# ArcSight Risk Insight

For the Linux Operating System

Software Version: 1.0

## Deployment Guide

Document Release Date: October 2013

Software Release Date: October 2013

# Legal Notices

## Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

The network information used in the examples in this document (including IP addresses and host names) is for illustration purposes only.

## Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

## Copyright Notice



Follow this link to see a complete statement of copyrights and acknowledgments for all HP ArcSight products: http://www.hpenterprisesecurity.com/copyright.

## Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

**This document is confidential.**

# Documentation Updates

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

- Software Version number, which indicates the software version.
- 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:

**http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

**http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

# Support

Visit the HP Software Support Online web site at:

**http://www.hp.com/go/hpsoftwaresupport**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

**http://h20229.www2.hp.com/passport-registration.html**

To find more information about access levels, go to:

**http://h20230.www2.hp.com/new_access_levels.jsp**

# Contents

# Chapter 1

# Welcome to This Guide

Welcome to the ArcSight Risk Insight Deployment Guide. This guide provides you information about the installation and initial configuration of Risk Insight.

This guide is intended for the Risk Insight System Administrator. Readers of this guide should be knowledgeable about enterprise system administration and have familiarity with information security concepts.

This guide includes the following chapters:



# About ArcSight Risk Insight

Risk Insight is an ArcSight ESM add-on that enables Risk Managers and Security Operation Center (SOC) Managers to analyze security risk information in a business context and prioritize actions to minimize that risk. Security risk information is processed periodically providing continuous monitoring capabilities on the risks imposed on your organization's assets.

Risk Insight optimizes the way risk information is delivered in the following ways:

- By building a hierarchical business model from the assets defined in ESM. The business model depicts the entire organization from high-level business assets to low-level IT assets, allowing you to quickly respond to real-time threats and to invest your resources efficiently.
- By defining risk factors based on the logic that exists in ESM to help focus the risk analysis on what really matters to the organization.
- By following up after the various risk factors using sophisticated executive dashboards. You can present risk information visually in configurable dashboards, create custom dashboards, create new KPIs, and apply any other type of logic to your risk information in order to make analysis more efficient.

Risk Insight also includes a Vulnerability Management module that collects vulnerabilities by using ArcSight SmartConnectors, removes duplicates, assigns them to assets, and prioritizes them accordingly, allowing you to manage the remediation process.

# Chapter 2

# Install Risk Insight

This chapter describes how to install and start Risk Insight.

Risk Insight is an ArcSight ESM add-on. Therefore, it can be installed only after ESM is installed. You need to install Risk Insight in a separate partition than ArcSight ESM.

Risk Insight integrates with SAP BusinessObjects Enterprise for creating reports and dashboards. Before you install Risk Insight, you must have a complete installation of BusinessObjects version 3.1 SP 5.0 running on the ESM server.

**Note:** Risk Insight supports only a new installation of BusinessObjects, which is delivered with the Risk Insight installation package. It does not support the installation of Risk Insight alongside an existing installation of BusinessObjects.

To install Risk Insight:

1. Review the system requirements and make sure that you comply with all the requirements. For more information, see "System Requirements" below.
2. Review the prerequisites and make sure that all pre-installation tasks are done. For more information, see "Prerequisites" on the next page.
3. Prepare your system before installing BusinessObjects. For more information, see "Preparing to Install SAP BusinessObjects" on the next page.
4. Install BusinessObjects. For more information, see "Install SAP BusinessObjects Enterprise " on page 15.
5. Configure SAP BusinessObjects Enterprise. For more information, see "SAP BusinessObject Configuration and Post Installation Tasks " on page 15.
6. Prepare your system before installing Risk Insight. For more information, see "Preparing to Install Risk Insight" on page 16.
7. Install Risk Insight. For more information, see "Install Risk Insight" on page 16.

# System Requirements

Risk Insight is an ArcSight ESM add-on. It is installed on the server on which ESM is installed (in a separate partition). Therefore, it is supported on Red Hat Enterprise Linux 6.4 64-bit platform and utilizes ArcSight CORR-Engine as its database.

**Server System Requirements**

Risk Insight requires 25 GB free disk space in addition to the system requirements defined for ESM. For more information, see *ArcSight ESM Installation and Configuration Guide*.

**Client Requirements**

Risk Insight requires Adobe Flash Player 11.0. For browser support, see *ArcSight ESM Product and Platform Lifecycle*.

# Prerequisites

Before you start the installation process, for both BusinessObjects and Risk Insight, perform the following tasks:

- From the installation medium, copy the following file to the ESM server:

  **ArcSightRiskInsight-xxxxx.tar**

  The xxxxx in the file name stands for the build number.

  Make sure that the **.tar** file is owned by user **arcsight**.

- Open the following TCP ports on your system (if they are not already open), and make sure that no other processes are using these ports:
  - For Risk Insight: 6060, 9005, 9009, 1099
  - For BusinessObjects: 8081, 6005, 8444, 6410, 6400
- Risk Insight is installed on the ESM server in GUI mode. Make sure that the X Window System package is installed on the ESM server (**xorg-x11-server-utils-7.5-13.el6.x86_64**).

# Preparing to Install SAP BusinessObjects

Before you run the installation file, you must prepare your system. Perform the following in console mode.

**Note:** Perform the following procedure using user **root**.

1. From the installation medium, copy the **Installation/SAP BusinessObjects/Deployment** directory to the ESM server.

# Install SAP BusinessObjects Enterprise

SAP BusinessObjects Enterprise is installed on the ESM server, which is a Linux platform. However, BusinessObjects client tools must be installed on a Windows platform. After you install SAP BusinessObjects Enterprise, install BusinessObjects client tools on another server running Windows.

### To install BusinessObjects

1. Log in to the ESM server with user **root**.
2. Open the directory to which you copied the **/Installation/SAP BusinessObjects/Deployment**.
3. Run the installation file as follows:

   **./installbo.sh**
4. Follow the instructions in the **BusinessObjects Setup Wizard**.

### To install BusinessObjects client tools

1. From the Risk Insight installation medium, unzip the file in the following folder:

   **SAP BusinessObjects/Client Tools**
2. Run **Setup.exe**.

After the installation is complete, follow the instructions in "SAP BusinessObject Configuration and Post Installation Tasks " below.

