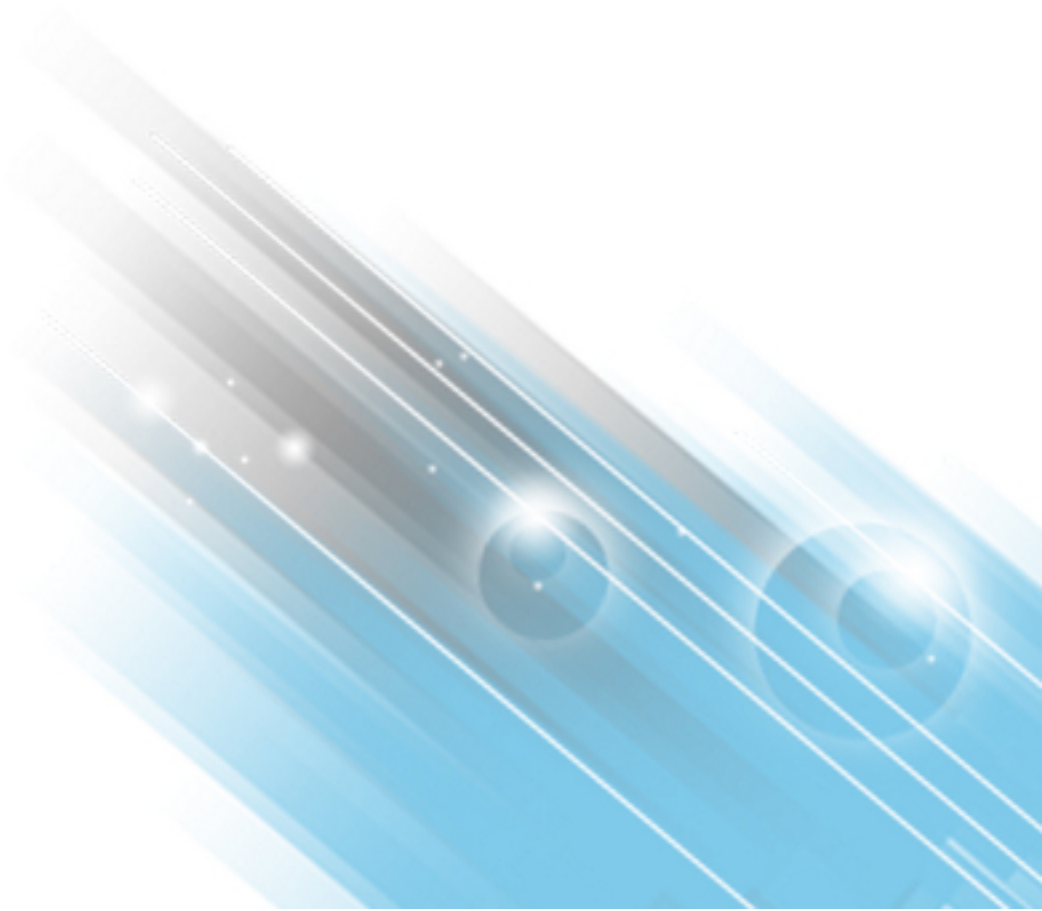
HP ArcSight Risk Insight

Software Version: 1.1
Linux Operating System

Administration Guide



November 27, 2015

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 hostnames) is for illustration purposes only.

HP ArcSight products are highly flexible and function as you configure them. The accessibility, integrity, and confidentiality of your data is your responsibility. Implement a comprehensive security strategy and follow good security practices.

This document is confidential.

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 acknowledgements:
https://www.protect724.hpe.com/docs/DOC-13026

Support

Contact Information

Phone	A list of phone numbers is available on the HP ArcSight Technical Support Page: https://softwaresupport.hp.com/documents/10180/14684/esp-support-contact-list
Support Web Site	https://softwaresupport.hp.com
Protect 724 Community	https://www.protect724.hpe.com

Contents

Chapter 1: Welcome to This Guide

Welcome to the ArcSight Risk Insight Administration Guide. This guide provides you information about day-to-day administrator tasks. Installation and initial configuration information can be found in the *ArcSight Risk Insight Deployment Guide*.

This guide is intended for the Risk Insight System Administrator. Readers of this guide should be knowledgeable about enterprise system administration and 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.

Getting Started

The following list includes step by step instructions for fully configuring Risk Insight. After Risk Insight is fully configured, you will be able to view near real-time risk factor information in the various dashboards.

1. Integrate with ESM and import assets, as described in the *Integrate with ArcSight Enterprise Security Manager* section of the *ArcSight Risk Insight Deployment Guide*. This task is usually done during the deployment phase.

2. After you have successfully imported assets for the first time, create the business model, as described in the *How to Build a Business Model* section in the *ArcSight Risk Insight User Guide*.

   For an overview on the business model, see the *Asset Profiling* chapter in the *ArcSight Risk Insight User Guide*.

3. Plan which risk factors you want to monitor, and do the following:

   a. Create risk factor reports in ESM, as described in the *Create an ESM Risk Factor Report* section in the *ArcSight Risk Insight Deployment Guide*.

   b. Define risk factors in Risk Insight, as described in the *Import Risk Information from External Sources* section in the *ArcSight Risk Insight Deployment Guide*.

