# HP EnterpriseView

For Windows

Software Version: 1.5

## User Guide

# Legal Notices

## Warranty

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

The information contained herein is subject to change without notice.

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

## Restricted Rights Legend

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

## Copyright Notice

© Copyright 2012 Hewlett-Packard Development Company, L.P.

Follow this link to see a complete statement of copyrights and acknowledgements for all ArcSight products: http://www.arcsight.com/copyrightnotice.

## Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

**This document is confidential.**

# Documentation Updates

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

- Software Version number, which indicates the software version.

- Document Release Date, which changes each time the document is updated.

- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

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

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

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

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

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

# Support

Visit the HP Software Support Online web site at:

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

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

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

- Search for knowledge documents of interest

- Submit and track support cases and enhancement requests

- Download software patches

- Manage support contracts

- Look up HP support contacts

- Review information about available services

- Enter into discussions with other software customers

- Research and register for software training

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

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

To find more information about access levels, go to:

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

# Contents

# Chapter 1

# Welcome to This Guide

Welcome to HP EnterpriseView User Guide. This guide provides you with information about all of the operational aspects of EnterpriseView.

This guide is intended for all EnterpriseView users.

This guide includes the following chapters:

# Chapter 2

# 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 EnterpriseView 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. EnterpriseView incorporates a holistic, enterprise approach, streamlining and integrating risk, compliance, threat and vulnerability information and providing a business context to executives. EnterpriseView anticipates threats and provides continuous monitoring, by regularly updating and testing security related functions.

EnterpriseView includes the following features:

- **Policy and Compliance Management**. In addition to auditing, this module includes out-of-the-box polices, such as Unified Compliance Framework (UCF) enabling "audit once - comply with many" functionality, a policy builder for creating customized policies, and Statement of Applicability (SoA) capability.

- **Risk Modeling**. Using the flexible and expandable threat library, you can define threat scenarios for the assets in your organization's business model and specify impact and probability to calculate their risk.

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

- **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 using the Assets module.

- **Dashboards and Reports**. Includes both out-of-the-box sophisticated executive dashboards, such as the Risk Register and reports, as well as the ability 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 3

# What's New

This topic describes the new features and enhancements added in this release.

**Data Trending**

Monitor risk measurements over time to identify trends using the trend charts included in EnterpriseView dashboards. EnterpriseView enables you to schedule the archiving process to suit your business needs.

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

**Key Performance Indicators**

Measure the progression of your organization towards its objectives by using EnterpriseView key performance indicators (KPIs). Use the KPIs included in EnterpriseView dashboards to monitor and improve upon the different aspects that comprise risk in your organization.

For more information, see "Key Performance Indicators" on page 92.

**Task Management**

Streamline processes in EnterpriseView and promote collaboration between your organization's personnel using the Task Management module. EnterpriseView enables you to create and manage workflows and workflow templates. Managers can now oversee, approve, and follow up on tasks assigned to their team members.

For more information, see "Task Management" on page 165.

**Risk Mitigation with Policy Controls**

Mitigate risk by mapping policy controls to threats defined in your organization's threat library. EnterpriseView includes a risk probability recalculation formula that is automatically applied to all mapped threats. The formula adjusts the probability of a threat occurring based on the existence of controls applied to an asset and its level of compliance.

For more information, see "Risk Mitigation with Policy Controls" on page 68.

**Support Application Scanners**

In addition to the various network scanners supported, EnterpriseView now supports HP Webinspect application scanner.

For more information, see the Import Vulnerabilities From Vulnerability Assessment Tools section, in the *HP EnterpriseView Deployment Guide*.

**Risk Indicators**

Risk Indicators provides you with graphical risk indication on top of your business model map for maximum visibility. The quickest way to identify risk sources in your organization's business model and perform root cause analysis.

For more information, see "Risk Indicators" on page 100.

### New Uploadable Policies

COBIT 5 and ISO/IEC 27001—new additions to EnterpriseView's uploadable and out-of-the-box policies.

For information on uploading policies, see "Import a Policy" on page 39.

### Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) is a widely adopted industry standard for assessing the severity of IT vulnerabilities. EnterpriseView labs now uses CVSS v2 as the scoring system for the vulnerabilities defined in the vulnerability dictionary.