# SAP BusinessObject Configuration and Post Installation Tasks

After BusinessObjects is installed, perform the following procedures:

### Configure the maximum number of simultaneous connections

1. Open SAP BusinessObjects Central management Console (CMC) using the following URL:

   **http://[server_name]:8081/CmcApp**
2. Under **Organize**, click **Servers**.
3. In the left pane, expand **Service Categories**, and then click **Web Intelligence**.
4. In the right pane, double-click **WebIntelligenceProcessingServer**.

5. In the **Properties** window, in the **Web Intelligence Processing Service** group box, enter the following information, and then click **Save**:
   - In the **Maximum Connections** box, enter **1000**.
   - In the **Maximum Document Cache Size (KB)** box, enter **10000000**.
   - In the **Maximum Documents Per User** box, enter **20**.
6. In the right pane, double-click **AdaptiveJobServer**.
7. In the **Properties** window, in the **Maximum Concurrent Jobs** box, enter **10**, and then click **Save**.

### Update the time zone

1. Open InfoView (BusinessObjects client tool) using the following URL:

   **http://[server_name]:8081/InfoViewApp**
2. On the top right corner, click **Preferences**.
3. From the **Current Time Zone** list, select your time zone.
4. Save the changes.

# Preparing to Install Risk Insight

Before you run the Risk Insight installation file, you must prepare your system.

1. Create the following installation directory using the **root** user:

   **/usr/local/riskinsight**
2. Make sure that the user **arcsight** has write and execute permission for the **/usr/local/riskinsight** directory.
3. Change the owner and group of **/usr/local/riskinsight** directory to **arcsight** user and **arcsight** group by issuing the following command:

   **chown arcsight:arcsight /usr/local/riskinsight**

# Install Risk Insight

This section describes how to install Risk Insight. You can install Risk Insight only in GUI mode.

**Note:** If the installation fails, you can find the log file in the following location:

**/tmp/riskinsight-installation.log**

When you finish installing Risk Insight, follow the instructions in "Integrate with ArcSight Enterprise Security Manager" on page 20.

### To install Risk Insight

1. Log in to the ESM server with user **arcsight**.
2. Untar the **ArcSightRiskInsight-xxxxx.tar** file by running the following command:

   **tar xvf ArcSightRiskInsight-xxxxx.tar**
3. Double-click the following file:

   **installArcSightRiskInsight.sh**
4. Click **Run in Terminal**.
5. Follow the instructions in the **Risk Insight Setup Wizard**. In the completion page, click **Finish**.
6. Log in as user **root** and run the following script to set up the required services:

   **/usr/local/riskinsight/bin/setup-service.sh**

   **Note:** This step is required in order to start the services.
7. You can open Risk Insight, as described in "Open Risk Insight" below.

# Open Risk Insight

Risk Insight is an ArcSight ESM add-on that is opened from ArcSight ESM.

To open Risk Insight, open **ArcSight Command Center** and then click **Applications**.

# Chapter 3

# Grant Permissions to Users

Risk Insight users are managed in through the ArcSight Console in ESM. If this is the first time that you have installed Risk Insight, then there is only one user authorized to open Risk Insight—the Administrator user. To allow other users to open Risk Insight you must give them permissions through the ArcSight Console. For information on managing users and groups, see the *Managing Users and Permissions* chapter in the *ArcSight ESM User's Guide*.

There are three Risk Insight permissions:

- Admin: A user with the Admin permission can view everything and perform any task in Risk Insight. Specifically, administrator tasks performed in the Administration module, such as managing Risk Insight's configuration and creating new dashboards.
- Editor: A user with Editor permissions can perform tasks in the Asset module, the Vulnerabilities module, and in Settings, as well as view all dashboards.
- Reader: A user with Reader permissions can view the Asset module, the Vulnerabilities module, the Settings module, and all the dashboards.

In ESM, users are managed in groups. If this is the first time that you have installed Risk Insight, create dedicated user groups for Risk Insight, and grant them permissions, as described in the procedures below. If you already have Risk Insight groups, then any user that you add to these groups automatically receives the group's permissions.

### To create Risk Insight groups

1. Create the following group hierarchy:
   - **Risk Insight**
     - **Risk Insight Admin**
     - **Risk Insight Editor**
     - **Risk Insight Reader**

   For instructions, see the *Handling User Groups* section in the *Managing Users and Permissions* chapter of the *ArcSight ESM User's Guide*.
2. Link users to the following groups according to their roles:
   - **Risk Insight Admin**
   - **Risk Insight Editor**
   - **Risk Insight Reader**

For instructions, see the *Moving or Linking a User* section in the *Managing Users and Permissions* chapter of the *ArcSight ESM User's Guide*.

### To grant permissions to Risk Insight user groups

Grant permissions to the groups as follows:

- **Risk Insight Admin** grant **ArcSight Risk Insight > Admin** permissions
- **Risk Insight Editor** grant **ArcSight Risk Insight > Editor** permissions
- **Risk Insight Reader** grant **ArcSight Risk Insight > Reader** permissions

For instructions, see the *Granting or Removing Operations Permissions* section in the *Managing Users and Permissions* chapter of the *ArcSight ESM User's Guide*.

# Chapter 4

# Integrate with ArcSight Enterprise Security Manager

You can integrate with ArcSight ESM in order to synchronize the Risk Insight business model with ArcSight ESM assets.

Integrating with ESM involves preparation in Risk Insight as well as in ArcSight ESM. Before you begin the integration process, the ArcSight ESM administrator must install the **Risk Insight.arb** (ArcSight Resource Bundle) file in ESM. This file defines the parameters of data from the ESM data source that will be delivered in the Risk Insight Report (in the form of a .csv file). For more information, see "Import Risk Insight Reports into ArcSight ESM" on page 44. The file is located in **<Risk Insight installation folder>\resources**. The Risk Insight Report will be triggered by Risk Insight and will be used to create a file (.csv) that includes asset information.

The ArcSight ESM administrator should provide you with connection parameters, described in "Define Connection Parameters with ESM" on page 22. After you have gathered all the information from the ArcSight ESM administrator, you can begin the integration process, as described in "How to Integrate with ESM for Asset Synchronization" on the next page .

After Risk Insight is fully integrated with ArcSight ESM, the Synchronization job runs periodically, according to the schedule that you defined. To learn more about the Asset Synchronization job, see "About ArcSight ESM Asset Synchronization Job" below.