4. Create dashboards that reflect the risk factor information that you want to display, by either creating a new dashboard or by customizing an existing dashboard:

   a. Create a new dashboard:

      i. Create a dashboard report in BusinessObjects for each component that you want to display in the dashboard, as described in the *Create a Report Using SAP BusinessObjects Web Intelligence* section in the *ArcSight Risk Insight User Guide*.

      ii. Create a new dashboard based on the reports that you created in BusinessObjects, as described in "Create a Customized Dashboard Page" on page 15.

      iii. To create dashboards or dashboard components that display risk factor KPIs, see "Create a KPI" on page 9.

   b. Edit an existing dashboard:

      i. Create a dashboard report in BusinessObjects for each component that you want to display in the dashboard, as described in the *Create a Report Using SAP BusinessObjects Web Intelligence* section in the *ArcSight Risk Insight User*

Guide.

ii. Edit the page layout, as described in "Edit Page Layout" on page 19.

iii. Add or remove components from the dashboard as described in "Create a Customized Dashboard Page" on page 15.

Chapter 2: KPI Management

You can create, edit, or delete key performance indicators (KPIs). For an overview of KPIs, see the *Key Performance Indicators* section in the *ArcSightRisk Insight User Guide*.

Create a KPI

You can create a KPI for any risk factor. Creating a KPI consists of three steps:

1. Creating a KPI report in BusinessObjects based on a KPI template. For more information, see "Create a KPI Report in BusinessObjects" below.
2. Defining the KPI in the KPI Management page. For more information, see "Define a KPI" on the next page.
3. Creating a KPI dashboard component and add it to an existing or new dashboard. For more information, see "Create a KPI Dashboard Component" on page 12.

Create a KPI Report in BusinessObjects

The first step in creating a KPI is creating its report in BusinessObjects.

Note: To create an Risk Insight report you must be familiar with the process of creating reports in *BusinessObjects*.

For general instructions on creating Risk Insight reports in BusinessObjects, see the *Create a Report Using SAP BusinessObjects Web Intelligence* section in the *ArcSight Risk Insight User Guide*.

To create a KPI report

1. Login to BusinessObjects InfoView (BusinessObjects web-based client tool) using following URL: `http://server_name:8081/InfoViewApp`
2. In the main window, click **Document List**, expand **Public Folders**, and then click **ArcSight Risk Insight Reports**. All Risk Insight reports are displayed in the right pane.
3. In the **Search title** box, search for **Risk Factor KPI Template**. This template is specific for KPIs for risk factors. Use this template to create risk factor KPI reports. This template enables you to create a report with an asset prompt, a KPI prompt, and a risk factor prompt, meaning that both the asset and the risk factor can be selected dynamically in the dashboard.

The search is not case-sensitive.

4. In the search results, right-click the template that you selected, and then click **Modify**. Confirm the execution of SAP BusinessObjects Web Intelligence java plugin if the browser prompts for that.

5. In the **Prompts** dialog box, click **Cancel**.

6. In the main window, click **Save > Save As** to display **Save Document** dialog box.

7. Enter a meaningful name for the report that reflects the KPI. The name of the report will be displayed in the KPI Management page in Risk Insight. Click the **Categories** tab, ensure the **KPI** check-box is selected, and then click **OK** to confirm the save of new report.

   Note: You must select the KPI check-box in order to display this report in Risk Insight.

8. In the main window, on the toolbar, click **Edit Query**.

9. In the Edit Query mode, drag objects from the left pane to the right pane in order to create the query. For more information on creating queries, see *Building Reports with BusinessObjects Web Intelligence User Guide*.

   Note: Do not edit the **Thresholds** query. The query currently being edited is displayed as tab on the bottom of main window.

10. Click **Run Query**.

11. In the main window in **Edit Report** mode, drag the object that represents the KPI score from the **Data** pane into the **Percentage** cell in the right pane.

12. In the main window, click **Save**.

    After you create the report you can define the KPI in Risk Insight. For more information, see "Define a KPI" below.

Define a KPI

Before you define a KPI in Risk Insight, you need to create a KPI report in BusinessObjects. For more information, see "Create a KPI Report in BusinessObjects" on the previous page.

To define a KPI

1. Click **Administration > KPI Management**.

2. In the **KPI Management** window, in the left pane, click **New**.
3. In the **Display Name** box, enter a meaningful name for the KPI. This name will be displayed in the KPI component as the title.
4. In the **Description** box, enter a description for the KPI. You can embed the KPI parameter into the description by using the string: {0}.

   For example, if the **KPI Parameter** is 20, and the description is “The percentage of assets with an overall score higher than {0}”, then the description displayed is “The percentage of assets with an overall score higher than 20”.
5. From the **BusinessObjects Report** list, select the KPI report that you created.
6. In the **KPI Parameter** box, enter the threshold that indicates a desirable or an undesirable result.

   For example, in a KPI that displays the percentage of assets with an overall score higher than 20, then “20” is the KPI Parameter. In this case, scores that are higher than 20 are not desirable.

   Note: The KPI parameter is not mandatory for all KPIs; it depends on the report that you created in BusinessObjects. make sure that if the KPI requires a parameter that you enter one, otherwise the corresponding KPI dashboard component will not display properly.
7. Drag the **Thresholds** sliders to define the severity of the percentage ranges, for low, medium, and high thresholds.

   These thresholds are reflected in the gauge that represents the KPI and they define whether the KPI is acceptable or not. For example, If the KPI is the percentage of assets with a maturity score over 3.5. If the low range is 0 – 40, the medium range is 40-70, and the high range is 70-100, and the percentage of maturity score over 3.5 is 30%, and the KPI will be colored in green, which means that it is acceptable.
8. To define the directionality of the score severity, select one of the following options:
   - **A lower score is better**: Meaning that a score within the low threshold will be displayed in green and a high score in red.
   - **A higher score is better**: Meaning that a score within the low threshold will be displayed in red and a high score in green.
9. From the **Belongs to module** list, select the module to which the KPI belongs. This defines in which settings page the KPI is added. For example, if you created a KPI for the overall score, then it will be added to **Settings > Executive View**.
10. Click **Save**.