For more information, see "Common Vulnerability Scoring System" on page 144.

### Refining Compliance Scores using Vulnerabilities

EnterpriseView introduces an automatic method for enhancing the compliance auditing process using the vulnerabilities found in your organization and correlating them to the organization's regulation controls. By applying a unique formula on top of already existing compliance scores, EnterpriseView creates a new dimension for performing a compliance audit.

For more information, see "Using Vulnerabilities to Refine the Compliance Score" on page 35.

### Vulnerability Dictionary User Interface

EnterpriseView now includes a vulnerability dictionary page, allowing users to easily search for vulnerabilities according to their ID, title, details, or group. This page takes advantage of the comprehensive vulnerability dictionary created and maintained by EnterpriseView labs. The dictionary includes all known vulnerabilities.

For more information, see "Vulnerability Dictionary" on page 164.

# Chapter 4

# Navigating the User Interface

You can navigate the EnterpriseView user interface using the navigation bar or by clicking on the module name in the home page. The navigation bar and the home page provide you access to all the modules and pages in EnterpriseView.

The module pages you have access to depend on the following factors:

- **Your EnterpriseView license**. Modules for which you are not licensed are disabled.

- **Your role**. Pages that you do not have permissions for are not displayed.

The navigation bar is conveniently located on the left side of every screen.
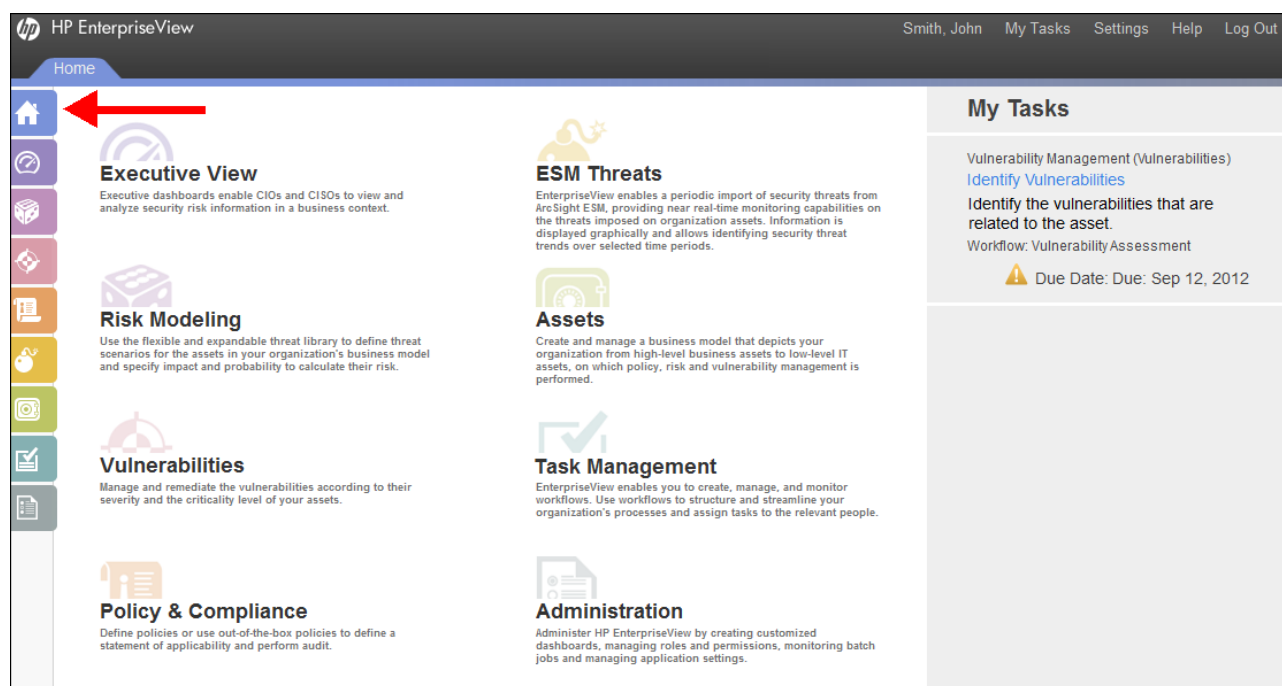


Clicking the icon of a module in the navigation bar opens a sub menu that includes its components.