## About ArcSight ESM Asset Synchronization Job

The Asset Synchronization Job periodically imports ArcSight ESM entities from ArcSight ESM into Risk Insight, as follows:

1. The ArcSight Resource Bundle (*.arb) file triggers the creation of the Risk Insight Asset Report.
2. The ArcSight ESM Report contains all of the asset information, according to the asset mapping between these two applications. Each record in the report represents an asset.
3. ArcSight ESM assets and their properties are converted into Risk Insight assets and relationships. For more information on mapping logic, see "Map Asset Types with ESM" on page 23.
4. The process checks the Risk Insight database for each of the assets/relationships.
   - If the **element does not exist** in the database, then the process writes that element to the database.
   - If the **element changed**, then the process updates these changes in the database.

5. Outdated assets and relationships are deleted from the Risk Insight database (meaning that they no longer exist in the database).

You can check the status of the job in the Job Management module. For more information, see the *Troubleshoot Batch Jobs* section in the *ArcSight  Risk Insight Administration Guide*.

# How to Integrate with ESM for Asset Synchronization

Before you begin integrating Risk Insight and ArcSight ESM, make sure that you have the connection parameters provided to you by the ArcSight ESM administrator.

The following procedure outlines the steps for integrating with ArcSight ESM. This procedure includes steps for configuring asset synchronization.

1. **Change the session timeout in ArcSight ESM**. The default session timeout in ArcSight ESM is 10 minutes; this amount of time is not always enough to generate the asset report. If your business model has more than 50,000 assets, then you need to change the session timeout in ArcSight ESM.

   **Note:** Changing the session timeout requires restarting ESM Manager.

   For more information, see "Change ESM Session Timeout" below.

2. **Define connection parameters**. Define the parameters necessary for connecting with ArcSight ESM. These parameters must be provided to you by the ArcSight ESM administrator. Follow the instructions in "Define Connection Parameters with ESM" on the facing page.

3. **Review Default Asset Type Mapping**. Review the default asset type mappings that are included in Risk Insight to see whether they reflect your business model. If required, follow the instructions in "Map Asset Types with ESM" on page 23 to tailor the mapping to your needs.

4. **Define Imported Asset Type properties**. Decide which asset properties will be imported from ArcSight ESM, as described in "Define Imported Asset Type Properties" on page 24.

5. **Schedule and activate the Synchronization job** in order to complete the process, as described in "Schedule and Activate the ESM Job" on page 25.

# Change ESM Session Timeout

**Note:** Changing the session timeout requires restarting ESM Manager.

### To change the session timeout

1. On the server on which ArcSight ESM is installed, open a command window or shell window on **<ARCSIGHT_HOME>/manager/config**.
2. Type the following file name, and then press **ENTER**:

   **./server.properties**
3. Change the session timeout by typing the following line, and then press **ENTER**:

   **servletcontainer.jetty311.session.timeout.default=20**
4. As user **arcsight**, restart the ESM Manager by typing the following command, and then press **ENTER**:

   **/sbin/service arcsight_services restart manager**

# Define Connection Parameters with ESM

The first step in integrating with ArcSight ESM is defining connection parameters. These parameters should be provided by the ArcSight ESM administrator, prior to integration.

### To define connection parameters with ArcSight ESM

1. Click **Administration > Configuration**.
2. In the left pane, click **Integrations > ArcSight ESM > Connector**.
3. In the **Connector** page, enter the parameters for connecting with ArcSight ESM as described in the following table:

**ArcSight ESM Integration Parameters**

| Parameter | Description |
|---|---|
| **Connector Name** | Enter a name for the ArcSight ESM system to which you want to connect. This is the name that is displayed in the **Source** property of the asset. |
| **Host** | The host name or IP address of the ArcSight ESM server, provided by the ArcSight ESM administrator. |
| **Port** | The server port, provided by the ArcSight ESM administrator. |
| **Username** | Credentials for accessing ArcSight ESM, provided by the ArcSight ESM administrator. |
| **Password** | Credentials for accessing ArcSight ESM, provided by the ArcSight ESM administrator. |

4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 42.

# Map Asset Types with ESM

**Note:** Before you begin, you should have a clear vision of what you want your business model to look like. If at any time you want to change the business model, then you can change the mapping configuration; the business model will be updated after the next Asset Synchronization Job runs.

ArcSight ESM holds assets that represent IP addresses in a flat file format. When these assets are imported to Risk Insight they are converted into the Risk Insight business model format, where the IP asset is the primary asset.

To help you create a hierarchical business model that reflects the ArcSight ESM network model but also provides business context, in addition to assets, the Asset Synchronization Job imports the following ArcSight ESM entities:

- Asset Group
- Asset Category
- Zone Group
- Zone

All of these entities have a corresponding asset type in Risk Insight, and they all belong to the Business Asset category, as presented in the following table.

| ESM Entities | Risk Insight Asset Category | Risk Insight Asset Type |
|---|---|---|
| Asset Group | Business Asset | Asset Group |
| Asset Category | Business Asset | Category |
| Zone Group | Business Asset | Zone Group |
| Zone | Business Asset | Zone |

The asset zone and zone group are reflected in the business model by design. You can decide whether to reflect the asset group and asset category in the business model. If you choose to reflect the asset group and the asset category, then two additional hierarchies will be created. So, potentially, you can have numerous hierarchies under the Organization asset.

By default, each of the ArcSight ESM entities is mapped to its corresponding asset type in Risk Insight, but you can map them to any asset type defined in Risk Insight. You can also create exceptions. For example, if you mapped a zone in ArcSight ESM to a zone in Risk Insight, but you want to map one specific zone to a subnet, then you can create an exception.

The following procedure describes how to select which hierarchies will be created, map asset types, and create exceptions.

### To map asset types with ArcSight ESM

1. Click **Administration > Configuration**.
2. In the left pane, click **Integrations > ArcSight ESM > Asset Synchronization > Asset Type Mapping**.
3. In the **Asset Type Mapping** page, depending on the number of hierarchies that you want to create, select the following:
   - **Create a Group-based Model**
   - **Create a Category-based Model**
4. If required, change the default mapping in the mapping table.
5. To create an exception, do the following:
   a. Click a new row in the mappings table to create a new record.
   b. From the **ESM Entities** list, select the ESM entity for which you want to create an exception.
   c. In the **ESM Entity Exception** cell, enter the name of the ESM entity for which you want to create a separate mapping.
   d. From the **Risk Insight Asset Category** list, select the category of the Risk Insight asset type that you want to map.
   e. In the **Risk Insight Asset Type** enter the asset type to which you want to map the exception.
6. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 42.

