HP EnterpriseView

For the Windows Operating System

Software Version: 2.5

Administration Guide

Document Release Date: April 2014

Software Release Date: April 2014

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

Copyright Notice

Trademark Notices

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

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Chapter 1: Welcome to This Guide

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

This guide is intended for the EnterpriseView System Administrator. Readers of this guide should be knowledgeable about enterprise system administration and information security concepts.

This guide includes the following chapters:

About EnterpriseView

EnterpriseView is a framework that enables Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) to analyze security risk information in a business context and prioritize actions to minimize that risk. By tying IT risk and compliance information to business services it ensures alignment with management objectives. EnterpriseView bridges the gap between IT operations and the security office by interconnecting and consolidating business processes across the organization and establishing a rational basis for decision making. This product incorporates a holistic, enterprise approach, streamlining and integrating risk, compliance, threat and vulnerability information, while providing a business context to executives. It anticipates threats and provides continuous monitoring, by regularly updating and testing security related functions.

The main modules in EnterpriseView are:

- **Policy and Compliance Management**: This module enables you to assess and audit the assets in your organization. Use the policy builder to create customized policies and the Statement of Applicability (SoA) feature to apply controls to assets. EnterpriseView includes out-of-the-box policies, such as Unified Compliance Framework (UCF) enabling "audit once - comply with many" functionality.

- **Risk Management**: This module enables you to manage all aspects of the risk life cycle. Use the flexible and expandable threat library to define the threats that may potentially harm your organization, create threat scenarios by assigning threats to assets, analyze the risk and specify its impact and likelihood, and mitigate the risk by using controls or other effective actions.

- **Vulnerability Management**: This module collects vulnerabilities from vulnerability assessment tools, removes duplicates, assigns them to assets, and prioritizes them accordingly, allowing you to manage the remediation process.

- **External Risk Factors**: This module enables you to import risk factor information from external sources, manage it and display it on top of the business model and in dashboards.

- **Asset Management**: Assets are the building blocks of the business model, which is the foundation for all core EnterpriseView functionality. The business model depicts the entire organization from high-level business assets to low-level IT assets, on which policy, risk, and vulnerability operations are performed. You can create the business model by synchronizing EnterpriseView with an external asset repository or by creating it by using the Assets module.

- **Dashboards and Reports**: This module includes sophisticated executive dashboards, such as Risk Register, and reports, and enables you to create your own customized dashboards and reports.

- **Task Management**: EnterpriseView enables you to create, manage, and monitor workflows. Use workflows to structure and streamline your organization’s processes and assign tasks to the relevant people.

Chapter 2: Update your EnterpriseView License

Before you begin, obtain a license for EnterpriseView from your support or sales representative and save a copy of the license on the EnterpriseView server

To update your license

1. Stop the EnterpriseView service.
2. On the EnterpriseView server, open the following folder from the command line:

   <**EnterpriseView installation folder>\bin**

3. Run the following command:

   upload-license.bat -f <full path to the location of the license file>

4. Start the EnterpriseView service.

Chapter 3: EnterpriseView Workspace

EnterpriseView comes with a variety of out-of-the-box dashboard pages, based on the common needs of IT and GRE personas, such as system administrators, auditors, and senior management. EnterpriseView administrators can create role-based dashboards for different types of users by mixing and matching components from the component gallery to form a rich UI experience. For each page, the administrator can define the layout of components on the page and their interaction with one another.

This section includes the following topics:

Create a Customized Dashboard Page

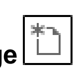
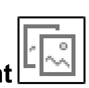
In addition to the dashboards already defined in EnterpriseView, you can create a customized dashboards using the BusinessObjects Reports component. The BusinessObjects Reports component includes predefined BusinessObjects reports, in addition to any existing user-created reports. For more information on creating EnterpriseView reports in BusinessObjects, see the *Create a Report Using SAP BusinessObjects Web Intelligence* section in the *HP EnterpriseView 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 page 12.
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/policy, select either **Select a Specific Asset** or **Select a Specific Policy**.

    - To create a dynamic report/dashboard, that receives the asset/policy as a parameter using the wiring capability, select either **Set up wiring between this component and an Asset Selector component** or **Set up wiring between this component and a Policy and Asset Selector component**. For more information on wiring, see "Set Up Wiring Between Components" on page 17.

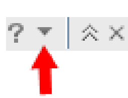
    Note: If the report requires an **Asset** parameter and you selected **Set up wiring between this component and an Asset Selector component**, then you must add an **Asset Selector** component to the page. If the report requires a **Policy** parameter and an **Asset** parameter and you selected **Set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

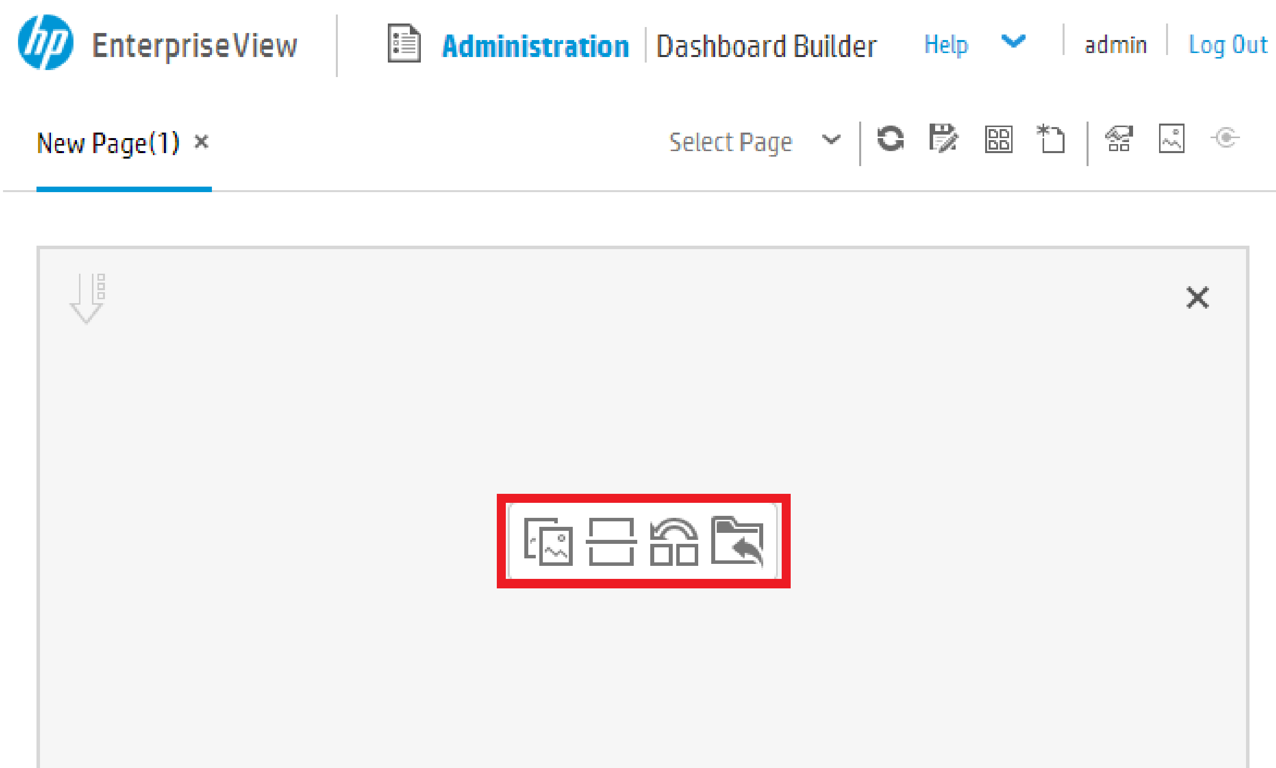
The component name is updated. (The component name is displayed in the component toolbar in the top left side.)