The following table includes information on the navigation bar, assuming you have a license for the complete module set.

| Module | Pages | Description |
|---|---|---|
| **Home** | None | The EnterpriseView home page includes links to all module components. In addition, it displays the tasks assigned to you in the My Tasks pane. You can click the task name to open the page on which you need to perform the task. For example, in the figure above, click on Identify Vulnerabilities to open the Vulnerability Management page. |
| **Executive View** | • Overall Score Heat Map<br>• Risk Register<br>• Risk Indicators | Executive dashboards enable CIOs and CISOs to view and analyze security risk information in business context. |
| **Risk Modeling** | • Risk Heat Map and Scorecard<br>• Risk Modeling Dashboard<br>• Threat Library Builder<br>• Risk Modeling Assessment<br>• Control to Threat Mapping | Use the flexible and expandable threat library to define threat scenarios for the assets in your organization's business model and specify impact and probability to calculate their risk. |
| **Vulnerabilities** | • Vulnerability Dashboard<br>• Vulnerability Assignment<br>• Vulnerability Management<br>• Vulnerability Dictionary | Manage and remediate the vulnerabilities according to their severity and the criticality level of your assets. |
| **Policy and Compliance** | • Compliance by Policy Dashboard<br>• Compliance Dashboard<br>• Compliance Map<br>• Policy Builder<br>• Statement of Applicability<br>• Policy and Compliance Assessment<br>• Policy Mapping<br>• Vulnerability to Control Mapping | Define policies or use out-of-the-box policies to define a statement of applicability and perform audit. |

| Module | Pages | Description |
|---|---|---|
| **ESM Threats** | ESM Threat View | EnterpriseView enables a periodic import of security threats from ArcSight ESM, providing near real-time monitoring capabilities on the threats imposed on organization assets. Information is displayed graphically and enables identifying security threat trends over selected time periods. |
| **Assets** | Asset Profiling | Create and manage a business model that depicts your organization from high-level business assets to low-level IT assets, on which policy, risk and vulnerability management is performed. |
| **Task Management** | Workflow 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. |
| **Administration** | • Audit Log<br><br>• Configuration<br><br>• Job Management<br><br>• User Management<br><br>• Dashboard Builder | Administer EnterpriseView by creating customized dashboards, managing roles and permissions, monitoring batch jobs and managing application settings. |

**Personalization**

 EnterpriseView "remembers" the last asset and policy element that you worked on. When you navigate EnterpriseView the UI pages appear in the context of that asset or that policy element. For example, you can view statistical information for a specific asset in the different dashboards without having to select the asset in every dashboard. The context is also saved when you log out.

# Chapter 5

# Asset Profiling

In EnterpriseView, an asset is an entity that represents a physical or logical resource in the system. For example, assets can represent hardware, software,services, people, documents or business units.

Assets are the building blocks of the business model. They are organized into a hierarchical format based on the dependencies in your organization's IT environment.The EnterpriseView business model depicts the entire IT environment, from the highest level of the organization (such as an office location or a line of business) to the lowest level (such as a software application). Each entity in the EnterpriseView business model is an asset. For more information on building a business model, see "How to Build a Business Model in EnterpriseView" on page 19.

The business model is the foundation for all core EnterpriseView functionality. Using a business model, risk and regulation compliance (policies) can be assessed effectively, providing "apply once—affect all" capabilities. Policies can be applied to top level assets and trickled down to all lower level assets that belong to that hierarchy. Conversely, risk assessments and policy audits can be performed on lower level assets and then trickled up and aggregated to top level assets, providing a business centric analysis of security risk and policy compliance. Data analysis, scorecards, and reports can be viewed on all asset levels, providing stakeholders in an organization with direct access to data that is relevant to their specific role. An extensive business model provides EnterpriseView users with more accurate information about the organization's overall risk.

There are many different types of assets, which are divided into categories. For more information, see "Manage Asset Types" on next page.