# Define Imported Asset Type Properties

For each asset category, you can decide which properties from the asset repository are periodically imported and synchronized, meaning that they cannot be overridden in Risk Insight. The following properties are common to all categories:

- Name
- Description

### To define imported asset type properties

1. Click **Administration > Configuration**.
2. In the **Configuration** module, in the left pane, click **Asset Management > Imported Asset Properties Policy**.
3. For each asset category displayed under **Imported Asset Properties Policy**, do the following:
   a. In the left pane, click the asset category.
   b. For each property, select or clear the **Synchronize** check box. If a check box is not selected, then the asset property will be editable in Risk Insight.
4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 42.

# Schedule and Activate the ESM Job

After you define all of the required parameters for connecting with ArcSight ESM, you can schedule and activate the Asset Synchronization job, the Event Import job, or both.

For more information on the jobs, see "About ArcSight ESM Asset Synchronization Job" on page 20.

### To schedule and activate a synchronization job

1. Click **Administration > Configuration**.
2. In the left pane, do one of the following:
   - Click **Integrations > ArcSight ESM > Asset Synchronization > Schedule Job**.
3. In the **Job** page, do the following:
   - **Job Schedule**: enter a Cron expression.

     For example, to run the job once every hour, every day, enter the following:

     **0 0 0/1 * * ?**

     For more information , see "Appendix B: Learn About Cron Expressions" on page 45.
   - Select the **Activate Job** check box.
4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 42.

   The Synchronization job is activated and will run according to the schedule that you have set.

# Chapter 5

# Import Risk Information from ESM

Risk Insight enables you to import information on risk factors from ArcSight ESM. For more information on risk factors, see the *Risk Factors* section in the *ArcSight Risk Insight User Guide*.

Information is imported by using a connector.

**Note:** Before you create an ESM connector, you must first integrate with ArcSight ESM in order to synchronize the Risk Insight business model with ArcSight ESM assets. Only assets that are imported from ArcSight ESM can be updated with risk factor scores from ArcSight ESM. For more information on integrating with ArcSight ESM, see "Integrate with ArcSight Enterprise Security Manager" on page 20.

Following are the steps for importing risk information into Risk Insight:

1. Create an ESM report. For more information, see "Create a Risk Factor Report in ESM" on the next page.
2. Define the risk factor and configure the connector. For more information, see "How to Create a Risk Factor in Risk Insight" on page 29.

   **Note:** For optimal performance, schedule the import jobs for each of the risk factors to run at different times, with at least a 30-minute difference between runs.

## About Risk Factor Import Job

The Risk Factor Import Job periodically imports risk information from ESM. For each risk factor that you define and configure in Risk Insight, a specific job is created with the name: <*risk factor name*>ImportJob. The job is created only after the new configuration is saved and activated.

Following is the process:

1. The process checks whether the data was already imported into Risk Insight. If it was, then the process completes without import.

   If the data is invalid, for example if one of the columns is missing, then the job fails.
2. The process reads the data from the data source.
3. The process writes the new data to the scores table in the database.

- If a score is out of range, then the record is skipped.
- If there are duplicate records, then the last record found overrides the previous record.
- If Risk Insight has more than one asset defined in the business matches the Asset Identifier in the data source, then the first one found is updated.

**Note:** In all of these cases, a warning is written to the error log.

4. If there is data in the scores table in the database, then the process deletes it according to the Delete Old Scores indicator.

   If you selected the **Delete Old Scores** check box when you configured the connection parameters, then all the scores are deleted regardless of whether they have been updated or not. If you did not select this check box, then only scores that were updated are deleted.

5. The process aggregates the scores and writes them to the database.

6. If you selected the **Archive immediately after import** check box in **Configuration**, then both scores and aggregate scores are archived.

   For more information on archiving, see the *Archive Trend Data* section in the *ArcSight Risk Insight Administration Guide*.

# Create a Risk Factor Report in ESM

When you create a risk factor report, you need to export it as a CSV file.

**Note:** Make sure that the ESM entities that are included in the file do not have a **","** character (comma) in their name. The file generated by the report includes a **","** delimiter, so if this character is used in an ESM entity name, then the name will be split into two.

The report must have the following format:

| Parameter | Format | Description |
|---|---|---|
| Asset Identifier | Maximum 255 characters | Mandatory<br>If the asset identifier is empty, then the record is skipped. |
| Score | Rational number | Mandatory<br>If the score is empty, then the record is skipped. |
| Comment | Maximum 255 characters | Optional |

The following procedure explains how to create a risk factor report in ESM.

To create a risk factor report

1. Follow the instructions in the *Building Reports* section in the *ArcSight Console User's Guide*.
2. When you define the query settings, create a query based on one of the following data sources:
   - **Events**
   - **Assets**
   - **Active List**

   These data sources are the most suitable for creating a risk factor report. Out-of-the-box reports included in Risk Insight are based on the data sources listed above. For more information, see the *Out-of-the-Box Risk Factor Reports* section in the *ArcSight Risk Insight User Guide*.
3. Edit the **Row Limit** query field. We recommend that the maximum number of rows is similar to the number of assets in the business model.
4. When you create the query structure, create three active columns in the following order:
   a. The asset identifier
   b. The score of the risk factor for a specific asset
   c. Additional evidence

   **Note: Comment** is a reserved word in ESM. When you create this column enter a different name. Change the column name back to **Comment** by editing the query later on.
5. When you define the report settings, in the **Report Data** area, change the **Alias** for each column that you defined to the following names:
   a. **Asset Identifier**
   b. **Score**
   c. **Comment**

   These names are the column names that are created in the CSV file. The column name is case-sensitive.
6. When you define the report settings, in the **Report Parameters** area, from the **Format** list, select **CSV**.
7. For each risk factor for which you want to import data into Risk Insight, deploy real-time rules, as described in the *Deploying Real-Time Rules* section in the *ArcSight Console User's Guide*.

# How to Create a Risk Factor in Risk Insight

In order to import risk information from ESM you must first define and configure the risk factors in Risk Insight.