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 the next page.

Configure Page Layout

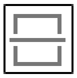
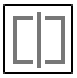
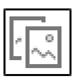
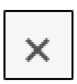
The layout refers to how components are arranged on a page. EnterpriseView enables you to define each layout as horizontal (components are displayed side by side), vertical (components are displayed one above the other), or in tabbed areas. When a layout is empty, the layout tools in the middle of the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

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 EnterpriseView 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 EnterpriseView 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 EnterpriseView 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 EnterpriseView 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**.

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 EnterpriseView 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 12, and then click the **Edit Page Layout** button to exit editing.

4. Save the page. For more information, see "Save Page" on page 13.

Manage Components

Components are areas on a page that display information relevant to EnterpriseView users' business tasks. The Component Gallery contains components that can be used within EnterpriseView, 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. For more information on the permissions of each page, see the *Roles and Permissions* section in the *EnterpriseView Deployment Guide*.

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 EnterpriseView 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 EnterpriseView 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 EnterpriseView 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 EnterpriseView 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 EnterpriseView 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 EnterpriseView 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 EnterpriseView and cannot be changed.

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

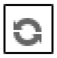
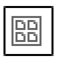
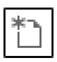
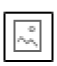
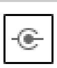
   a. If there is more than one potential source component, from the **Source Components** area, click the component that you want to set as the source. If you are setting up the wiring from the source component, then this area does not display.

   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 Page	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 13.
	**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 14.
	**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 10.
	**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 15. **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 15.
	**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 the previous page.

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 EnterpriseView 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 21.

- **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 21.

The following table includes all the batch jobs defined in EnterpriseView.

Batch Job	Description
CsvAssetSyncJob	CSV Asset Synchronization Job For more information, see the *About CSV Asset Synchronization Job* section in the *HP EnterpriseView Deployment Guide*
EsmAssetSyncJob	ArcSight ESM Asset Synchronization Job For more information, see the *About ArcSight ESM Asset Synchronization Job* section in the *HP EnterpriseView Deployment Guide*
UcmdbAssetSyncJob	UCMDB Asset Synchronization Job For more information, see the *About UCMDB Asset Synchronization Job* section in the*HP EnterpriseView Deployment Guide*
VulnerabilitiesImportJob	Vulnerability Import Job For more information, see the *About Import Vulnerability Job* section in the *HP EnterpriseView Deployment Guide*
DictionaryInfoImportJob	Dictionary Information Import Job For more information, see the *About the Dictionary Information Import Job* section in the *HP EnterpriseView Deployment Guide*

Batch Job	Description
ArchiveAuditLogDataJob	Archive Audit Log Job For more information, see "About Archive Audit Log Job" on page 35
ExtractDataToArchiveJob	Archive Trend Data Job For more information, see "Archive Trend Data" on page 32
VulnerabilitiesArchiveJob	Archive Vulnerabilities Job For more information, see "About the Vulnerabilities Archive Job" on page 37
RestoreIndexesJob	Restore Indexes Job For more information, see "Restore Search Engine Indexes" on page 71
<External Risk Factor Name>ImportJob	<External Risk Factor Name> Import Job For more information, see the *About External Risk Factor Import Job* in the *HP EnterpriseView Deployment Guide*.
<External Risk Factor Name>ArchiveJob	Archive External Risk Factor Job For more information, see "Archive Trend Data" on page 32

Launch Batch Jobs Manually

To launch batch jobs manually

1. In EnterpriseView 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 EnterpriseView 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: BusinessObjects Reports

This chapter includes the following topics:

Create a Report Using SAP BusinessObjects Web Intelligence

In addition to the various reports provided by EnterpriseView, you can create customized reports by using BusinessObjects Web Intelligence. For information on creating reports, see *Building Reports with BusinessObjects Web Intelligence User Guide*.

You can create printable reports, dashboard reports, or reports that belong to both categories.

> **Note:** To create a report you must be familiar with the process of creating reports in *BusinessObjects*.

General instructions for creating a report for EnterpriseView

1. Select **EnterpriseView Universe** when you create a new document (report). For detailed information on the classes and objects in the EnterpriseView Universe, see the *EnterpriseView Universe* section in the *HP EnterpriseView User Guide*.

2. Prompts can be added to the report in order to get the application context. Add an **assetId** prompt to create a report for a certain asset or a **policyId** prompt to create a report for a certain policy. For more information on prompts, see the *Filtering Data Using Prompts* chapter in the *Building Reports with BusinessObjects Web Intelligence User Guide*

3. The query that you created could be an ambiguous query. In this case, after you run the query, you are prompted to select a context. For detailed information on ambiguous queries and query contexts, see the *Query Contexts* section in the *Building Reports with BusinessObjects Web Intelligence User Guide*. The EnterpriseView Universe includes predefined contexts. For information on the contexts, see " Universe Query Contexts" on page 27.

4. Assign a category to the report when you export the document to the Central Management Server (CMS). Select the categories that apply to the report (one or more). The category determines from which page the report will be available. If you are creating a report for a page that does not have a category, then you need to create a category, as described in the *Working*

with Categories section in the *SAP BusinessObjects Enterprise Administrator's Guide*. The name of the category must reflect the name of the page and it is not case-sensitive.

5. **Note:** If you do not assign the report to a category, then it will not be displayed in EnterpriseView.

Note: If you create a customized report that utilizes the following objects, then the report can include only one asset:

- Objects from the **SoA** class
- Objects from the **Policy Compliance** class
- Objects from the **Policy Assessment** class used in **Policy Assessment Context**

To create a report for a single asset, use the **Asset ID** object as query filter and the **@AssetPrompt** object as the prompt value.

To create an EnterpriseView report that displays the children of a specific asset

- When you create the query, drag the following objects to the **Results Object** area:
  - **Parent Asset ID** (**Asset Children** class)
  - **Child Asset ID** (**Children** class)
  - **Hierarchy Level** (**Children** class)

  Add the rest of the objects that you want to display to the **Results Object** area.

  For information on how to create a query, see the *Building and Working with Queries* section in the *Building Reports with BusinessObjects Web Intelligence User Guide*.