Create a KPI Dashboard Component

You can create a KPI dashboard component and add it to an existing or a new page.

To create a KPI dashboard component

1. Click **Administration > Dashboard Builder**.

   The **Dashboard Builder** opens in a new window.

2. On the **Dashboard Builder** window, select one of the following:

   - **Create a new page**
   - **Open an existing page**

3. Configure the page layout, as described in "Configure Page Layout" on page 16.

4. In an empty layout area, click the **Add Component**  button.

5. In the **Component Gallery** dialog box, in the left pane, select the **Executive View** category.

6. From the right pane, drag the **KPI** component to the empty layout space.

7. Close the **Component Gallery** dialog box.

8. In the **KPI** component, from the **KPI** list, select the KPI you want to use in the dashboard that you are creating.

   The Asset and Risk Factor parameters are enabled according to the KPI report. If one or both of them is required, then they are marked as mandatory.

9. Select a parameter:

   - To create a KPI dashboard for a specific asset/risk factor, select **Select a Specific Asset** or **Select a Specific Risk Factor**.
   - To create a dynamic report/dashboard, that receives the asset/risk factor as a parameter using the wiring capability, select **Set up wiring between this component and an Asset Selector component** or **Set up wiring between this component and a Risk factor Selector component**.

   Note: If the report requires an **Asset** parameter and you selected **Set up wiring between this component and an Asset Selector component**, then you must add an **Asset Selector** component to the page. If the report requires a **Risk Factor** parameter and an **Asset**

parameter and you selected **Set up wiring between this component and a Risk Factor Selector component**, then you must add a **Risk Factor Selector** component to the page.

10. To remove a component from a page, select a component, and then click the **Remove Component**  button.
11. Click **Create**.
12. Save the page, as described in "Save Page" on page 18.

Edit a KPI

You can edit a KPI in the KPI Management page. You can also configure the KPI parameter and thresholds from Settings, as described in the *Configure KPI Settings* section in the *ArcSight Risk Insight User Guide*.

To edit a KPI

1. Click **Administration > KPI Management**.
2. In the **KPI Management** window, in the left pane, from the list of KPIs, click the KPI that you want to edit.
3. Make the necessary changes to the KPI, and then click **Save**.

Delete a KPI

You can delete both out-of-the-box and user-created KPIs. Before you delete a KPI you must remove all of the KPI dashboard components from dashboard pages, otherwise, you will not be able to delete it.

Note: Deleting a KPI does not delete the KPI report in BusinessObjects.

To delete a KPI

1. Click **Administration > KPI Management**.
2. In the **KPI Management** window, in the left pane, from the list of KPIs, click the KPI that you want to delete.

3. Click the **Delete**  button.

Chapter 3: Create a Customized Dashboard Page

In addition to the dashboards already defined in Risk Insight, you can create a customized dashboards using the BusinessObjects Reports component. The BusinessObjects Reports component includes predefined BusinessObjects reports, in addition to any existing user-created reports. For more information on creating Risk Insight reports in BusinessObjects, see the *Create a Report Using SAP BusinessObjects Web Intelligence* section in the *ArcSight Risk Insight User Guide*.

To create a customized dashboard page

Note: Before you begin, plan which components you want to use and how to arrange them on the page.

1. Click **Administration > Dashboard Builder**.

   The **Dashboard Builder** opens in a new window.

2. In the **Dashboard Builder** window, click the **New Page**  button.

3. Configure the page layout, as described in "Configure Page Layout" on the next page.

4. In an empty layout area, click the **Add Component**  button.

5. In the **Component Gallery** dialog box, in the left pane, select the **Executive View** category.

6. From the right pane, drag the **BusinessObjects Reports** component to the empty layout space.

7. Close the **Component Gallery** dialog box.

8. In the BusinessObjects Reports component, from the **Reports** list, select the report you want to use in the dashboard that you are creating.

9. If the report requires parameters, select one of the following:

   Note: If the report does not require parameters, skip this step.

   - To create a report/dashboard for a specific asset, select **Select a Specific Asset**.
   - To create a dynamic report/dashboard, that receives the asset as a parameter using the wiring capability, select **Set up wiring between this component and an Asset Selector component**. For more information on wiring, see "Set Up Wiring Between Components" on page 22.

Note: If the report requires an **Asset** parameter and you selected **Set up wiring between this component and an Asset Selector component**, then you must add an **Asset Selector** component to the page.

10. Click **Create**.
11. Name the component that you created by doing the following:
    a. From the component toolbar, click the **Component Menu** button and then click **Preferences**.

       The **Component Menu** button is located in the component toolbar:

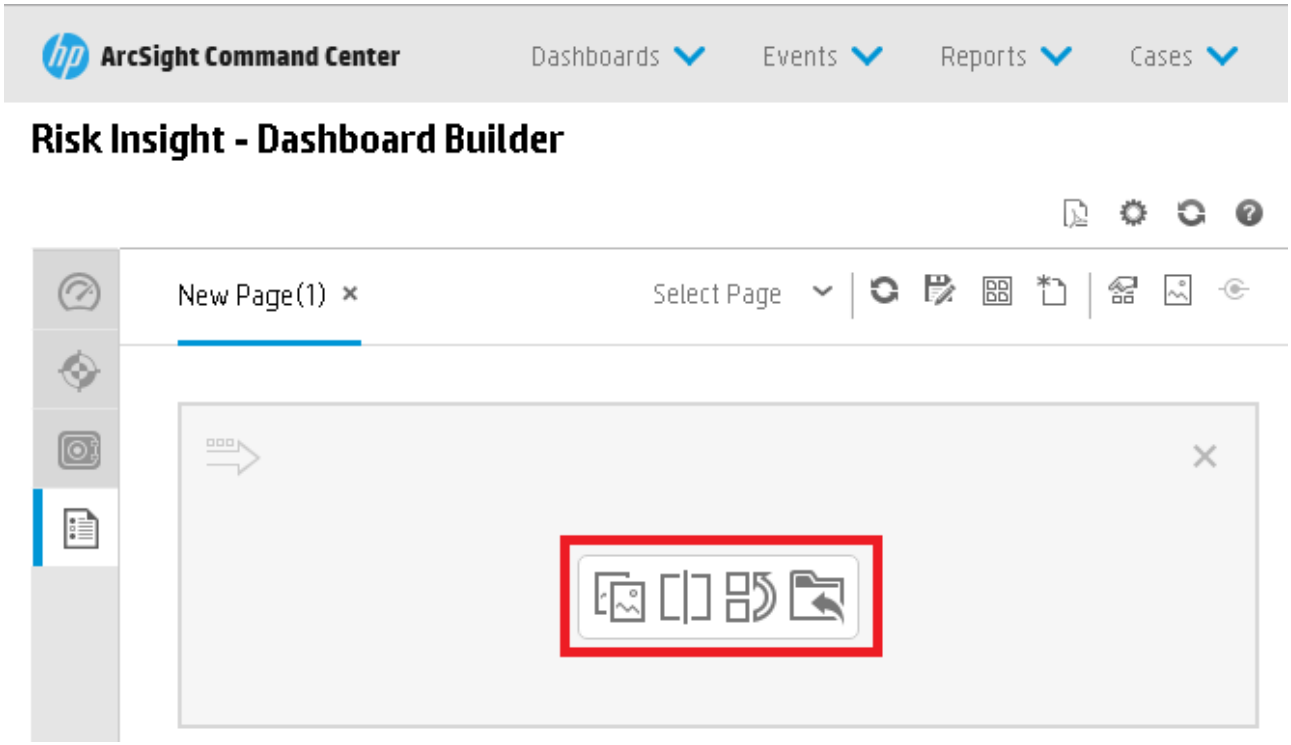
       

    b. In the **Preferences** dialog box, in the **Name** box, replace BusinessObjects Reports with a meaningful name.
    c. Click **OK**.

       The component name is updated. (The component name is displayed in the component toolbar in the top left side.)
12. To remove a component from a page, select a component, and then click the **Remove Component**  button.
13. Save the page, as described in "Save Page" on page 18.

Configure Page Layout

The layout refers to how components are arranged on a page. Risk Insight enables you to define each layout as horizontal (components are displayed side by side), vertical (components are displayed one above the other), or in tabbed areas. When a layout is empty, the layout tools in the middle of the page enable you to define the layout.



To configure page layout

On the new page, use the layout tools to configure the layout, as described in the following table.

Note: You can drag components from the Component Gallery to the required section on the page.

Layout tool	Description
	**Split** Click to divide a vertical layout into two layouts, one above the other.
	**Split** Click to divide a horizontal layout into two layouts, side by side.
	**Switch to Horizontal** Click to change the layout from vertical or tabbed to horizontal. Components placed in this area will be added side by side.
	**Switch to Vertical** Click to change the layout from horizontal or tabbed to vertical. Components placed in this area will be added one above the other.

Layout tool	Description
	**Switch to Tabs** Click to change the layout from vertical or horizontal, to a tab layout. Components placed in this area will be added as tabs.
	**Add Component** Click to open the Component Gallery. You can then double-click a component to place it in the layout area.
	**Remove Layout** Click to remove a layout from the page.

Save Page

Save the page to the Page Gallery.

To save a page

1. On the Risk Insight toolbar, click the **Save or Save as**  button.
2. In the **Save to Page Gallery** dialog box, do the following, and then click **OK**:
   a. In the **Name** box, enter a name for the page. This is the name that is displayed in Risk Insight.
   b. If you are saving the page as a new page, select the **Save as new page** check box.
   c. In the **Description** box, if necessary, enter a description. The description appears as a tooltip for the page, within the Page Gallery.
   d. From the list of categories, select the category to which the page belongs. If you do not select a category, the page will be added to the **Not Categorized** group.

   Note: Pages that are saved to a specific category are displayed under that category in the Risk Insight Home page and in the navigation bar. Pages in the **Not Categorized** group are not displayed.
3. Refresh your browser to display the list of saved pages.

Edit Page Layout

To edit page layout

1. Select the page that you want to lay out again from the **Select Page** list on the Risk Insight toolbar.
2. Click the **Edit Page Layout**  button.

   The components are hidden and the layout of the page is displayed.
3. Lay out the page again using the layout tools, as described in "Configure Page Layout" on page 16, and then click the **Edit Page Layout**  button to exit editing.
4. Save the page. For more information, see "Save Page" on the previous page.

Manage Pages

Pages are collections of components that are displayed together and that interact with one another.

Default pages are located in the Page Gallery, together with any pages you created and saved. Through the Page Gallery, you can select a page, open it in the Risk Insight workspace, assign pages to categories, and clone or delete pages. You can delete only user-created pages.

To assign a page to a category

1. On the Risk Insight toolbar, click the **Page Gallery**  button.
2. In the **Page Gallery** dialog box, select the category check box from the categories on the left side, and then select the page.
3. Click the **Categorize Page**  button. Select the category check box, and then click **OK**.

To clone a page

1. On the Risk Insight toolbar, click the **Page Gallery**  button.

2. In the **Page Gallery** dialog box, select the category check box from the categories on the left side, and then select the page.