The following procedure outlines the steps for defining and configuring risk factors:

1. Define a new risk factor in Risk Insight. For more information, see "Define a New Risk Factor " below.
2. Configure the connection parameters. For more information see "Configure the Risk Factor Connector Parameters" on the facing page.
3. Configure the risk factor import job. For more information see "Configure the Risk Factor Import Job" on the facing page.
4. Configure the normalization settings for the risk factor. For more information, see "Configure the Risk Factor Normalization Settings" on page 31.
5. Configure the risk factor score aggregation method. For more information, see "Configure the Risk Factor Aggregation Method" on page 32.
6. Configure the archive settings. For more information, see the *Configure the Risk Factor Archive Settings* section in the *ArcSight Risk Insight Administration Guide*.
7. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 42.
8. Configure risk factor ranges in order to display the risk factor scores with the appropriate score severity. For more information, see "Configure Risk Factor Ranges" on page 33.

# Define a New Risk Factor

You can define any number of risk factors in Risk Insight.

Whenever you add a risk factor to Risk Insight, a corresponding KPI is created automatically. For more information, see the *Risk Factor Dashboard* section in the *ArcSight Risk Insight User Guide*.

After you define the risk factor you can configure its connection parameters, as described in "Configure the Risk Factor Connector Parameters" on the facing page.

### To define a new risk factor

1. Click **Administration** > **Configuration**.
2. On the **Configuration** page, in the left pane, click **Risk Factor**.
3. Click the **Add configuration to configuration set**  button, and select **ESM Connector**.

4. In the left pane, expand the risk factor folder, and then click the empty folder.
5. In the left pane, enter the following information:
   a. **Risk Factor Name**: enter the name of the risk factor for which you want to import risk information.

      **Note:**

      - The name cannot include the following characters: *** ? = ' :**
      - This is also the display name of the risk factor. It will be displayed in the folder name, Risk Register, Risk Indicators, Risk Factor Dashboard, and any other report that includes this risk factor.

   b. **Description**: this field is optional.

# Configure the Risk Factor Connector Parameters

You need to configure the connection parameters to ESM from which you are importing the risk factor information.

### To configure connection parameters

1. Open the risk factor folder. Click **Administration** > **Configuration**, expand the risk factor folder, and then click the factor that you defined.
2. Under the folder of the risk factor that you defined, click **Connector Parameters**.
3. Do the following:
   a. In **Resource ID**, enter the resource ID that you defined when you created the report in ESM.
   b. In **Port**, enter the ESM server port.
4. Select the **Delete Old Scores** check box if you want all the scores to be deleted when the Risk Factor Import Job is run regardless of whether the scores have been updated or not. if you do not select this check box, then the job will only delete scores that have changed and will leave the unchanged scores in the database.
5. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 42.

# Configure the Risk Factor Import Job

After the connector parameters are configured, you need to schedule and activate the Risk Factor Import Job. For each risk factor that you define and configure in Risk Insight, a specific job is

created with the name: <*risk factorname*>ImportJob. The job is created only after the new configuration is saved and activated. For more information on the job, see "About Risk Factor Import Job" on page 26.

### To schedule and activate the import job

1. Open the risk factor folder. Click **Administration** > **Configuration**, expand the risk factor folder, and then click the factor that you defined.
2. Under the folder of the risk factor that you defined, click **Import Job**.
3. In the **Import Job** window, in the right pane, do the following:
   a. Select the **Activate Job** check box.
   b. In the **Job Schedule** box, enter a Cron expression.

      For example, to run the job at 02:00, every day, enter the following:

      **0 0 2 * * ?**

      For more information, see "Appendix B: Learn About Cron Expressions" on page 45.
4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 42.

# Configure the Risk Factor Normalization Settings

In order to be included in the asset overall score calculation, all risk factors are normalized to a score between 0 and 100 (inclusive). In order to normalize the score, you must set the score range for the risk factor. You must also define the directionality of the score severity. For example, a low score is considered low risk while a high score is considered high risk.

These settings affect the definition of the severity ranges reflected in **Settings > Risk Factor**. For more information, see "Configure Risk Factor Ranges" on page 33.

### To configure normalization settings

1. Open the risk factor folder. Click **Administration** > **Configuration**, expand the **Risk Factor** folder, and then click the risk factor that you defined.
2. Under the folder of the risk factor that you defined, click **Normalization**.
3. In the **Normalization** page, do the following:
   - **Minimum Score**: enter the first number in the score range.
   - **Maximum Score**: enter the last number in the score range.

**Note:** The score range is inclusive.

- **Display score with this number of digits after the decimal point**: to define the score display precision level, enter the number of digits after the decimal point that you want to display.
- To define the directionality of the score severity, select or clear the **Lower Score is Best** check box.

4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 42.

# Configure the Risk Factor Aggregation Method

You can configure the aggregation method for each of the risk factors defined in Risk Insight.

## To configure aggregation method

1. Click **Administration > Configuration**.
2. In the left pane, click **Risk Factor** > ***<Risk Factor Name>*** > **Aggregation Method**.
3. In the right pane, from the **Aggregation Method** list, select one of the following options:
   - **Average** (default)

     The weighted average of aggregate scores of an asset's children including the score of asset itself. This is the default method. The asset's score and the aggregate score of its children is taken into account.

     $$\frac{\sum(AggregateScoreChildren * CriticalityLevel) + AssetScore * CriticalityLevel}{\sum(CriticalityLevel)}$$

   - **Override Children**

     If the asset already has a score, then its aggregate score receives the value of the score. If the asset does not have a score, then its aggregate score is calculated according to the Average formula. The asset's score takes precedence over its children's aggregate score.

     Asset score or $\frac{\sum(AggregateScoreChildren * CriticalityLevel)}{\sum(CriticalityLevel)}$

   - **Average of Children**

     The weighted average of aggregate scores of an asset's children, excluding the score of the asset itself. The aggregate score of the children takes precedence over the asset's own

score.

$$\frac{\sum(AggregateScoreChildren * CriticalityLevel)}{\sum(CriticalityLevel)}$$

4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 42

# Configure Risk Factor Ranges

You can configure the ranges for the score severity indication for any risk factor defined in Risk Insight.

Score ranges and the directionality of the score severity may differ between risk factor. These settings are defined during the configuration process of the risk factor. For more information, see "Configure the Risk Factor Normalization Settings" on page 31..