# Manage Asset Types

EnterpriseView includes the following asset categories:

- **Organization**: Includes only one asset type—Organization. The Organization is the starting point of the business model. EnterpriseView includes a predefined Organization asset.

- **Location**: Includes types such as Country, City, and Building.

- **Business**: Includes a business reference or a line of business, such as online banking.

- **IP**: Includes only one of asset type—IP Address.

- **Infrastructure Elements**: Includes hardware, such as a computer (network entity) or a printer.

- **Running Software**: Includes software applications, such as a mail server or a database.

- **People**: Includes groups and people.

- **Documents**: Includes one asset type—Document.

Each of these categories includes various predefined asset types. In addition to the asset types that are provided by EnterpriseView, you can add new asset types to any category, except the Organization category, which includes only one Organization asset.

You can also edit or delete an asset type.

> **Note:** If you delete an asset type or change an asset type name in the Configuration module, then these changes affect only new assets; they are not automatically reflected in existing assets in the business model. Asset types that appear in the business model after being changed or deleted in the Configuration module, are displayed with a question mark icon.

## To add an asset type

1. Click **Administration > Configuration**.

2. In the **Configuration** module, in the left pane, click **Asset Management > Asset Type Categories**, and then click the asset category to which you want to add an asset type.

3. In the right pane, click the **Add configuration to configuration set** button, and then do the following:
   - In the **Type** box, enter the internal name of the asset type.

   - In the **Label** box, enter the display name of the asset type.

   - From the **Icon** drop-down list, select the image for the asset type icon.

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

## To edit an asset type

1. Click **Administration > Configuration**.

2. In the **Configuration** module, in the left pane, click **Asset Management > Asset Type Categories**, and then click the asset category to which the asset type that you want to edit belongs.

3. In the right pane, make the required changes for the asset type that you want to change.

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

## To delete an asset type

1. Click **Administration > Configuration**.

2. In the **Configuration** module, in the left pane, click **Asset Management > Asset Type Categories**, and then click the asset category from which you want to delete an asset type.

3. In the right pane, click the asset type that you want to delete, and then click the **Remove configuration from the configuration set** button.

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

# How to Build a Business Model in EnterpriseView

There are two ways to build a business model in EnterpriseView:

- **Import**: you can synchronize EnterpriseView with the external asset repository that is the primary asset management system in your organization.

  > **Note:** You can add assets that you created in EnterpriseView to an imported business model.

- **Create locally**: you can use EnterpriseView as the primary asset management system of your organization and build a business model within EnterpriseView.

The following procedures outline the steps for creating a business model in EnterpriseView.

## To import a business model

1. Follow the instructions in the *Synchronize Assets with External Asset Repository* section in the *EnterpriseView Deployment Guide*.

2. During the first import, all imported assets are saved as **Unattached**. Follow the instructions in "Connect an Asset to the Business Model" on page 21. Repeat this process until all imported assets are connected to the business model.

   Creating the business model from imported assets is a one-time task. After the business model is created, each subsequent synchronization automatically updates the business model for all existing assets, and only newly introduced assets are saved as unattached.

## To build a local business model

1. Review the predefined asset types.
   a. Click **Administration > Configuration**.

   b. On the **Configuration** window, click **Asset Management > Asset Type Categories**.

   c. Review the asset types for all categories to see whether they reflect the asset types required by your organization's business model.

   d. If required, add asset types, as described in "Manage Asset Types" on page 17.

2. Create the business model.
   a. Click **Assets > Asset Profiling**.

   b. On the **Asset Profiling** window, click the **New** tab. The predefined **My organization** asset icon is displayed in the map area.

   c. Click the **My organization** asset.

   d. In the asset card, click the **Edit Asset Properties** button, and enter the asset name and any other information that you have an this asset.

   e. Follow the instructions in "Create an Asset" on next page to add assets to the business model.

# Create an Asset

When you create a new asset in EnterpriseView you must also connect it to the business model, meaning that you cannot create an asset as unattached.

### To create an asset

1. Click **Assets > Asset Profiling**.

2. Search for the source (parent) asset, as described in "Search for an Asset" on page 22 or click the asset in the map.

3. Click the **Mark as Source Asset** button.

   The connection panel is displayed in the map area.