3. Click the **Clone Page**  button.

To delete a page

1. On the Risk Insight toolbar, click the **Page Gallery**  button.

2. In the **Page Gallery** dialog box, select the category check box from the categories on the left side, and then select the page.

3. Click the **Delete Page**  button. A confirmation message is displayed. Click **Yes**.

Manage Components

Components are areas on a page that display information relevant to Risk Insight users' business tasks. The Component Gallery contains components that can be used within Risk Insight, grouped by categories. You can add, edit and delete user-created component categories through the Component Gallery, as described in "Manage Component Categories" below. You can also create external components, as described in "Create an External Component" on the next page.

Each component has permissions that are relevant to the function that it provides. When you create a new page, the components that you choose define which roles will be able to access the page. Only users with roles that include permissions for all of the components on the page are granted access to that page.

Manage Component Categories

You can add, rename, and delete user-created component categories through the Component Gallery.

To create a new component category

1. On the Risk Insight toolbar, click the **Components**  button.

2. In the **Components Gallery** dialog box, click the **New Category**  button on the top left side.

3. In the **New Category** dialog box, in the **Name** field, enter a name for the category that you are creating, and then click **OK**.

To rename a component category

1. On the Risk Insight toolbar, click the **Components**  button.
2. In the **Components Gallery** dialog box, from the list of categories on the left side, select the check box for the category that you want to rename, and then click the **Edit Category Name**  button.
3. On the **Edit Category Name** dialog box, in the **Name** field, enter a new name for the category, and then click **OK**.

To delete a component category

1. On the Risk Insight toolbar, click the **Components**  button.
2. In the **Components Gallery** dialog box, from the list of categories on the left side, select the check box of the category you want to delete, and then click the **Delete Category**  button. A confirmation message is displayed. Click **Yes**.

   Any components that belonged to this category are now in the **Not Categorized** group.

Create an External Component

The following procedure describes how to create a component using a URL. You must use a static URL, where the component simply opens the URL that you enter. The URL for an external component must begin with one of the following protocols:

- https://
- http://
- ftp://

To create an external component

1. On the Risk Insight toolbar, click the **Components**  button.
2. In the **Components Gallery** dialog box, in the right pane, click the **Add External Component**  button.

3. In the **New Component** dialog box, do the following, and then click **OK**:

   a. In the **Name** field, enter a name for the component.

   b. In the **URL** field, enter the URL.

   c. Click **Categorize Component** to expand the section. Select the check box of the category to which you want to add the component or click the **New Category**  button to create a new one.

Set Up Wiring Between Components

The interaction between components on a page in Risk Insight is called wiring. After you place components on a page, you can define how components interact with one another. For example, you can set up a page so that if you select an asset in one component (source), the other components on the page display information relating to that asset (target).

Default pages have predefined wiring. You can define wiring for user-created pages in addition to modifying default wiring definitions.

To set up wiring between components

1. Do one of the following:

   - On the Risk Insight toolbar, click the **Page Wiring**  button.

     OR

   - **To set up wiring from the source component**, on the top right side of the component, click the **Component Menu**  button, and then click **Wiring**. This option is only available when a component can function as a source component; if it only functions as a target component, then the Wiring option is disabled. The capability of a component as a source, target or both is defined within Risk Insight and cannot be changed.

2. In the **Wiring** dialog box, do the following, and then click **OK**:

   a. If there is more than one potential source component, from the **Source Components** area, click the component that you want to set as the source. If you are setting up the wiring from the source component, then this area does not display.

   b. In the **Target Components** area, select the check boxes of all the target components that you wire to the source. To remove wiring, clear the relevant check boxes.

Dashboard Builder Toolbar

The Dashboard Builder toolbar enables you to create customized dashboards.

The following table describes the toolbar's functionality.

UI Element	Description
	Select a page from this list to open the page in your workspace. The list contains the dashboards that are defined in the Page Gallery. The list is narrowed when you start typing a page name in this box.
	**Refresh** Click to refresh the page.
	**Save or Save As** Click to save the current page to the Page Gallery. A dialog box enables you to name the page, give the page a description, and select a category for the page. The description appears as a tooltip for the page in the Page Gallery. For more information, see "Save Page" on page 18.
	**Page Gallery** Click to open the Page Gallery. The Page Gallery contains default pages, as well as pages you have saved. You can then edit page definitions, or open pages. For more information, see "Manage Pages" on page 19.
	**New Page** Click to create a new page. After opening a new page, you can configure its layout and add components. For more information, see "Create a Customized Dashboard Page" on page 15.
	**Edit Page Layout** Click to modify the layout of an existing page. Use the Layout tools in the top left corner of each layout to modify the layout areas. For more information, see "Edit Page Layout" on page 19. **Exit Editing** When you are done, click this button to stop editing.
	**Components** Click to open the Component Gallery, which contains default components, as well as components you have added. You can edit component definitions, or add components to a page. For more information, see "Manage Component Categories" on page 20.

UI Element	Description
	**Page Wiring** Click to define the wiring between components; this determines how components interact with one another. For more information, see "Set Up Wiring Between Components" on page 22.

Manage SAP BusinessObjects Report Settings

The BusinessObjects reports settings are configured during the installation of Risk Insight.

Note: If these settings are changed in BusinessObjects, then you must update this information manually in Risk Insight.

To update BusinessObjects reports settings

1. Click **Administration > Configuration**.
2. In the **Configuration** module, in the left pane, click **BusinessObjects > Report Settings**.
3. In the right pane, make the necessary changes to the Shared Secret parameter.

   Note: The Shared Secret parameter is located in the Authentication > Enterprise area of SAP Business Objects.

