is High, other rules in the policy are not executed. A message, `Access has been denied` is displayed and the user is denied access to the resource.
- **Proceed with next rule**: The next rule in the policy is executed irrespective of whether this rule succeeds or fails.

For more information, see "**Action If Condition Succeeds" on page 8**.

IMPORTANT: If you have configured **Deny Access** as **Rule Actions** for the rule, you must set the score as `0` for this rule in **Advanced Mode**. This ensures that the risk score is not accumulated for low-risk and medium-risk Interset users.

For information about configuring risk scores, see Configuring Advanced Settings for a Risk Policy.

---

4 Configure the risk levels.

You can define risk levels according to the number of failed rules in the policy. Numeric values that display below the slider represent the number of rules that are assigned to the policy.

4a Move the blue slider and set the preferred number of rules to signify a medium-risk level.

4b Move the green slider and set the preferred number of rules to signify a low-risk level.

NOTE: The red segment indicates a high risk-level.

For example, let us assume the policy contains three rules and you want to accomplish the following configuration:

Failed Rules	Risk Level
0	Low
1	Medium
2 or 3	High

Set the blue slider to 1 and the green slider to 0 values respectively.

5 Click **Save**.

6 (Optional) Set the risk scores for rules. For details, see Configuring Advanced Settings for a Risk Policy.

Configuring Advanced Settings for a Risk Policy

After configuring a risk policy, you can configure risk score for each rule in that policy. This risk score indicates the priority and criticality of the rule.

For example, you have configured a set of rules in a risk policy. You want one of these rules to be the most important rule. To achieve this, assign that rule a higher risk score compared to other rules. If the rule evaluation is successful, the risk score is set as zero.

If a rule evaluation is not successful, the risk score is set as the value of the rule. If you have configured multiple rules, the total risk score is the sum of risk scores of all the failed rules.

To configure the risk score, perform the following steps:

1. Open the risk policy for which you want to configure risk scores.
2. Click **Configuration** (⚙) icon > **Advanced Mode**.
3. Change the value in **Risk Score** for each rule as required.

   By default, the risk score for each rule is set to 100.

   You can define risk levels according to the risk score accumulated due to failed rules. Numeric values that display below the slider represent the total risk score for all rules.
4. Click **Save**.

2.2 Configuring Risk Rules

Table 2-1 *Risk Rules*

Rule	Description
Cookie Rule	Use this rule if you want to track login attempts from a browser-based application that has a specific cookie value or name. For example, you have a financial application and a user accessing this application has cookies stored on the browser. If the cookie has a specific value or name, the risk level is low. If the user's browser has no cookies stored, the risk level is high.
External Parameters Rule	Use this rule to consider inputs from external providers to evaluate the risk associated with an access attempt.
HTTP Header Rule	Use this rule to track the requests that contain a specific value in the HTTP header. For example, if you want to track HTTP requests containing the custom HTTP header information, you can define the action to be performed on the evaluation of this rule.
IP Address Rule	Use this rule to define a condition to track login attempts from an IP address, range of IP addresses, an IP subnet range, or a list of IP addresses from an external provider. For example, if you are aware that login attempts from a specific range of IP addresses are riskier, you can define a rule to watch for such login attempts. When a request originates from the specified IP address range, you can prompt for additional authentication.

Rule	Description
User Last Login Rule	This rule creates a cookie in the browser after successful additional authentication. Subsequent login verifies this cookie. Use this rule to define the duration for which the cookie is valid. When the cookie is expired, the user is prompted for additional authentication. For example, this rule can be used to evaluate if the user is logging in by using the same browser that was used earlier for a login attempt. You can define the risk level and request additional authentication, as necessary.
User Time of Login Rule	Use this rule to define a condition based on the user's attempts to log in within a specific duration. For example, if the usual login pattern for an employee is between 9 a.m. to 5 p.m., you can define a rule that takes action if the login pattern differs from the observed pattern.

To configure a rule, perform the following steps:

1. Click the **Risk Rules** () icon > plus icon.
2. Specify the rule name and the description.
3. Select the preferred type of rule from **Choose a Rule Type**.
4. Configure the following rules as required:

   Cookie Rule | External Parameters Rule | HTTP Header Rule

   IP Address Rule | User Last Login Rule | User Time of Login

   For description of these rules, see Table 2-1 on page 13.