4. On the left pane, click the **New** tab.

5. In the **New** tab, click the asset type that you want to create and connect to the business model.

6. Click the **Create as Target Asset** button. This asset will be connected to the business model as a child asset.

7. In the connection panel, click **Create and Connect**.

   The asset is added to the business model and the **Edit Asset Properties** dialog box opens.

8. On the **Edit Asset Properties** dialog box, enter the relevant information, and then click **Save**. For a detailed description on asset properties, see "Asset Properties" on page 25.

9. To cancel the connection, in the connection panel, click **Cancel**.

> **Note:** You can also drag the asset from the **New** tab and drop it on the parent asset in the map area. For example, To create a city asset under the **My organization** asset, drag the **City** asset from the left pane and drop it on the **My organization** asset in the map area. The following path is created:
>
>

# Connect an Asset to the Business Model

You can connect unattached assets to the business model or connect assets that are already part of the business model to a different parent asset.

There are two scenarios in which assets are saved as unattached in EnterpriseView:

- Assets are saved as unattached the first time that they are imported from an external asset repository. After the business model is created, each subsequent synchronization automatically updates the business model for all existing assets, and only newly introduced assets are saved as unattached.

- Assets that have been disconnected from the business model are also saved as unattached.

## To connect an asset to the business model

1. Click **Assets > Asset Profiling**.

2. On the left pane, click the **Unattached** tab and find the asset that you want to connect ot the business model or search for the asset, as described in "Search for an Asset" on next page.

3. Click the **Mark Target Asset** button. This asset will be connected to the business model as a child asset.

   The connection panel is displayed in the map area.

4. Search for the source (parent) asset, as described in "Search for an Asset" on next page or click the asset in the map.

5. Click the **Mark as Source Asset** button.

6. In the connection panel, click **Connect**.

   The asset is added to the business model.

7. To cancel the connection, in the connection panel, click **Cancel**.

   **Note:** You can also drag the asset from the left pane and drop it on the parent asset in the map area.

# Search for an Asset

You can search for a name or a partial name of any asset, either attached to the business model or unattached.

## To search for an asset

1. Click **Assets > Asset Profiling**, and then, on the left pane, click the **Search** tab.

2. In the **Search asset name** box, enter the asset name or a partial asset name, and then press **ENTER**.

   The search results are displayed in the left pane. The two immediate parent assets are displayed next to each asset that is found.

3. Click **Advanced** to search by asset category or type. Select the category or type from the list, and then click **Search**.

4. To display the asset in the business model map, click the **Show in Map** button.

# Disconnect an Asset from the Business Model

When you disconnect an asset from the business model, the relationship between the asset and its parent asset is deleted. Only relationships that have been created within EnterpriseView can be deleted. The asset itself is not deleted; it is saved as **Unattached**. If the asset has more than one parent, then it remains in the business model. If you disconnect an asset that contains other assets, then that asset and its children remain intact.

Disconnected assets can be reconnected to the business model at any time.

### To disconnect an asset from the business model

1. Click **Assets > Asset Profiling**.

2. Search for the asset that you want to disconnect, as described in "Search for an Asset" on previous page.

3. In the **Search** tab, click the asset that you want to disconnect, and then click the **Show in Map** button.

4. In the map area, click the relationship between the asset that you want to disconnect and its parent asset, and then press **DELETE**.

    A confirmation message is displayed. Click **Yes** to confirm this action.

    The disconnected asset can be viewed in the **Unattached** tab in the left pane.

# Delete an Asset

You can delete only assets created in EnterpriseView. In order to preserve the integrity of the business model, assets imported from an external asset repository cannot be deleted directly from EnterpriseView; they must be deleted in the system from which they originated. When the business model is next synchronized, the change will be displayed in EnterpriseView.

## To delete an asset

1. Click **Assets > Asset Profiling**.

2. Search for the asset that you want to delete, as described in .

3. Click the asset that you want to delete and then click the **Delete** 🗑 button or select the asset in the map and press **DELETE**.

   A confirmation message is displayed. Confirm this action by clicking **Yes**.