- Use the following objects as **Query Filters**:
  - **Parent Asset ID** to determine the asset that contains the assets that you want to display.
  - **Hierarchy Level** to determine which levels of children are displayed in the report.

  For information on query filters, see the *Filtering Data Using Query Filters* section in the *Building Reports with BusinessObjects Web Intelligence User Guide*.

To create a report that displays the policy elements of a specific policy

- When you create the query, drag the following objects to the **Results Object** area:

  - **Policy ID** (**Policy** class)
  - **Policy Security Category Parent ID** (**Policy Security Category Hierarchy** class)
  - **Policy Security Category Level** (**Policy Security Category** class)

  Add the rest of the objects that you want to display to the **Results Object** area.

  For information on how to create a query, see the *Building and Working with Queries* section in the *Building Reports with BusinessObjects Web Intelligence User Guide*.

- Use the following objects as **Query Filters**:
  - **Policy ID** to determine the policy that contains the policy elements that you want to display.
  - **Policy Security Category Parent ID** to display a specific section in the hierarchy. Used for drill-down purposes.
  - **Policy Security Category Level** to display the hierarchy graphically in the report.

    For information on query filters, see the *Filtering Data Using Query Filters* section in the *Building Reports with BusinessObjects Web Intelligence User Guide*.

The report that you created is automatically added to EnterpriseView. You can access printable reports by clicking the **Generate Report** button from any page that has a report associated with it.

You can access dashboard reports and create customized dashboards from the BusinessObjects Reports component, as described in the *Create a Customized Dashboard Page* section in the *HP EnterpriseView Deployment Guide*.

Export EnterpriseView Data

You can export data from EnterpriseView by using BusinessObjects reporting capabilities. The data is anything that can be accessed from the EnterpriseView Universe. For example, all vulnerability occurrences managed in EnterpriseView. You can export data to a CSV file.

You can schedule the report to run periodically or to run once. You can also use a file-based event to trigger report generation, as described in the procedure below. For more information on events, see the *Managing Events* section in the *SAP BusinessObjects Enterprise Administrator's Guide*.

To export to a CSV file

1. Add a **File System** destination to the **Adaptive Job Server**. Follow the instructions in the *To enable or disable destinations for a job server* section in the *SAP BusinessObjects Enterprise Administrator's Guide*.
2. Configure the destination properties for the **Adaptive Job Server**. Do the following:

   a. Follow the instructions in the *Configuring the destination properties for job servers* section in the *SAP BusinessObjects Enterprise Administrator's Guide*.

   b. Set the properties according to the instructions in the *File system destination properties* section. In the **Directory** box, enter the path to the directory where the CSV will be written to.

      This is a default path where all File System destination outputs are written to. You can override this setting for each report when you schedule the report (explained in the following steps).

3. Select a report or create a new report.

   > **Note:** The exported data is based only on the query. Any additional manipulation done on the data is not reflected in the output. If your report is dedicated strictly to exporting data (and not used in a dashboard or as a printable report), then you can create only a query.

   For information on creating reports, see *Building Reports with BusinessObjects Web Intelligence User Guide*.

4. Schedule the report. Follow the instructions in the *To schedule an object* section in the *SAP BusinessObjects Enterprise Administrator's Guide*, and do the following:

   a. In the left pane, under **Schedule**, click **Formats and Destinations**.

   b. Under **Output Format**, select **Comma Separated Values (CSV)**.

   c. Under **Output Format Details**, select **File location**.

   d. From the **Charset** list, select **UTF-8(Unicode)**.

5. Set a specific destination directory for the report (optional):

   a. Click **Destination Options and Settings**.

   b. Clear the **Use Job Server's defaults** check box.

   c. In the **Directory** box, enter the absolute path to the directory.

6. Click **Schedule**.

To schedule a report using a file-based event

1. Create an event, as described in the *To create a file-based event* section in the *SAP BusinessObjects Enterprise Administrator's Guide*.

2. Schedule the report, as described in the *Scheduling an object with events* section in the *SAP BusinessObjects Enterprise Administrator's Guide*.

Manage SAP BusinessObjects Report Settings

The BusinessObjects reports settings are configured during the installation of EnterpriseView.

> **Note:** If these settings are changed in BusinessObjects, then you must update this information manually in EnterpriseView.

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 *HP EnterpriseView Deployment Guide*.

Universe Query Contexts

The EnterpriseView Universe includes predefined contexts.The following table includes a description for all EnterpriseView query contexts. For detailed information on ambiguous queries and query contexts, see the *Query Contexts* section in the *Building Reports with BusinessObjects Web Intelligence User Guide*.

Context Name	Description
Policy Context	Defines the group of objects with which you can create a report that includes policy elements (policy name, categories, and controls). For example, you can use this context to create a printout of the ISO/IEC 27001 policy.
Threat Library Context	Defines the group of objects with which you can create a report that includes threat library elements (categories, actors, operations, and impacts).
Policy Compliance Context	Defines the group of objects with which you can create a report that provides information on the compliance of a certain policy according to assessments made on another policy. For example, the Policy Compliance Details printout report utilizes the Policy Compliance Context.

Context Name	Description
Asset Policy Assessment Context	Defines the group of objects with which you can create a report on the assessment of a an asset required to comply with a specific policy. For example, the P5 Score Breakdown dashboard report utilizes the Asset Policy Assessment Context.
Asset SoA Context	Defines the group of objects with which you can create a report that provides information on the Statement of Applicability (SoA) of an asset.
Asset Scores Context	Defines the group of objects with which you can create a report that includes the various aggregate scores on an asset: compliance, maturity, risk, vulnerability, ESM threat, and the overall asset score.
Asset Profiling Context	Defines the group of objects with which you can create a report that includes information on the business model, such as a printout of the asset hierarchy.
Policy Mapping Context	Defines the group of objects with which you can create a report that provides information on mapping between the controls of two polices.
Vulnerability Context	Defines the group of objects with which you can create a report that includes information on vulnerabilities on the asset level. For example, the dashboard reports in the vulnerability dashboard utilize the Vulnerability Context.
Vulnerability Aggregation Context	Defines the group of objects with which you can create a report that includes information on vulnerabilities on the asset in addition to its aggregate scores.
Asset Risk Context	Defines the group of objects with which you can create a report on risk assessments on an asset.
Asset External Risk Factor Score Context	Defines the group of objects with which you can create a report on the external risk factor scores of an asset.
Aggregated Asset External Risk Factor Score Context	Defines the group of objects with which you can create a report on the aggregate external risk factor scores of an asset.
Asset External Risk Factor Score Archive Context	Defines the group of objects with which you can create a report on the archived external risk factor scores of an asset.
Aggregated Asset External Risk Factor Score Archive Context	Defines the group of objects with which you can create a report on the archived aggregate external risk factor scores of an asset.