4. Save and apply the configuration changes. For more information, see the *Save and Apply Configuration Changes* section as described in *ArcSight Risk Insight Deployment Guide*.

Chapter 4: Job Management

You can use the Job Management module to perform the following tasks:

- **Launch batch jobs manually**

  Generally, batch jobs are scheduled to run automatically through the Risk Insight Configuration module. However, you can also launch jobs manually when required, for example, in order to re-run a job that failed or in order to test a job in a test environment. For more information, see "Launch Batch Jobs Manually" on page 27.

- **Troubleshoot batch jobs**

  You can inspect the details of each step that comprises the job in order to identify where it failed. For more information, see "Troubleshoot Batch Jobs" on page 27.

The following table includes all the batch jobs defined in Risk Insight.

Batch Job	Description
EsmAssetSyncJob	ArcSight ESM Asset Synchronization Job For more information, see the *About ArcSight ESM Asset Synchronization Job* section in the *ArcSight Risk Insight Deployment Guide*
VulnerabilitiesImportJob	Vulnerability Import Job For more information, see the *About Import Vulnerability Job* section in the *ArcSight Risk Insight Deployment Guide*
DictionaryInfoImportJob	Dictionary Information Import Job For more information, see the *About the Dictionary Information Import Job* section in the *ArcSight Risk Insight Deployment Guide*
ArchiveAuditLogDataJob	Archive Audit Log Job For more information, see "About Archive Audit Log Job" on page 32
ExtractDataToArchiveJob	Archive Trend Data Job For more information, see "Archive Trend Data" on page 30
RestoreIndexesJob	Restore Indexes Job For more information, see "Restore Search Engine Indexes" on page 37

Batch Job	Description
<Risk Factor Name>ImportJob	<Risk Factor Name> Import Job For more information, see the *About Risk Factor Import Job* in the *ArcSight Risk Insight Deployment Guide*.
<Risk Factor Name>ArchiveJob	Archive Risk Factor Job For more information, see "Archive Trend Data" on page 30

Launch Batch Jobs Manually

To launch batch jobs manually

1. In Risk Insight click **Administration > Job Management**, and then, from the toolbar, click **Jobs**.
2. From the **Jobs Names Registered** table, click the job that you want to launch.
3. In the **Job Parameters** box, the timestamp that is displayed belongs to the last batch job that was run. Increment the timestamp by 1, and then click **Launch**.

   Note: If the job is not scheduled or if this is the first time that you are running this job, then enter "**Key=n**", where n is a unique number.

   The job instance is displayed in the **Job Instances for Job** table with a **Started** status.
4. To stop the batch job before it is completed, in the **Job Instances for Job** table, identify the job instance that you want to stop, click the **Started** status in the **LastJob Execution** column, and then click **Stop**.
5. To view the progress of the batch job and the status of each of its steps, in the **Job Instances for Job** table, identify the job instance, and click the status in the **LastJob Execution** column. A table with the job steps is displayed on the bottom of the page.

Troubleshoot Batch Jobs

You can inspect the details of each step that comprises the job in order to identify where it failed.

To troubleshoot batch jobs

1. In Risk Insight click **Administration > Job Management**, and then, from the toolbar, click **Executions**.
2. From the **Recent and Current Job Executions** table, identify the job that you want to inspect and click on the **Executions** link in the **ID** column.

   The **Details for Job Execution** page displays the following information:

   - Details on the job level.
   - A table that includes all the job steps and their statuses.

3. From the job steps table, identify the step with the **Failed** status, and in the **Status** column click the **Failed** link.

   The **Step Execution Progress** page displays detailed information on the step:

   - **History for Step Execution for Step**: Displays the history of the execution of this step across all job executions.
   - **Details for Step Execution**: Displays the meta data for this step, in addition to an extract of the stack trace from any exception that caused the failure of the step.

Chapter 5: Audit Log

The audit log enables you to track user initiated and automatic actions performed in Risk Insight. You can view the audit log through the Risk Insight user interface. The information presented in the log can be filtered according to different parameters, such as date and time, user name, or the page on which the action was performed. By default, the audit log records are sorted by date and time in descending order. You can sort the records according to any one of the parameters by clicking the parameter title.

The Administrator can view all actions in the audit log, but all other users can view only actions that they performed.

Click the **Export to CSV File**  button to export the audit log to a CSV file. The information included in the file is based on the filter that you set.

The following table includes a description of the parameters that comprise the audit log.

Parameter	Description
From Date	The date and time on which the action occurred.
Module	The module in which the action occurred. These include: , **Vulnerabilities**, **Settings**, **Assets**, **Administration**.
User Name	The Risk Insight user name of the user that performed the action. If the action was preformed automatically, then the user name is empty.
Page	The page on which the user performed the action. For example, if the user added an asset to the business model, then the page is Asset Profiling.
Action	The action that the user performed.
Success	Indicates whether the action was successful or a failure, **Yes** or **No**.
Method	One of the following options: • **Manual**: the action was initiated by a user. For example, a user changes the properties of an asset. • **Automatic**: the action was initiated by the system. For example, when a vulnerability is automatically closed or reopened.
Description	Specific information about the action. For example, the name of a vulnerability.

Chapter 6: Archive Data

You can archive the following data:

- Trend data. For more information, see "Archive Trend Data" below.
- Audit log. For more information, see "Archive the Audit Log" on page 32.

Archive Trend Data

Risk Insight dashboards include trend charts which are used to show a general pattern of change in data over time. Displaying data over time helps you understand performance and compare it to your organization's established objectives.