Cookie Rule

1. Specify the name of the cookie.
2. Specify the value of the cookie. The different search criteria that you can use are **Is** and **Is Not**.
3. [Optional] If the cookie is not found, but you want to create a cookie after the user authenticates, select **Create cookie if the user authenticates successfully**.
   a. Specify the validity of the cookie in hours.
   b. Specify the path for the cookie.

IMPORTANT: A cookie is set when a user authenticates using second-factor authentication. The cookie is not created if the risk is low and the user authenticates using primary authentication method.

External Parameters Rule

1. Select **Negate Result** to reverse the result of the rule evaluation. For example, if this rule fetches authentication details of a request using a specific IP address, use **Negate Result** to make the rule to not consider inputs from that IP address.
2. Specify the URL of the external source to retrieve GET requests that return simple JSON responses.
   a. Select **Get parameters from an external source** and specify **Source URL**.
   b. Select **Authentication Type** for authenticating the external source URL.
   c. If you selected `Basic Authentication` in **Authentication Type**, specify **Username** and **Password** to access the specified external source.
   d. Specify the **Request Timeout** value. After the specified time, the request is expired.
   e. Select a **Request Method** that is accepted by the specified external source.
   f. Select request parameters.
3. Add the following details for a parameter set:
   a. Name of the parameter.
   b. Specify a regular expression if required. For example, an external source sends the following value for the Virtual IPv4 parameter:

      ```
      The Virtual IP address is 127.0.0.1
      ```

      To extract the IP address from this string, specify the following value:

      ```
      (?:(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)
      ```

      This expression extracts the IP address `127.0.0.1` from the string and uses it for evaluating the configured condition. For information about regular expression syntax, see the Javadoc for java.util.regex.Pattern.
   c. Select a relational or string operator to define a relationship between parameter and parameter value. For example, whether a parameter must contain the specified parameter value or it must not be equal to the specified value.
   d. Specify a parameter value for evaluation.
   e. Click **Add Parameter** to add more parameters in this parameter set.
4. (Conditional) Click **Add Parameter Set** to define additional parameter set.
5. For two or more parameter sets, specify how the conditions for parameters must match. The available options are **Or** and **And**.

HTTP Header Rule

1. Specify the HTTP header Name.
2. Specify the value that you want an HTTP header to include.

   For example, if you want to search for an HTTP header that includes the value NetIQ, you can use the search criterion **Equals**. Whereas, if you want to query for an HTTP header that does not include the value NetIQ, use **Does Not Contain**.

IP Address Rule

1. Specify the condition whether to allow login using the IP addresses in the list.
2. To manually add IP addresses, select **Manually enter the Datasource**. You can specify a single IP address, IP address range, IP address subnet, or upload a text file containing IP addresses. To specify IPv4 subnets, use the Classless Inter-Domain Routing (CIDR) notation.

   Click **Add to List**.

   Sample text format

   ```
   # Example IP List
   10.0.0.0
   172.16.0.0
   192.168.0.0
   ```

   Each entry in the text files must be on a separate line.
3. To consider the list of IP addresses provided by an external provider or an internal web service, select **Dynamically consume from the Datasource**.
   a. Specify **URL** of the provider.
   b. Specify **Connection Timeout.** After this time, an unresponsive connection is closed.
   c. Specify **Refresh Interval**. The connection will be refreshed at the specified interval.

   The external provider provides the list of IP addresses in text or JSON formats.

   Sample text format

   ```
   # Example IP List
   10.0.0.0
   172.16.0.0
   192.168.0.0
   ```

   Sample JSON format

   ```
   ["10.0.0.0","172.16.0.0","192.168.0.0"]
   ```
4. Specify how the conditions for the rule must match. The available options are **Is** and **Is Not**.
5. To validate the user history recorded in the database, select **Check user history**. You can use this option only when **Record user history** is enabled in the **User History** tab.

   IMPORTANT: You cannot specify the IP subnet in the IPv6 format. Instead, you can use the IP range condition and define it in the IPv6 format.

User Last Login Rule

1. Specify the name of the last login cookie.
2. Specify the path for the cookie.
3. Specify the validity of the cookie in days.
4. If you want the cookie to be secured by HTTPS, select **Secure Cookie**.
5. Specify the number of days the cookie can be accessed from the same device or system. This value must be less than the value in **Max Age**.
6. Specify the crypto key to encrypt the cookie.