Chapter 6: Audit Log

The audit log enables you to track user initiated and automatic actions performed in EnterpriseView. You can view the audit log through the EnterpriseView 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: **Login**, **Policy and Compliance**, **Risk Modeling**, **Assets**, **Vulnerabilities**, **Settings**, **Assets**, **Administration**, and **Task Management**.
User Name	The EnterpriseView 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 7: Update the Vulnerability Dictionary

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

To update the vulnerability dictionary, contact your EnterpriseView 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 EnterpriseView. 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 EnterpriseView. For more information, see "About the Dictionary Information Import Job" below.

To update the vulnerability dictionary

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

   <EnterpriseView 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 21.

About the Dictionary Information Import Job

The Dictionary Information Import Job imports new and updated vulnerability data from files provided by the EnterpriseView labs into the EnterpriseView 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 EnterpriseView 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 EnterpriseView database, then the process proceeds to the following step.

3. The vulnerability dictionary tables in the EnterpriseView database are updated. The version of the vulnerability dictionary records is updated.

4. Open vulnerabilities in EnterpriseView are updated, if any of their properties have changed.

5. The **DictionaryInfo.zip** file is renamed to **DictionaryInfo<date>.zip.old**.

Chapter 8: 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 35.
- Vulnerabilities. For more information, see "Archive Vulnerabilities" on page 36.

Archive Trend Data

EnterpriseView 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, EnterpriseView archives data for all assets for the following measurements:

- Aggregate overall score
- Number of open vulnerabilities
- Aggregate risk score
- Aggregate maturity score
- Aggregate compliance score
- Scores and aggregate scores for any external risk factor defined in EnterpriseView
- Aggregate vulnerability score

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

Measurement	Trend Chart	Dashboard Name
Aggregated overall score	Asset Overall Score Over Time	Risk Register
Number of open vulnerabilities	Number of Open Vulnerabilities Over Time	Vulnerability Dashboard
Risk	Aggregated Risk Score Over Time	Risk Modeling Dashboard
Maturity	Maturity Score Over Time	Compliance Dashboard and Compliance by Policy Dashboard

Measurement	Trend Chart	Dashboard Name
Compliance	Compliance Score Over Time	Compliance Dashboard and Compliance by Policy Dashboard
External risk factor	Aggregate Risk Factor Score Over Time	External Risk Factors Dashboard
Aggregated vulnerability score	Aggregated Vulnerability Score Over Time	Vulnerability Dashboard

Archiving internal risk factors and external risk factors is done differently.

- **Internal risk factors**

  All internal risk factors data is archived by using the same job: **ExtractDataToArchiveJob**. You can configure EnterpriseView to archive trend data of internal risk factors on a weekly basis, as described in "Schedule and Activate the Archive Trend Data Job" below. 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 21. 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.

  > **Note:** When you complete an audit process and you perform a clear assessment, the aggregated maturity score and the aggregated compliance score are archived for all assets for the policies you cleared. The trend chart displays an indication that the snapshot is due to clear assessment.

- **External risk factors**

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

Schedule and Activate the Archive Trend Data Job

> **Note:** The Archive Trend Data Job archives data for internal risk factor information; it does not archive information for external 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 *HP EnterpriseView Deployment Guide*.

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

Configure the External Risk Factor Archive Settings

> **Note:** The <External Risk Factor> Archive Job archives data for external risk factor information; it does not archive information for internal risk factors.

For information on archiving trend data, see "Archive Trend Data" on page 32.

To configure the archive settings

1. Open the external risk factor folder. Click **Administration** > **Configuration**, expand the **External Risk Factor** folder, and then click the factor that you defined.
2. Under the folder of the external 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 EnterpriseView, 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).
4. Save and apply the configuration changes. For more information, see the *Save and Apply Configuration Changes* section as described in *HP EnterpriseView 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 EnterpriseView 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 21.

The archived data is kept in EnterpriseView 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" below.

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" below.

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 EnterpriseView.

> **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 62.

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 62.

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

Archive Vulnerabilities

You can archive vulnerabilities in order to keep the vulnerabilities displayed in the Vulnerabilities module in a manageable size. You can either schedule the Vulnerabilities Archive Job to run at a certain time or you can run it manually through the Job Management module. For more information on scheduling the job, see "Schedule and Activate the Vulnerabilities Archive Job" below. For information on running the job manually, see "Launch Batch Jobs Manually" on page 21.

You can archive only network and application vulnerabilities that fulfill the following conditions:

- They are closed (their status is Closed)
- They have not been updated or reported for certain (configurable) amount of time.

Vulnerabilities are fully archived. This means that all their properties are archived along with any notes that are attached to them.

The archived data is kept in EnterpriseView database in the **RC_VULNERABILITY_ARCHIVED** table.

For information on the job , see "About the Vulnerabilities Archive Job" below.

About the Vulnerabilities Archive Job

The Vulnerabilities Archive job periodically archives vulnerabilities as follows:

1. Check the vulnerabilities table (RC_VULNERABILITY) for vulnerabilities that fulfill the following conditions:
   - They are closed (Status=CLOSED).
   - They have not been updated or reported for certain (configurable) amount of time (Last Updated On=n).
2. Copy vulnerabilities from RC_VULNERABILITY to RC_VULNERABILITY_ARCHIVED.
3. Delete vulnerabilities from RC_VULNERABILITY.
4. Copy notes from RC_VULNERABILITY_NOTE to RC_VULNERABILITY_NOTE_ARCHIVED.
5. Delete notes from RC_VULNERABILITY_NOTE.

Schedule and Activate the Vulnerabilities Archive Job

Vulnerabilities are archived under the following conditions:

- They are closed (their status is Closed)
- They have not been updated or reported for certain amount of time (configured in the following task)

For more information on archiving vulnerabilities, see "Archive Vulnerabilities" on the previous page. For information on the job , see "About the Vulnerabilities Archive Job" above.

To schedule and activate the job

1. Click **Administration > Configuration**.
2. In the left pane, click **Vulnerability Management > Schedule Archive Job**.
3. In the **Schedule Archive Job** page, do the following:
   a. Select the **Activate Job** check box.
   b. 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).
   c. In **Automatically archive closed network vulnerabilities after (days)**, enter the number of days that you want to keep network vulnerabilities in the Vulnerabilities module before they are archived.
   d. In **Automatically archive closed application vulnerabilities after (days)**, enter the number of days that you want to keep application vulnerabilities in the Vulnerabilities module before they are archived.
4. Save and apply the configuration changes.For more information, see the *Save and Apply Configuration Changes* section as described in *HP EnterpriseView Deployment Guide*.

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

Chapter 9: Import Risk Information from External Sources

EnterpriseView enables you to import information on risk factors from any external source. For more information on external risk factors, see the *External Risk Factors* section in the *HP EnterpriseView User Guide*.

Information is imported by using a connector. EnterpriseView supports the connector types described in the table below.

Type	How	Supported with business model
CSV connector	Create an add-on data connection allowing you to load data directly from a comma separated file (CSV) into EnterpriseView.	All types
ESM connector	Create an ESM connector allowing you to load data from an ESM report into EnterpriseView.	ESM and UCMDB
UCMDB connector	Create a UCMDB connector allowing you to load data by using a TQL into EnterpriseView.	UCMDB only
Custom connector	Create a JAR file connector allowing you to load data from any source into EnterpriseView.	All types

Following are the steps for importing risk information into EnterpriseView:

1. Create a connector.

   - To create a CSV connector, see "Create a CSV Connector" on page 41.