To support the trend charts, Risk Insight archives data for all assets for the following measurements:

- Scores and aggregate scores for any risk factor defined in Risk Insight
- Aggregate vulnerability score

The corresponding trend charts for these measurements are displayed in the following dashboards:

Measurement	Trend Chart	Dashboard Name
Risk factor	Aggregate Risk Factor Score Over Time	Risk Factors Dashboard
Aggregated vulnerability score	Aggregated Vulnerability Score Over Time	Vulnerability Dashboard

Archiving vulnerabilities and risk factors is done differently.

- **Vulnerabilities**

  Vulnerability data is archived by using job: **ExtractDataToArchiveJob**. You can configure Risk Insight to archive vulnerability trend data on a weekly basis, as described in "Schedule and Activate the Archive Trend Data Job" on the next page. You can also archive trend data at any time by manually running the **ExtractDataToArchiveJob**. To run a job manually, see "Launch Batch Jobs Manually" on page 27. If the job is scheduled to run more than once a day, only the scores from the last job are reflected in the trend chart.

- **Risk factors**

  Each risk factor has a separate archiving job. The job name is <Risk Factor>ArchiveJob. You can configure Risk Insight to archive trend data of risk factors, as described in "Configure the Risk Factor Archive Settings" on the next page.

Schedule and Activate the Archive Trend Data Job

Note: The Archive Trend Data Job archives vulnerability scores; it does not archive information for imported risk factors.

For information on archiving trend data, see "Archive Trend Data" on the previous page.

To schedule and activate the job

1. Click **Administration > Configuration**.
2. In the left pane, click **Archive > Schedule Job**.
3. In the **Schedule Job** page, do the following:
   - Select the **Activate Job** check box.
   - From the **Day** list, select the day of the week on which you want to run the job.
   - From the **Hour** list, select the hour in the day on which to run the job.

     Note: While the job runs, you cannot make any changes in the system. Make sure to consider this when selecting the time of day.
4. Save and apply the configuration changes. For more information, see the *Save and Apply Configuration Changes* section as described in *ArcSight Risk Insight Deployment Guide*.

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

Configure the Risk Factor Archive Settings

Note: The <Risk Factor> Archive Job archives data for risk factor information; it does not archive information for vulnerabilities.

For information on archiving trend data, see "Archive Trend Data" on the previous page.

To configure the archive settings

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 **Archive**.
3. In the **Archive** page, do the following:
   - If you want to archive scores immediately after information is imported into Risk Insight, then select the **Archive immediately after import** check box. Selecting this option adds another snapshot to the archive and affects this factor's trend charts.
   - Select the **Activate Job** check box.
   - In **Job Schedule**, select the options for the recurrence pattern you want (every number of minutes, every number of hours, every number of days, or on certain days of the week).

     Note: HPE recommends that you schedule the job to run no more than once a day. If you import information more than once a day, only the last import will be saved.
4. Save and apply the configuration changes. For more information, see the *Save and Apply Configuration Changes* section as described in *ArcSight Risk Insight Deployment Guide*.

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

Archive the Audit Log

You can archive the Risk Insight audit log in order to keep it in a manageable size. You can either schedule the Archive Audit Log Job to run at a certain time or you can run it manually through the Job Management module. For information on scheduling the job, see "Schedule and Activate the Archive Audit Log Job" on the next page. For information on running the job manually, see "Launch Batch Jobs Manually" on page 27.

The archived data is kept in Risk Insight database in the **RC_EV_AUDIT_LOG_ARCHIVE** table. You can choose to delete the data in the archive table. For more information, see "Configure Archive Audit Log Job Settings" on the next page.

For more information on the Archive Audit Log Job, see "About Archive Audit Log Job" below.

About Archive Audit Log Job

The Archive Audit Log job periodically archives the audit log as follows:

1. Data from the audit log table (RC_EV_AUDIT_LOG) is extracted and written to the audit log archive table (RC_EV_AUDIT_LOG_ARCHIVE). You can determine the scope of data in the Configuration module. For more information, see "Configure Archive Audit Log Job Settings" on the next page.
2. The archived data is deleted from the audit log table (RC_EV_AUDIT_LOG).

3. Depending on how you configured the job settings, data is deleted from the archive table (RC_EV_AUDIT_LOG_ARCHIVE).

Configure Archive Audit Log Job Settings

You can configure the scope of the data that you want to archive.

To configure the job settings

1. Click **Administration > Configuration**.
2. In the left pane, click **Audit Log > Archiving Settings**.
3. To archive data, select one of the following options:
   - **Archive All**: Select this check box if you want to archive the entire audit log table. This means that the entire audit log table will be deleted after the archiving is complete.
   - **Archive Data Older Than (Days)**: Enter the number of days for which you want to save data in the audit log table. Older data will be archived.

   Note: If you selected **Archive All** then it overrides any value entered in **Archive Data Older Than (Days)**. If neither of these options are selected, then the audit log will not be archived.
4. To delete archived data, select one of the following options:
   - **Delete All Archived Data**: Select this check box if you want to delete the entire archive table.
   - **Delete Data Older Than (Days)**: Enter the number of days for which you want to save data in the archive table. Older data will be deleted permanently from Risk Insight.

   Note: If you select **Delete All Archived Data** then it overrides any value entered in **Delete Data Older Than (Days)**. If neither of these options are selected, then the archive table will not be deleted.
5. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 39.

Schedule and Activate the Archive Audit Log Job

After you define the job settings, you can schedule and activate the Archive Audit Log job.

For more information on the flow of the job, see "About Archive Audit Log Job" on the previous page.