IMPORTANT: The `User Last Login` cookie is set only when a user is authenticated by using second-factor authentication. This cookie is not created if the risk is assessed to be low and the user authenticates by using the primary authentication method.

User Time of Login

1. Select Is/Is not condition based on your requirements. This determines how the conditions for the rule must be matched.
2. Specify the date and time of the user login.

2.3 Enabling User History

You can enable recording user details for the IP Address rule.

1 Click **Risk Settings** > **Configuration** (⚙) icon > **User History Database**.

2 Select one of the following options under **Record Limit:**

- **Consider all historical records for a user**: To examine all historical records during the rule execution.
- **Consider historical records for a previous number of days**: To examine historical records of days as specified in **Number of days**.

3 Select one of the following **History Data Store** where you want to store details:

- **Built-in Data Store**: In a production environment, this option is not recommended to use.
- **External Database**: To store the session details in an external database, perform the following actions:

  1. Select the preferred **Database Type**. The following are available options:
     - Postgres
     - Others (Unsupported)

     The **Database Driver** and **Database Dialect** are auto-populated. You can change the driver and dialect details if required.
  2. Specify the administrator **Username** and **Password** to access the database.
  3. Specify the **Host URL** to access the database.

     To enable SSL communication to the database, append the following string in the URL:

     ```
     ?verifyServerCertificate=false&useSSL=true
     ```

For example, if the URL is `jdbc:postgresql://10.0.0.0:5432/riskdb`, it looks similar to the following after appending the string:

```
jdbc:postgresql://10.0.0.0:5432/
riskdb?verifyServerCertificate=false&useSSL=true
```

4 Click **Save**.

2.4 Configuring NAT Settings

You can configure Risk Service to retrieve IP addresses in a NAT environment.

1 On the Risk Settings page, click **Configuration** (⚙) icon > **NAT Settings**.

2 Select **Identity Server behind NAT**.

3 In **Client IP Header Name**, specify the header name of the field to fetch the IP address of a client. For example, `X-Forwarded-For`.

4 In **Client IP Header Parser**, specify the regular expression to retrieve the client's IP address from the HTTP header value. Header Parser is set as ".*" by default.

With the regular expression ".* ", the rule execution fails even if the client IP address exists in the list of multiple IP addresses. So, if you want to retrieve an IP address from a list of multiple IP addresses, modify the regular expression accordingly.

5 Click **Save**.

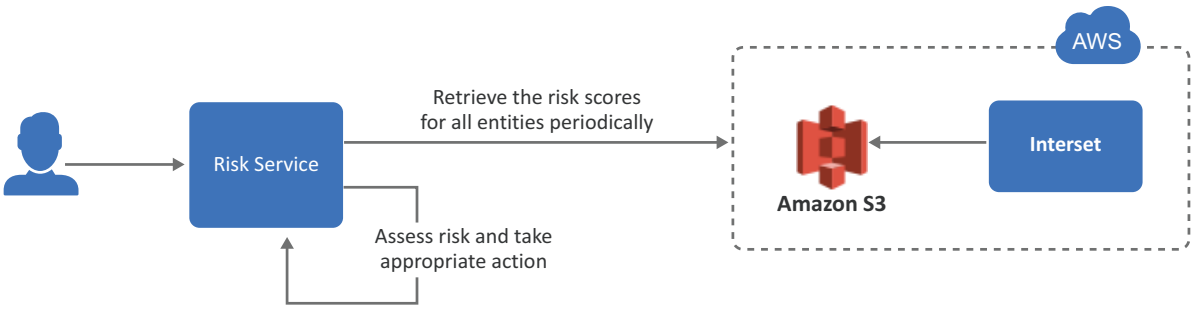
2.5 Configuring Behavioral Analytics

You can integrate Risk Service with Micro Focus Interset to leverage its User and Entity Behavioral Analytics (UEBA) capability. Using the organization's data, Interset establishes the normal behavior for the organizational entities. Interset then, using advanced analytics and machine learning, identifies the anomalous behaviors that constitute potential risks. For example, compromised accounts, insider threats, or other cyber threats.

How It Works

Risk Service periodically fetches risk scores for all entities from Interset and keeps the latest scores in the cache. While configuring Interset, you need to configure it to receive data from various applications used in your organization. Interset analyzes the behavior of entities and users using this data.

The following diagram illustrates how this integration works:



1. A user tries to log in to a protected resource.
2. Risk Service checks the behavioral risk score for this user in the risk score cache.