     Put the CSV connector file anywhere on the EnterpriseView server or on a different server that can be accessed by EnterpriseView.

   - To create an ESM connector, see "Create a Risk Factor Report in ESM" on page 41.

   - To create a UCMDB connector, see "Create a UCMDB Connector" on page 44.

   - To create a custom connector, see "Create a Custom Connector" on page 45.

Put the custom connector JAR file in the following folder:

<EnterpriseView Installation Folder>\Plugins

2. Define the external risk factor and configure the connector. For more information, see "How to Configure External Risk Factors" on page 45.

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

About External Risk Factor Import Job

The External Risk Factor Import Job periodically imports risk information from external sources. For each external risk factor that you define and configure in EnterpriseView, a specific job is created with the name: <*external 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 EnterpriseView. 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 reconciles the assets by matching the Asset Identifier parameter to one of the asset properties defined in Configuration. For more information, see "Configure Asset Reconciliation Parameters" on page 49.

4. 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 EnterpriseView 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.

5. 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.

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

7. If you selected the **Archive immediately after import** check box in **Configuration**, then both scores and aggregate scores are archived. If you are using a CSV connector, then the timestamp is the Date Time from the CSV file.

   For more information on archiving, see the *Archive Trend Data* section in the *HP EnterpriseView Administration Guide*.

Create a CSV Connector

View the sample CSV file:

<EnterpriseView Installation Folder>\Samples\sampleRiskFactorCsvFile

Create a CSV connector with the following format:

Parameter	Format	Description
SnapshotDate	dd/mm/yyyy	Optional This parameter represents the timestamp of the score, for archiving purposes. If this parameter is empty, then the import date is used as the timestamp. If a value exists but is different from the required format, then the job fails.
Asset Identifier	Maximum 255 characters	Mandatory If the asset identifier is empty, then the record is skipped.
Score	Rational number	Mandatory If the score is empty, then the record is skipped.
Comment	Free text	Optional A maximum of 1024 characters can be displayed in EnterpriseView. A comment that exceeds the maximum length is truncated.

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.

There are two types of report formats:

- **ESM-based business model format**: Use this format when your business model is imported from ESM.
- **Non-ESM business model format**: Use this format when your business model is imported from any source other than ESM.

The following tables detail the formats.

ESM-based business model format

Parameter	Format	Description
Asset Identifier	Maximum 100 characters	Mandatory If the asset identifier is empty, then the record is skipped. This parameter is used for asset reconciliation. You do not need to configure a reconciliation parameter in EnterpriseView, as described in "Configure Asset Reconciliation Parameters" on page 49.
Score	Rational number	Mandatory If the score is empty, then the record is skipped.
Comment	Maximum 1024 characters	Optional

Non-ESM business model format

Parameter	Format	Description
Asset Name, External ID, IP Address, DNS Name, Mac Address	Maximum 100 characters	These parameters are used for asset reconciliation. It is mandatory to pass at least one of these parameters. We recommend to create a report with all of these parameters. You need to configure a reconciliation parameter in EnterpriseView, as described in "Configure Asset Reconciliation Parameters" on page 49.

Non-ESM business model format, continued

Parameter	Format	Description
Score	Rational number	Mandatory If the score is empty, then the record is skipped.
Comment	Maximum 1024 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 EnterpriseView are based on the data sources listed above. For more information, see the *Out-of-the-Box Risk Factor Reports* section in the *ArcSight EnterpriseView 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, depending on the report format, do the following:
   - **ESM-based business model format**. Create active columns in the following order:
     i. The asset identifier
     ii. The score of the risk factor for a specific asset
     iii. Additional evidence
   - **Non-ESM business model format**. Create active columns in the following order:
     i. Asset Name
     ii. External ID
     iii. IP Address
     iv. DNS Name

v. Mac Address

vi. The score of the risk factor for a specific asset

vii. 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, depending on the report format, do the following:

   - **ESM-based business model format**. Change the **Alias** for each column that you defined to the following names:

     i. **Asset Identifier**

     ii. **Score**

     iii. **Comment**

   - **Non-ESM business model format**. Change the **Alias** for the last two columns that you defined to the following names:

     i. **Score**

     ii. **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 EnterpriseView, deploy real-time rules, as described in the *Deploying Real-Time Rules* section in the *ArcSight Console User's Guide*.

Create a UCMDB Connector

The UCMDB connector is created according to the information that you enter when you configure the connection parameters in "Configure the External Risk Factor Connector Parameters" on page 48. You do not have to perform any additional tasks.

Create a Custom Connector

The following table includes general information about the methods that you need to implement when creating a custom connector. For further instructions and assistance in creating a custom connector, contact your HP Support representative.

Return Value	Method Name and Parameters	Call this method
void	**init**(Map<String, String> params)	To initialize the connector. It is the first method that is called. It can be called several times during one import process. This method passes the connection parameters.
String	**getSourceVersion String**()	To get the version of the latest source read. If the version is equal to the previously read version,then the process completes without import. If it returns NULL, then the import is always carried out.
Date	**getTimestamp** ()	To get the timestamp of the scores currently being received. The timestamp is used for archiving purposes.
List<ScoreRecord>	**readRecords**()	To retrieve all scores. When this method returns an empty list, then it is no longer called.
List<String>	**readWarnings**()	After all scores are read. All warnings returned are written into the error log. This method can return an empty list or NULL if there are no warnings.

How to Configure External Risk Factors

In order to import risk information from external sources you must first define and configure the external risk factors in EnterpriseView.

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

1. Define a new external risk factor in EnterpriseView. For more information, see "Define a New External Risk Factor " on the next page.

2. Configure the connection parameters, depending on the connector that you created. For more information see "Configure the External Risk Factor Connector Parameters" on page 48.

3. Depending on the connector that you are defining and on the source of your business model, define the asset reconciliation parameters, as described in "Configure Asset Reconciliation

Parameters" on page 49. In one of the following cases, you do not need to define an asset reconciliation parameter:

- A UCMDB connector. You can import risk factors from UCMDB only if your business model is based on UCMDB, therefore, the reconciliation parameter is already known.
- An ESM connector when your business model is based on ESM. In this case, the External ID is used as the reconciliation parameter.

4. Configure the external risk factor import job. For more information see "Configure the Risk Factor Import Job" on the next page.
5. Configure the normalization settings for the risk factor. For more information, see "Configure the External Risk Factor Normalization Settings" on page 50.
6. Configure the external risk factor score aggregation method. For more information, see "Configure the External Risk Factor Aggregation Method" on page 51.
7. Configure the archive settings. For more information, see the *Configure the External Risk Factor Archive Settings* section in the *ArcSight EnterpriseView Administration Guide*.
8. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 62.
9. Configure external risk factor ranges in order to display the risk factor scores with the appropriate score severity. For more information, see the *Configure External Risk Factor Ranges* section in the *HP EnterpriseView User Guide*.