Risk factor scores are displayed with one of the following icons:

Low score

Medium score

High score

This configuration is reflected throughout the application, wherever these measurements are displayed. For example, on the Risk Register page in the Asset Summary component.

### To configure risk factor ranges

1. On the Risk Insight toolbar, click the **Settings** button.
2. On the **Settings** dialog box, click **Risk Factors**.
3. In the left pane, click the risk factor for which you want to configure ranges.
4. Drag the slider to define the ranges.
5. Click **Save**.

# Delete a Risk Factor

You can delete a risk factor from Risk Insight when it is no longer relevant.

When you delete a risk factor all of the data pertaining to this factor in the database is deleted, as well.

The job that is created when you create a new risk factor ( *<risk factor name>*ImportJob) is not deleted and can be viewed in the Job Management module.

### To delete a risk factor

1. Click **Administration** > **Configuration**.
2. On the **Configuration** page, in the left pane, expand **Risk Factor**.
3. Click the risk factor that you want to delete, and then click the **Remove configuration from configuration set**  button.
4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 42.

# Chapter 6

# Import Vulnerabilities From Vulnerability Assessment Tools

Risk Insight enables you to regularly import vulnerability information from vulnerability assessment tools, providing near real-time monitoring capabilities on the vulnerabilities and exposures affecting your organization's physical and business assets.

Risk Insight imports the vulnerability information from vulnerability scanner reports by using ArcSight SmartConnectors. For an overview on the Vulnerabilities module, see the *Vulnerability Management* chapter in the *ArcSight Risk Insight User Guide*.

**Note:** In order to work with the Vulnerabilities module, you must have at least one of the vulnerability assessment tools supported by Risk Insight installed in your network.

The following table includes the vulnerability assessment tools supported by Risk Insight and their corresponding ArcSight SmartConnector.

| Vulnerability Assessment Tool | ArcSight SmartConnector |
|---|---|
| Tenable Nessus Vulnerability Scanner | Tenable Nessus .nessus File |
| McAfee Vulnerability Manager (Foundscan) | McAffee Vulnerability Manager DB |
| Qualys Guard | Qualys Vulnerability Scanner File |
| HP WebInspect | ArcSight FlexConnector XML file |
| Rapid7 Nexpose | Rapid7 NeXpose XML File |

The Risk Insight installation kit includes a separate ArcSight SmartConnector executable along with the relevant documentation.

Vulnerability assessment tools generate reports in a variety of formats, such as an XML file or a database. The ArcSight SmartConnector normalizes the different formats into one format. In Risk Insight, the ArcSight SmartConnector is configured to use a CSV file format. The CSV file is then processed by the Vulnerabilities Import Job. The vulnerability information is imported into Risk Insight and displayed in the Vulnerability Management window.

**Note:** HP WebInspect does not generate reports automatically. In order to load vulnerability information into Risk Insight, you must manually export the scans in Full XML format, as described in the *Export scan details in WebInspect* task, in the *Web Application Firewall Integration Tool* section, in the *HP WebInspect User Guide.*

After you export the scan, copy it to the reports folder that you defined when you installed the connector.

To import vulnerabilities, first "Install and Configure ArcSight SmartConnector" on the facing page and then "Schedule and Activate Vulnerabilities Import Job" on page 39.

# About the Vulnerability Import Job

The Vulnerability Import Job periodically imports and processes vulnerability information from scanners into Risk Insight, as follows:

1. The process retrieves CSV files that are generated by ArcSight SmartConnectors that have a ***.done.csv** extension from the following folder:

   **<Risk Insight Installation folder>\vm\import\pending\<connector ID>**

2. Each record from the CSV file is standardized (normalized) and enhanced to create a single vulnerability instance. Records are processed in batches.

   a. For each CSV record, the process checks whether the vulnerability is defined in the vulnerability dictionary. If it is, then the vulnerability's name (classifier) is taken from the vulnerability dictionary and its information is enhanced accordingly. If it is not, then the vulnerability name receives the identifier provided by the source, taken from the CSV file.

   b. Information is modified and standardized in a consistent manner. For example, vulnerability priority or severity is normalized to a score between 0 and 10.

   c. The vulnerability instance records are saved in the Risk Insight database.

3. The process aggregates vulnerability instances that represent the same vulnerability into a single vulnerability occurrence, according to the vulnerability name and location. For more information on these properties, see the *Vulnerability Properties* section in the *ArcSight Risk Insight User Guide*.

4. Closed vulnerability occurrences that do not have a remediation status of Not an Issue and that have new vulnerability instances, are reopened.

5. The process maps vulnerability occurrences to assets of type IP Address in the business model according to the host, IP address, and MAC address.All matched vulnerabilities are attached to assets.

6. Outdated vulnerability occurrences (no vulnerability instances have been reported for over an N number of days) are closed, with remediation status Automatically Closed. The **Automatically close vulnerability after (days)** parameter is configured in "Schedule and Activate Vulnerabilities Import Job" on page 39.

7. The CSV files are moved to the following folders:

   - Successfully processed files are moved to the **<Risk Insight Installation folder>\vm\import\done\<connector ID>** folder.

   - Files that contain erroneous records are moved to the **<Risk Insight Installation folder>\vm\import\errors\<connector ID>** folder.

For more information, see the *Vulnerability Error Handling* section in the *ArcSight Risk Insight User Guide*.

You can check the status of the job in the Job Management module. For more information, see the *Troubleshoot Batch Jobs* section in the *ArcSight Risk Insight Administration Guide*.

# Install and Configure ArcSight SmartConnector

You can either install a new connector or add a destination to an existing connector. For more information on destinations, see the *SmartConnector Destinations* chapter in the *ArcSight SmartConnector User's Guide*. Connectors do not have to be installed on the ESM server.

If you are installing a new connector, for all installation instructions, including system requirements for the connector that you want to install, see the *SmartConnector Configuration Guide* for:

- Tenable Nessus .nessus File
- McAfee Vulnerability Manager DB
- Qualys QualysGuard File
- ArcSight FlexConnector XML file (for HP WebInspect)
- Rapid7 NeXpose XML File

In order for Risk Insight to work with ArcSight SmartConnectors, you need to run the configuration tool for each connector, this means that if you have two connectors, then you need to run the tool twice, once for each connector. The configuration tool configures the connector to write the CSV files containing the vulnerability information to the following folder on the Risk Insight server:

**<Risk Insight installation folder>\vm\import\pending\<connector ID>**

The tool also configures other settings, such as fields in the CSV file and the CSV file rotation interval.