   Risk Service keeps retrieving the latest behavioral risk scores for all entities at a regular interval and updates the cache.
3. Risk Service assesses the score and takes appropriate action.

For more information about Interset UEBA, see User and Entity Behavioral Analytics.

For step-by-step details for integrating Risk Service with Interset, see the following resources:

- Enabling Behavioral Analytics Using Interset for Access Manager
- Enabling Behavioral Analytics Using Interset for Advanced Authentication

Prerequisites for Configuring Interset Details

Before you start configuration, ensure that you have the following information with you:

- ❒ An ArcSight Intelligence (formerly Interset) account on AWS is available. For more information, see ArcSight Intelligence.
- ❒ AWS S3 Interest URL from where you want to get the data
- ❒ AWS region name
- ❒ AWS access key and access secret required to access AWS S3 Interset URL

Configuring Interset Details

1 On the Risk Settings page, click **Configuration** (⚙) icon > **Behavioral Analytics**.

2 Select **Enable**.

3 Specify the following details:

Field	Description
Interset Data URL	The AWS S3 bucket URL from where you want to get the Interset data.
AWS Region	The AWS region where Interset is deployed.
Access Key ID	The AWS access key ID to access the Interset URL.
Secret Access Key	The AWS secret access key to access the Interset URL.
Update every	The interval for syncing the data from Interset. The recommended value is 360 minutes (sync four times a day).

NOTE: To prevent disruption of service, ensure that Access Key ID and Secret Access Key specified here are up to date when these are rotated as per AWS guidelines.

4 Click Save.

An external parameter rule is configured using the appropriate Interset-specific values. The rule is named as `BehavioralAnalyticsRule`.

5 Go to Risk Rules. Click `BehavioralAnalyticsRule`, verify, and edit it if required.

This rule is configured with the default behavior to consider any user with Interset score less than 50 as a low-risk user. You can modify this rule to change how the score from Interset is interpreted. You can modify Negate Result and the value for the score (the default value for the score condition is < 50). Do not modify any other field.

Field	Details
Negate Result	Select this option to reverse the result of the rule evaluation.
Parameters Set 1	Modify the value for the score parameter, if required.

6 Add `BehavioralAnalyticsRule` to a risk policy. Assign the risk score and the levels to configure appropriate weightage to the behavioral risk score.

See Configuring a Risk Policy.

2.6 Sample Configuration: Demo Risk Policy

On the Risk Settings page, you can create a sample policy named `Demo_RiskPolicy`. This sample policy is configured for the following use case:

Let us assume a company named `Company1` wants to control access to its resources. Company1 wants to configure specific authentication methods for each of the following scenarios:

- **Scenario 1**: A user accesses the resource using the internal network.
- **Scenario 2**: A user accesses the resource from an external network and the request contains a cookie from the Intranet site indicating that the user has earlier logged in to the resource.

- **Scenario 3**: A user accesses the resource from an external network during regular work hours that is from 9 am to 5 pm.
- **Scenario 4**: A user accesses the resource from an external network and beyond regular work hours that is from 9 am to 5 pm.

When you click **Create Sample Data**, A policy named `Demo_RiskPolicy` is created. The following are the details of the policy:

Name of the policy: Demo_RiskPolicy

Rules: The policy contains the following rules in the same sequence. The rules are executed from top to bottom.

1. **DemoRule_InternalNetwork**: To check whether the employee is in the internal network.
   - **Rule Type**: `IP Address Rule`
   - **IP address range**: `121.1.1.1 - 121.121.255.254`
   - **Action If Condition Succeeds**: `Allow Access`
2. **DemoRule_IntranetCookie**: To check whether the employee is accessing with a valid cookie from an Intranet site.
   - **Rule Type**: `Cookie Rule`
   - **Cookie Name**: `IntranetCookie`
   - **Cookie Value**: **is**/`test`
3. **DemoRule_TimeOfLogin**: To check whether the employee is accessing from an external network and time is between 9 AM to 5 PM.
   - **Rule Type**: `Use Time of Login Rule`
   - **User time of login**: `is`
   - **Day**: `Monday to Friday`
   - **Time**: `9 AM to 5 PM`

Risk Levels:

- Low: The green slider is set to 0. When conditions of all rules are met, the risk is low.
- Medium: The blue slider is set to 2. When conditions of two rules fail, the risk is medium.
- High: If all three rules fail, the risk is high.