Define a New External Risk Factor

You can define any number of external risk factors in EnterpriseView.

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

After you define the risk factor you can configure its connection parameters, as described in "Configure the External Risk Factor Connector Parameters" on page 48.

To define a new external risk factor

1. Click **Administration** > **Configuration**.
2. On the **Configuration** page, in the left pane, click **External Risk Factor**.
3. Click the **Add configuration to configuration set**  button, and select the type of connector that you want to create:

- **CSV Connector**
- **Custom Connector**
- **ESM Connector**
- **UCMDB Connector**

4. In the left pane, expand the external 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 external 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 external risk factor. It will be displayed in the folder name, Risk Register, Risk Indicators, External Risk Factor Dashboard, and any other report that includes this risk factor.

   b. **Description**: this field is optional. You can include information about the external source.

Configure the Risk Factor Import Job

After the connector parameters are configured, you need to schedule and activate the External Risk Factor Import Job. For each external risk factor that you define and configure in EnterpriseView, a specific job is created with the name: <*external risk factorname*>ImportJob. The job is created only after the new configuration is saved and activated. For more information on the job, see "About External Risk Factor Import Job" on page 40.

To schedule and activate the import job

1. Open the external risk factor folder. Click **Administration** > **Configuration**, expand the external risk factor folder, and then click the factor that you defined.

2. Under the folder of the external 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 **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).

4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 62.

Configure the External Risk Factor Connector Parameters

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

The connection parameters depend on the type of connector that you defined.

The connection parameters for a custom connector are user-defined. For example, if the external source is a database, then the connection parameter may be the database user credentials.

To configure connection parameters

1. Open the external risk factor folder. Click **Administration** > **Configuration**, expand the external risk factor folder, and then click the factor that you defined.

2. Under the folder of the external risk factor that you defined, click **Connector Parameters**.

3. If you are configuring a CSV connector, enter the path to the CSV file.

4. If you are configuring a custom connector, do the following:

    a. In **Connector JAR File Name**, enter the name of the connector file.

    b. For each connection parameter that you want to add, click the **Add configuration to configuration set**  button.

    c. In the **Parameter Name** box, enter the name of the connection parameter exactly as defined in the connector file.

    d. In the **Parameter Value** box, enter the value expected by the external source.

5. If you are configuring an ESM connector, do the following:

    a. In **Resource ID**, enter the resource ID that you defined when you created the report in ESM.

    b. In **Host**, enter the ESM server IP address or domain name.

    c. In **Port**, enter the ESM server port.

    d. In **Username**, enter the username for connecting to ESM.

    e. In **Password**, enter the password for connecting to ESM.

6. If you are configuring a UCMDB connector, do the following:

> **Note:** Most of the following fields were populated during the UCMDB-EnterpriseView synchronization process. You can copy these values from **Integrations > UCMDB > Asset Synchronization > HP Universal CMDB > Connector**.

   a. In **Communication Protocol**, select either **HTTP** or **HTTPS**, according to the specifications received from the UCMDB administrator.

   b. In **Communication Host**, enter the host name or IP address of the UCMDB server, provided by the UCMDB administrator.

   c. In **Communication Port**, enter the UCMDB server port, provided by the UCMDB administrator.

   d. In **UCMDB User Name**, enter the user name for accessing UCMDB, provided by the UCMDB administrator..

   e. In **UCMDB Password**, enter the password for accessing UCMDB, provided by the UCMDB administrator.

   f. The default value of **Customer ID** is **1**. Do not change this value.

   g. In **TQL Query Name**, enter the name of the TQL query that EnterpriseView activates for retrieving assets, provided by the UCMDB administrator. You can also enter a different TQL (a subset of the TQL for retrieving the assets).

   h. In **CI Field**, enter the name of the CI that represents the risk factor, as defined in UCMDB.

   i. In **Max Bulk Size**, enter the maximum number of UCMDB entities (assets and relationships) that the query returns to EnterpriseView at a time.

7. Select the **Delete Old Scores** check box if you want all the scores to be deleted when the External 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.

8. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 62.

Configure Asset Reconciliation Parameters

Reconciliation is the process of identifying and matching entities from different data repositories. In this case, matching assets from external sources to assets in EnterpriseView. This process is designed to assure unique identification of assets in EnterpriseView.

You must select at least one property for asset reconciliation.The reconciliation process tries to match the parameter passed from the external source to one of the asset properties that you select, starting with the first asset property. If an asset is not found, then the second property is used, and so forth.

> **Note:** If there is more than one asset defined in EnterpriseView with the same identification, such as name or external ID, then the first asset found is matched.

To configure asset reconciliation parameters

1. Open the external risk factor folder. Click **Administration** > **Configuration**, expand the **External Risk Factor** folder, and then click the factor that you defined.

2. Under the folder of the external risk factor that you defined, click **Asset Reconciliation**.

3. On the **Asset Reconciliation** page, for each reconciliation parameter that you want to add, do the following:

    a. Click the **Add configuration to configuration set** button.

    b. Under **Parameter**, expand the list and select a property.

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

Configure the External 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 > External Risk Factor**. For more information, see the *Configure External Risk Factor Ranges* section in the *HP EnterpriseView User Guide*.

To configure normalization settings

1. Open the external risk factor folder. Click **Administration** > **Configuration**, expand the **External 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 62.

Configure the External Risk Factor Aggregation Method

You can configure the aggregation method for each of the external risk factors defined in EnterpriseView.

To configure aggregation method

1. Click **Administration > Configuration**.

2. In the left pane, click **External 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 62

Delete an External Risk Factor

You can delete an external risk factor from EnterpriseView when it is no longer relevant.

When you delete an external 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 external risk factor (<*external 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 **External 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 62.

Chapter 10: Email Notifications

There are two types of email notifications:

- BusinessObjects allows you to send an report as an attachment in an email to one or more recipients. For more information, see "Send a Report in an Email Notification" on page 56.
- EnterpriseView supports email notifications for different events that occur in the system. For example, every time a workflow is completed, the workflow owner and the workflow stakeholders receive an email notification. To activate email notifications, follow the instructions in "Configure Email Notifications" on page 55.

In order to get email notifications, you need to make sure that:

- All EnterpriseView users have an email address defined in BusinessObjects.
- The EnterpriseView server has network access to the email server.

Email notifications are sent in one of the following ways:

- Immediately after the event takes place.
- By using a batch job. EnterpriseView includes the following jobs for sending notifications:
  - Task Management Notifications Job
  - Treatment Notifications Job

For more information on scheduling the job, see "Schedule Notification Jobs" on page 56.

The following table includes all the events that trigger alerts, whether the notification sent immediately or by the Notifications Job, and the recipients of the notifications.