**Note:** It is important that you perform the configuration procedure immediately after you install or modify the connector.

## To install a connector

**Note:** ArcSight FlexConnector XML file installation is only supported on a Windows operating system.

1. From the Risk Insight installation medium, open the **Connectors** folder.
2. Start the ArcSight SmartConnector Installer by running one of the following (depending on the operating system installed on the server):

**ArcSight-<version>-Connector-Win.exe**

**ArcSight-<version>-Connector-Linux.bin**

3. Run the wizard with the default settings until the installation is completed. Enter the required information:

   a. When prompted to select the destination type for the connector, select **CSV File**.

   b. When prompted to select a **Mode**, select **Automatic**.

   c. When prompted, select **Yes, I want to configure the SmartConnector to run as a service**.

   For each connector that you install, a dedicated folder (for example, ArcSight SmarConnector Nessus) is created under the root folder.

## To add a destination to an existing connector

1. Open the following location:

   **<Connector Installation Folder>\current\bin**

2. Depending on your operating system, run one of the following:

   - **runagentsetup.sh**
   - **runagentsetup.bat**

3. In the wizard, do the following:

   a. In the first page, **Modify Connector** is selected by default. Click **Next**.

   b. In the second page, select **Add, modify, or remove destinations**, and then click **Next**.

   c. In the third page, select **Add destination**, and then click **Next**.

   d. In the forth page, select **CSV File**, and then click **Next**.

   e. In the fifth page, enter a **CSV Path**, and then click **Next**. The path that you enter is a placeholder and will be overridden by the configuration tool.

   f. Complete the wizard.

## To configure a connector

1. From your ArcSight Risk Insight installation medium, copy the following:

**\Connectors\ArcSight SmartConnectors\Tools\ArcSight SmartConnector Configuration tool.zip**

To this directory:

**<Connector Installation Folder>\current**

For example: ArcSightSmartConnectors Nessus\current

2. Extract the zip file to a separate folder. Make sure that the **bin**, **jre**, and **lib** folders are under the extracted folder.
3. Open the following folder from the command line:

   **<Connector Installation Folder>\current\<extracted zip folder>\bin**

   The directory includes four files. Select the one that you want to run:

   - For a 64-bit Windows operating system
   - For a 32-bit Windows operating system
   - For a 64-bit Linux operating system
   - For a 32-bit Linux operating system
4. Run the configuration tool with a parameter :

   **run_vm_connector_config_*.* <Risk Insight installation folder>\vm\import\pending**

   **Note:** Make sure that the connector has **write** permissions for the following folder in Risk Insight:

   **<Risk Insight installation folder>\vm\import\pending**

   **Note:** If you are working on a Linux operating system, make sure that the shell script has execute permissions.
5. Start the ArcSight SmartConnector service.

# Schedule and Activate Vulnerabilities Import Job

After the connector/connectors are running, you need to schedule and activate the Vulnerabilities Import Job. For more information on the job, see "About the Vulnerability Import Job" on page 36.

### To schedule and activate the Vulnerabilities Import Job

1. Click **Administration > Configuration**.
2. In the left pane, click **Vulnerability Management > Schedule Import Job**.
3. In the **Schedule Import Job** window, in the right pane, do the following:
   a. Select the **Activate Job** check box.
   b. In the **Job Schedule** box, enter a Cron expression.

      For example, to run the job at 02:00, every day, enter the following:

      **0 0 2 * * ?**

      For more information, see "Appendix B: Learn About Cron Expressions" on page 45.
   c. Select the **Automatically Close Vulnerabilities** check box in order to enable automatic closing of vulnerabilities.
   d. If you selected the **Automatically Close Vulnerabilities** check box, then in the **Automatically Close Vulnerability After (days)**, enter the number of days after which the remediation status should be changed to Automatically Closed.
4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 42.

# Chapter 7

# Manage Configuration Sets

The Configuration module enables you to define the configuration settings needed to set up your environment.

A configuration set contains the properties defined for the system. You can create any number of configuration sets and then select one with which to run your system. Risk Insight maintains a history of all the configuration sets created. For more information, see "Select Configuration Set" below.

A new configuration set is initially saved as a draft. A draft is a configuration set that has not yet been activated. A draft can be edited only until it is first activated. The new configuration properties are only applied to Risk Insight when a draft is activated. For details on how to activate a draft, see "Save and Apply Configuration Changes" on the next page.

You cannot edit a configuration set after it has been activated, you must create a new draft instead. You can create a new draft based on an existing configuration set and save it with a new name.

Risk Insight validates the configuration set and identifies the problems in the configuration, such as, a field with a missing value. If a problem is found, Risk Insight displays a description of the problem, a link to the configuration pane in which the problem was found, and an icon that indicates the severity of the problem.

## Select Configuration Set

You can create any number of configuration sets and then select one with which to run your system.

### To select a configuration set

1. Click **Administration > Configuration**.
2. In the **Configuration** window, in the left pane, click the **Open Configuration Set**  button.

   The currently active configuration set is displayed in bold.
3. In the **Open Configuration Set** window, from the list of configuration sets, click the one that you want to run, and then click **Open**.

   You can filter the list of configuration sets by selecting one of the following options:

   - **Activated**
   - **Drafts**
4. In the left pane, click the **Activate current configuration set**

 button.

In the **Activate Configuration Set** dialog box, click **Yes**.

# Save and Apply Configuration Changes

You can save configuration changes and then apply the new configuration settings to Risk Insight by creating a new configuration set.

When a change is made to one of the settings, an asterisk appears next to the category name in the left pane.

### To create a new configuration set

1. Click **Administration > Configuration** and make the required configuration changes.
2. In the **Configuration** window, in the left pane, click the **Save current editable configuration set**  button.
3. In the **Save as Draft** dialog box, in the **Draft name** box, type the name of the draft, and then click **Save**.

   Risk Insight applies the new configuration settings when you activate the draft.

   **Note:** If the configuration set contains invalid or missing values, messages are displayed in the **Problems** pane at the bottom of the screen. To navigate to the page on which the problem occurs, click the **Code** link and try to resolve the problem. You can activate only configuration sets that do not have any problems.