To schedule and activate the job

1. Click **Administration > Configuration**.
2. In the left pane, click **Audit Log > Archiving Settings**.
3. In the right pane, select the **Activate Job** check box.
4. In **Job Schedule**, select the options for the recurrence pattern you want (every number of minutes, every number of hours, every number of days, or on certain days of the week).
5. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 39.

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

Chapter 7: Update the Vulnerability Dictionary

The Risk Insight labs regularly release vulnerability dictionary updates. For more information about the vulnerability dictionary, see the *Vulnerability Dictionary* section in the *ArcSight Risk Insight User Guide*.

To update the vulnerability dictionary, contact your Risk Insight sales representative.

A vulnerability dictionary update includes new vulnerabilities and updated information for existing vulnerabilities. Updated information can be anything from a different title to a score. When you update the dictionary, the entire Vulnerabilities module is updated. Meaning that if the value of any property of the vulnerability has changed (such as the score), then this change will be reflected in all the open vulnerabilities in Risk Insight. Closed vulnerabilities are not updated. If you choose to reopen a closed vulnerability, then it will be updated with the new vulnerability information.

The Dictionary Information Import Job parses and loads the updates to Risk Insight. For more information, see "About the Dictionary Information Import Job" below.

To update the vulnerability dictionary

1. Obtain the **DictionaryInfo.zip** file from your Risk Insight sales representative and copy it to the following location:

   <Risk Insight installation folder>\vm\import\dictionary

   Note: Do not change the file name or content.

2. Run the **DictionaryInfoImportJob**, as described in "Launch Batch Jobs Manually" on page 27.

   Note: By default, the Vulnerability dictionary is not populated during installation to minimize the initial setup deployment time. The initial **DictionaryInfo.zip** is in the corresponding folder.

   Run **DictionaryInfoImportJob** with the **timestamp=1** parameter to populate the dictionary with initial data on vulnerabilities.

About the Dictionary Information Import Job

The Dictionary Information Import Job imports new and updated vulnerability data from files provided by the Risk Insight labs into the Risk Insight database, as follows:

1. The **DictionaryInfo.zip** file is extracted.
2. The version of the package is checked.
   - If the version of the package is lower than the version that exists in the Risk Insight database, then no change is made in the database and the process proceeds to step 4.
   - If the version of the package is higher than the version that exists in the Risk Insight database, then the process proceeds to the following step.
3. The vulnerability dictionary tables in the Risk Insight database are updated. The version of the vulnerability dictionary records is updated.
4. Open vulnerabilities in Risk Insight are updated, if any of their properties have changed.
5. The **DictionaryInfo.zip** file is renamed to **DictionaryInfo<date>.zip.old**.

Chapter 8: Restore Search Engine Indexes

The search engine used in the vulnerability dictionary is based on indexing. Risk Insight includes an index restoration job in case the index files become corrupted or in case the entire file system becomes corrupted. If the search functionality in the vulnerability dictionary does not work properly, then it might indicate that the index files are corrupted. In this case, we recommend running the **RestoreIndexesJob**.

The job retrieves vulnerability data from the Risk Insight database, creates indexes, and writes them to the relevant files in Risk Insight.

To restore search engine indexes

1. Stop the Risk Insight service.
2. Delete the following folder:

   <Risk Insight Installation Folder>\Indices

3. Start the Risk Insight service.
4. Run the **RestoreIndexesJob** from the Job Management module, as described in "Launch Batch Jobs Manually" on page 27.

Chapter 9: 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.

Chapter 10: Security

Risk Insight is designed so that it can be part of a secure architecture, and can therefore meet the challenge of dealing with the security threats to which it might be exposed. This section includes procedures for implementing a more secure (hardened) Risk Insight.

Encrypt Password

If you want to change the credentials for accessing a database or an application in Risk Insight, then you need to encrypt the new password and copy it to the appropriate properties file.

The default encryption algorithm is compliant with the standards of FIPS 140-2. The encryption is accomplished by means of a symmetric key, through which the password is encrypted. The key itself is then encrypted using another key, known as a master key. For details on the parameters used in the encryption process, see "Encryption Properties" on page 1.

To encrypt a password

1. On the server running Risk Insight, from the command line, open the following location:

   <Risk Insight Installation Folder>\bin

2. Run the following utility:

   /encrypt-password.sh -p <new password>

3. Copy the encrypted password including the **<ENCRYPTED>** prefix to the password field in the relevant properties file in the **conf** folder (for example, to the **db.password** field in the **db.properties** file).

Update Encryption Properties

You can change the encryption properties in order to change the encryption algorithm.

Note: If you change the encryption algorithm, all previously encrypted passwords are no longer usable. After you change the encryption algorithm you need to:

- Create new encrypted passwords and copy them to the relevant properties files. For example, to the **db.password** field in the **db.properties** file.
- Modify all password configured through the Risk Insight Configuration module. For example, the password for the ArcSight ESM connector.

To update the encryption properties

Update of the encryption properties include fetching new SSL certificate from ESM in case it was re-issued or ESM was converted to FIPS mode.

1. Run command line script **generate-keys.sh** in the following location:

   <Risk Insight Installation Folder>\bin

   The following file is created:

   <Risk Insight Installation Folder>\security\encrypt_repository

2. Regenerate all the encrypted passwords, as described in "Encrypt Password" on the previous page.

3. In Risk Insight, click **Administration > Configuration**.

4. Modify all passwords configured via the Risk Insight Configuration module. For example, the password for the ArcSight ESM connector **(Administration > Configuration > Integrations > ArcSight ESM > Connector**).

5. Save the changes, as described in "Save and Apply Configuration Changes" on page 39

Send Documentation Feedback

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

Feedback on Administration Guide (Risk Insight 1.1)

Just add your feedback to the email and click send.

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

We appreciate your feedback!