Event Name	Description	When	Recipients
Workflow Complete	After a workflow is complete (the last task in the workflow is complete), EnterpriseView automatically sends an email notification to the workflow owner.	Immediately	Workflow owner Workflow Stakeholders

Event Name	Description	When	Recipients
Workflow Warnings	The Task Management Notifications Job sends the workflow owner an email that summarizes the following: • Task exceeds workflow due date - A workflow is considered overdue if one of its tasks has a due date that is later than the workflow due date. • Overdue Task - A task is considered overdue when it is passed it's due date and its status is In Progress (meaning that it was not completed). • Task Approaching Due Date - A task is considered to be approaching its due date on the day before the due date and on the day that it is due, if it is in progress. This means that this notification will be sent twice.	Scheduled - Task Management Notifications Job	Workflow owner Workflow Stakeholders
Overdue Task	A task is considered overdue when it is passed it's due date and it is not completed.	Scheduled - Task Management Notifications Job	Task assignee
Task Approaching Due Date	Approaching Due Date - A task is considered to be approaching its due date on the day before the due date and on the day that it is due. This means that this notification will be sent twice.	Scheduled - Task Management Notifications Job	Task assignee
Expired Treatment Activity	The Risk Management Notifications Job sends the activity owner an email for the following treatment activities: Accept, Defer, Transfer, Avoid. When the following conditions occur: • Avoid/Transfer: When they are passed their expiration date and their status is not completed. • Accept/Defer: When they are passed their expiration date.	Scheduled - Risk Management Notifications Job	Activity owner

Event Name	Description	When	Recipients
Overdue Mitigation Activity	The Risk Management Notifications Job sends the activity owner an email when the activity is passed its due date and its actions are not completed.	Scheduled - Risk Management Notifications Job	Activity owner

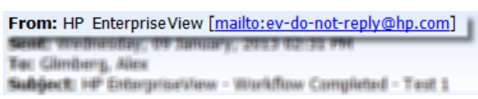
Configure Email Notifications

You can configure email notifications to be sent automatically by EnterpriseView.

Note: EnterpriseView supports only Simple Mail Transfer Protocol (SMTP).

To configure email notifications

1. Click **Administration** > **Configuration**.
2. In the left pane, expand **Notifications**, and then click **Email Notifications**.
3. In the **Email Notifications** page, select **Activate Email Notifications**.
4. In the **Sender Address** box, enter an email address that indicates to the recipient that the email is a notification from EnterpriseView. This is the email address that appears in the 'From' line in the email.
5. In the **Sender Name** box, enter the name that is displayed next to the sender address in the 'From' line in the email.

6. In the **Port** box, enter the port for the email server.
7. In the **SMTP Server** box, enter the IP address or the domain name.
8. To limit the number of addressees in each email notification and avoid being blocked or considered spam, in the **Maximum number of addressees in an email notification** box, enter the maximum number of addressees in each email notification. If the number of addressees is greater than the maximum, then the addressees will be split and more than one email notification will go out.

   Note: You can contact your email server administrator for information on the policies with which you need to comply.

9. Save and apply the configuration changes. For more information, see the *Save and Apply Configuration Changes* section as described in *HP EnterpriseView Deployment Guide*.

Schedule Notification Jobs

Some notifications are sent by using batch processes. EnterpriseView includes the following jobs for sending notifications:

- Task Management Notifications Job
- Treatment Notifications Job

For more information on the events that trigger these notifications, see "Email Notifications" on page 53. For more information on the jobs, see .

To schedule notification jobs

1. Click **Administration** > **Configuration**.
2. In the left pane, click **Notifications** > **Notification Jobs**, and then click one of the following:
   - **Schedule Risk Management Notifications**
   - **Schedule Task Management Notifications**
3. On each page, do the following:
   - 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).
4. Save and apply the configuration changes. For more information, see the *Save and Apply Configuration Changes* section as described in *HP EnterpriseView Deployment Guide*.

   The jobs are activated and will run according to the schedule that you have set.

Send a Report in an Email Notification

BusinessObjects allows you to send a report as an attachment in an email to one or more recipients. You can schedule the email to be sent periodically or to run once.

To send as an attachment in an email

1. Add an **Email** destination to the **Adaptive Job Server**. Follow the instructions in the *To enable or disable destinations for a job server* section in the *SAP BusinessObjects Enterprise*

Administrator's Guide.

2. Configure the destination properties for the **Adaptive Job Server**. Do the following:

   a. Follow the instructions in the *Configuring the destination properties for job servers* section in the *SAP BusinessObjects Enterprise Administrator's Guide*.

   b. Set the properties according to the instructions in the *Email destination properties* section.

3. Select a report or create a new report.

   > **Note:** The exported data is based only on the query. Any additional manipulation done on the data is not reflected in the output. If your report is dedicated strictly to exporting data (and not used in a dashboard or as a printable report), then you can create only a query.

   For information on creating reports, see *Building Reports with BusinessObjects Web Intelligence User Guide*.

4. Schedule the report. Follow the instructions in the *To schedule an object* section in the *SAP BusinessObjects Enterprise Administrator's Guide*, and do the following:

   a. In the left pane, under **Schedule**, click **Formats and Destinations**.

   b. Under **Output Format Details**, select **Email recipients**.

5. Set email recipients:

   a. Click **Destination Options and Settings**.

   b. Clear the **Use Job Server's defaults** check box.

   c. Select the **Add attachment** check box.

   d. Set the properties according to the instructions in the *Email destination properties* section in the *SAP BusinessObjects Enterprise Administrator's Guide*.

6. Click **Schedule**.

Chapter 11: Migrate EnterpriseView Metadata

The following is considered metadata in EnterpriseView:

- Policies: Including attachments on security categories and mappings between controls.
- Settings
- Threat Library
- Control to threat mappings
- Vulnerability dictionary
- Vulnerability to control mappings
- Workflow templates: Can be migrated manually, as described in "To migrate workflow templates" on the next page.
- Configuration: Can be migrated manually, as describe in the *Migrate Configuration Data* section in the *HP EnterpriseView Deployment Guide*.
- BusinessObjects reports can be migrated manually, as described in "To migrate BusinessObjects reports" on page 60.

  For additional methods of migrating reports, see the *Importing and Promoting Replicated Content* section in the *BusinessObjects Enterprise Administrator's Guide*.

  Note:

  - If you created custom KPIs, then after you migrate BusinessObjects reports, you will need to select their report in the target EnterpriseView application.
  - You cannot migrate custom dashboards or modified dashboards. You must create the custom dashboards or make the necessary modifications to existing dashboards in the target EnterpriseView application.

You can migrate metadata in order to duplicate EnterpriseView environments. For example, if you want to move from a pre-production environment to a production environment.

Note: We recommend that you import metadata on a clean installation of EnterpriseView because any existing metadata will be deleted.

To migrate metadata you need to export metadata from a source EnterpriseView application and import it into the target EnterpriseView application.

Note: You must migrate the configuration data before you perform the following procedure.