4. In the left pane, click **Open configuration set**  button.
5. In the **Open Configuration Set** dialog box, select the required draft, and then click **Open**. You can select the **Draft** option to display only draft configuration sets. The name of the currently selected configuration set appears at the top of the left pane.
6. In the left pane, click the **Activate current configuration set**  button to activate the selected draft and apply the new configuration settings to Risk Insight.

# Appendix A: Asset Reporting

The following sections describe this report and provide additional information about accessing it and interpreting its content. For more information about integration with Risk Insight, see "Integrate with ArcSight Enterprise Security Manager" on page 20.

## About the Asset Report

The Asset report lists all of the assets currently stored in your ArcSight ESM environment. An asset is defined in ArcSight ESM as a network endpoint that contains an IP address and a host name or external ID. The report is generated by querying the ArcSight ESM asset schema, from which the relevant fields are retrieved. The report can provide asset information from these fields. (Not all fields will be populated all of the time.)

- Asset ID
- Asset External ID
- Asset Name (The name used to identify the asset )
- Asset Description (The description of the asset)
- IP Address (The IP address of the network device represented by the asset)
- Zone URI (The URI of the zone to which the asset belongs)
- Hostname (The host name of the network device represented by the asset)
- MAC Address (The MAC address of the network device represented by the asset)
- OS (The operating system under which the asset is run)
- Application
- Location
- Location ID
- Modification Time
- Create Time
- Zone Name
- Zone ID
- Asset URI
- All Categories

The Asset report is located in the following directory in the ArcSight ESM environment:

**.. /All Reports/JumpStart/ArcSight/Risk Insight/Asset Report**

# Import Risk Insight Reports into ArcSight ESM

Risk Insight reports are available from a bundled file, Risk_Insight.arb, in the ArcSight ESM Manager.

### To install the reports and import the .arb file as a package

1. In the **ESM Manager Console**, in the **Navigator** panel, click the **Packages** tab.
2. Click the green down-arrow icon.
3. Select the **Risk_Insight.arb** file, and click **Open**.

   **Note:** To import the package without installing it, clear the check box next to the .arb file name. (The default is to install all imported packages.)

4. Review the **Import** dialog box for any conflicts. Each conflict displays one or more resolution options. To resolve a conflict, choose the preferred resolution option and click the **OK** button next to the options window. For more about resolving conflicts, see the section *Resolving Package Conflicts* in the *ArcSight Console User Guide*.
5. Click **OK** to complete the import process.

   The package from which the reports can be generated will be imported into the folder:

   **/All Packages/JumpStart/ArcSight/Risk Insight**

# Appendix B: Learn About Cron Expressions

A Cron expression is a string comprised of 6 or 7 fields separated by white space. Fields can contain any of the allowed values, along with various combinations of the allowed special characters for that field. The fields are as follows:

**Cron Expression Format**

| Field Name | Mandatory | Allowed values | Allowed Special Characters |
|---|---|---|---|
| Seconds | YES | 0-59 | , - * / |
| Minutes | YES | 0-59 | , - * / |
| Hours | YES | 0-23 | , - * / |
| Day of month | YES | 1-31 | , - * ? / L W |
| Month | YES | 1-12 or JAN-DEC | , - * / |
| Day of week | YES | 1-7 or SUN-SAT | , - * ? / L # |
| Year | NO | empty, 1970-2099 | , - * / |

You can use the following special characters:

**Cron Expression Special Characters**

| Character | Description |
|---|---|
| ***** **(all values)** | Used to select all values within a field. For example "*" in the minute field means "every minute". |
| **?** **(no specific value)** | Used to specify something in one of the two fields in which the character is allowed, but not the other. For example, if you want your trigger to fire on a particular day of the month (say, the 10th), but don't care what day of the week that happens to be, you can put "10" in the day-of-month field, and "?" in the day-of-week field. |
| - | Used to specify ranges. For example, "10-12" in the hour field means "the hours 10, 11 and 12". |
| **,** | Used to specify additional values. For example, "MON,WED,FRI" in the day-of-week field means "the days Monday, Wednesday, and Friday". |
| **/** | Used to specify increments. For example, "0/15" in the seconds field means "the seconds 0, 15, 30, and 45". And "5/15" in the seconds field means "the seconds 5, 20, 35, and 50". You can also specify '/' after the '' character - in this case '' is equivalent to having '0' before the '/'. '1/3' in the day-of-month field means "fire every 3 days starting on the first day of the month". |

**Cron Expression Special Characters, continued**

| Character | Description |
|---|---|
| **L**<br>**(last)** | When used in the day-of-month field: The value "L" means "the last day of the month" - day 31 for January, day 28 for February on non-leap years. You can also specify an offset from the last day of the month, such as "L-3" which would mean the third-to-last day of the calendar month. When used in the day-of-week field: - Used by itself, it simply means the last day of the week, which is "7" or "SAT". - Used after another value, it means "the last xxx day of the month", for example "6L" means "the last Friday of the month". When using the 'L' option, it is important not to specify lists, or ranges of values, as you'll get confusing/unexpected results. |
| **W**<br>**(weekday)** | Used to specify the weekday (Monday-Friday) nearest the given day. As an example, if you were to specify "15W" as the value for the day-of-month field, the meaning is: "the nearest weekday to the 15th of the month". So if the 15th is a Saturday, the trigger will fire on Friday the 14th. If the 15th is a Sunday, the trigger will fire on Monday the 16th. If the 15th is a Tuesday, then it will fire on Tuesday the 15th. However if you specify "1W" as the value for day-of-month, and the 1st is a Saturday, the trigger will fire on Monday the 3rd, as it will not 'jump' over the boundary of a month's days. The 'W' character can only be specified when the day-of-month is a single day, not a range or list of days.<br>The 'L' and 'W' characters can also be combined in the day-of-month field to yield 'LW', which translates to "last weekday of the month". |
| **#** | Used to specify "the nth" XXX day of the month. For example, the value of "6#3" in the day-of-week field means "the third Friday of the month" (day 6 = Friday and "#3" = the 3rd one in the month). Other examples: "2#1" = the first Monday of the month and "4#5" = the fifth Wednesday of the month. Note that if you specify "#5" and there is not 5 of the given day-of-week in the month, then no firing will occur that month. |

* The legal characters and the names of months and days of the week are not case-sensitive. MON is the same as mon.