To migrate metadata

1. Stop the EnterpriseView service for the source application and the target application.
2. On the server on which the source application is installed, open a command line from the following folder:

   <EnterpriseView Source Application Installation Folder>\bin

3. Run the following command:

   export-data.bat

   The following file is created:

   EV-data-export_<timestamp>.zip

4. Open the following folder:

   <EnterpriseView Source Application Installation Folder>\data-migration\export

5. Copy the **EV-data-export_<timestamp>.zip** file to the following folder in the target application:

   <EnterpriseView Target Application Installation Folder>\data-migration\import

6. On the server on which the target application is installed, open a command line from the following folder:

   <EnterpriseView Target Application Installation Folder>\bin

7. Run the following command:

   import-data.bat EV-data-export_<timestamp>.zip

8. Start the EnterpriseView service for the source application and the target application.

To migrate workflow templates

1. On the server on which the source application is installed, open the following folder:

   <EnterpriseView Source Application Installation Folder>\content\taskManagement\templates

2. Copy the content of the folder to the following folder in the target application environment:

   <EnterpriseView Target Application Installation Folder>\content\taskManagement\templates

3. In the target application, follow the instructions described in the *Upload a Workflow Template to EnterpriseView* in the *EnterpriseView User Guide*.

To migrate BusinessObjects reports

1. In the source BusinessObjects server, open BusinessObjects Web Intelligence.
2. Use the **Save As** command to save each report locally.
3. In the target BusinessObjects server, open BusinessObjects Web Intelligence.
4. Use the **File > Export to CMS** command to copy all the reports to the target BusinessObjects CMS.

   Note: When you export the report files, make sure to all the reports to their respective category under the EnterpriseView Reports folder.

Chapter 12: 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. EnterpriseView 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 EnterpriseView 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.

EnterpriseView validates the configuration set and identifies the problems in the configuration, such as, a field with a missing value. If a problem is found, EnterpriseView 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**.

Migrate Configuration Data

You can export configuration data from one EnterpriseView application to another.

Note: Import and export of configuration data is supported only on Microsoft Internet Explorer.

To migrate configuration data

1. In the source application, click **Administration > Configuration**.
2. On the **Configuration** toolbar, click the **Export configuration set to a zip file** button.
3. In the **Export Configuration Set** dialog box, clear the following check boxes, and then click **Export**:
   - **Connector** in the following paths:

     Integrations > ArcSight ESM

     Integrations > UCMDB > Asset Synchronization > HP Universal CMDB
   - BusinessObjects
4. Save the zip file to a location that can be accessed from the target application.
5. In the target application, click **Administration > Configuration**.
6. On the **Configuration** toolbar, click the **Import configuration set** button.
7. In the **Import Configuration Set** dialog box, do the following and then click **Import**:
   a. Click Browse and select the zip file that you want to import.
   b. In the **Draft name** box, enter a name for the configuration set.
8. Click the **Activate current configuration set** button to activate the draft and apply the new configuration settings to EnterpriseView.

Save and Apply Configuration Changes

You can save configuration changes and then apply the new configuration settings to EnterpriseView 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**.

   EnterpriseView 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 EnterpriseView.

Chapter 13: 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 *HPEnterpriseView User Guide*.

This chapter includes the following sections:

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 in EnterpriseView" on page 66.

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 67.

Create a KPI Report in BusinessObjects

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

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

For general instructions on creating EnterpriseView reports in BusinessObjects, see the *Create a Report Using SAP BusinessObjects Web Intelligence* section in the *HP EnterpriseView User Guide*"Create a Report Using SAP BusinessObjects Web Intelligence" on page 23

To create a KPI report

1. Open BusinessObjects Web Intelligence.

2. In the main window, click **File > Import from CMS**.

3. In the **Import Document** dialog box, expand **Public Folder**, and then click **EnterpriseView Reports**.

All EnterpriseView reports are displayed in the right pane.

4. In the **Search title** box, search for **External Risk Factor KPI Template**. This template is specific for KPIs for external risk factors. Use this template to create external 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.

5. In the search results, click the template that you selected, and then click **Add**.
6. Click **Import**, verify that the import was successful, and then click **Click to Continue**.
7. Click **Open All**.
8. In the **Prompts** dialog box, click **Cancel**.
9. In the main window, click **File > Save As > Web Intelligence Document (.WID)**.
10. Select the following check-boxes:
    - **Save for all users**
    - **Remove document security**
11. 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 EnterpriseView. Save the report with a **.wid** file extension.
12. In the main window, on the toolbar, click **Edit Query**.
13. In the **Edit Query** dialog box, 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.

14. Click **Run Query**.
15. In the main window, drag the object that represents the KPI score from the **Data** pane into the **Percentage** cell in the right pane.
16. In the main window, click **File > Save As**.
17. Select the following check-boxes, and then save the file:

- **Save for all users**
- **Remove document security**

18. In the main window, click **File > Export to CMS**.

19. In the **Export Document** dialog box, expand **Public Folder**, and then click **EnterpriseView Reports**.

20. Click the **Categories** tab, select the **KPI** check-box, and then click **Export**.

> **Note:** You must select the **KPI** check-box in order to display this report in EnterpriseView.

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

Define a KPI in EnterpriseView

Before you define a KPI in EnterpriseView, you need to create a KPI report in BusinessObjects. For more information, see "Create a KPI Report in BusinessObjects" on page 64.

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**.

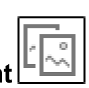
   The **Dashboard Builder** opens in a new window.

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 12.

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 Policy 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/policy, select either **Select a Specific Asset** or **Select a Specific Policy**.

   - To create a dynamic report/dashboard, that receives the asset/policy as a parameter using the wiring capability, select either **Set up wiring between this component and an Asset Selector component** or **Set up wiring between this component and a Policy and Asset 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 **Policy** parameter and an **Asset** parameter and you selected **Set up wiring between this component and a Policy and Asset Selector component**, then you must add a **Policy and Asset 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 13.

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 *HP EnterpriseView 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 14: Configure the Group Population Job

The Group Population Job updates the groups that are displayed in EnterpriseView in the User Management module and in Activiti Modeler according to the groups defined in BusinessObjects. The job is scheduled to run once a day, but you can schedule it to run at any frequency you require. You can also run this job manually, as described in "Launch Batch Jobs Manually" on page 21.

Note: Groups that are deleted in BusinessObjects are not deleted in EnterpriseView.

To configure the group population job

1. Click **Administration > Configuration**.
2. In the left pane, click **Task Management > Schedule Group Population Job**.
3. On the **Schedule Group Population Job** page, do the following:
   - 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).
4. Save and apply the configuration changes.For more information, see the *Save and Apply Configuration Changes* section as described in *HP EnterpriseView Deployment Guide*.

Chapter 15: Restore Search Engine Indexes

The search engine used in the vulnerability dictionary is based on indexing. EnterpriseView 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 EnterpriseView database, creates indexes, and writes them to the relevant files in EnterpriseView.

To restore search engine indexes

1. Stop the EnterpriseView service.
2. Delete the following folder:

   <EnterpriseView Installation Folder>\Indices

3. Start the EnterpriseView service.
4. Run the **RestoreIndexesJob** from the Job Management module, as described in "Launch Batch Jobs Manually" on page 21.