   > **Note:** If you delete an asset that has children, then the asset is deleted and the children are saved as unattached.

# Asset Properties

The following table describes all of the properties for each asset category.

**Asset Properties**

| Category | Property | Description |
|---|---|---|
| General | **Name**<br><br>(mandatory) | The name of the asset. It is displayed in the business model's graphic view along with the asset type icon. |
| | **Description** | Additional information about the asset. |
| | **Type** | The asset type. |
| | **Source** | The source name for the Organization asset is **System**.<br><br>The source name for assets created in EnterpriseView is empty.<br><br>For assets imported from an external asset repository, the source name is the same as the connector name defined in the **Configuration** module. |
| | **Owner** | The person in the organization responsible for the asset and who is contacted in situations requiring manual intervention. |
| Location | **Latitude** | The geographical coordinates of the asset's location. |
| | **Longitude** | The geographical coordinates of the asset's location. |
| | **Address** | The street address of the asset. |
| | **ZIP Code** | The asset location ZIP code. |
| | **City** | The city of the asset. |
| | **State** | The state of the asset. |
| | **Country** | The country of the asset. |
| | **Criticality Level** | A numeric index, between 0 and 10, indicating the severity of a potential catastrophe and the probability of its occurrence.<br><br>The default criticality level of all assets is 1.<br><br>The criticality level of an asset affects the weight of its scores when policy assessment aggregation, risk aggregation, and vulnerability score aggregation are done. For more information, see "Weights and Criticality Level" on page 66, "Risk Score Aggregation Mechanism" on page 90, and "Asset Vulnerability Score Aggregation Mechanism" on page 156. |

| Category | Property | Description |
|---|---|---|
| Business | **Criticality Level** | See "Criticality Level" on previous page |
| | **Value** | A numeric, monetary value. |
| Infrastructure Element | **OS Name** | The operating system that is installed on the infrastructure element. |
| | **OS Version** | The version of the operating system that is installed on the infrastructure element. |
| Running Software | **Application Name** | The name of the application. |
| | **Application Version** | The version of the application. |
| IP | **DNS Name** | The server name as defined in the network DNS. |
| | **MAC Address** | The server MAC address. |
| | **IP Address** | The server IP address. |
| People | **Role** | The role of the person or the group in the organization. |
| Documents | **Version** | The version of the document. |
| | **Purpose** | The purpose for which the document was created. |
| | **Classification** | The type of document, such as legal or technical. |
| | **Release Date** | The date on which the document was published. |

# Asset Profiling Window

The Asset Profiling window enables you to create and maintain your organization's business model.The different areas and the functionalities available in each are described in the following sections.

## Map Area

| UI Element | Description |
|---|---|
| (Layout) | **Tree**<br><br>Tree structured graph. |
| (Layout) | **Circular**<br><br>Interconnected ring and star topology. |
| | **Optimize Layout**<br><br>Refreshes the layout of the business model in the graph. |
| | **Fit to Window**<br><br>Resizes and displays the entire business model in the map area. |
| **Save View** | Saves the current business model view displayed in the map.<br><br>After you save the view, when you reopen the Asset Profiling page, the business model displayed in the map area is resized to the default zoom and to fit to window.<br><br>**Note:**<br><br>• A business model view can have only one root asset.<br><br>• Assets that were disconnected from the business model are not displayed in the view.<br><br>Views are saved for each user. |
| | **Zoom**<br><br>Zooms the business model in and out. |
| | **Refresh**<br><br>Refreshes the data on the page. |

## Left Pane

| UI Element | Description |
|---|---|
| **Search tab** | The Search tab enables you to search for a name or a partial name of any asset in EnterpriseView, connected to the business model or unattached. You can also search by asset category or type by clicking **Advanced**. |
| **Unattached tab** | The Unattached tab includes assets that have either been imported from an external asset repository and have not been connected to the business model or any asset that has been disconnected from the business model. |
| **New tab** | The New tab displays all of the asset types according to categories. When you create a new asset in EnterpriseView you also connect it to the business model. |
|  | **Delete**<br><br>Deletes the selected asset.<br><br>You can delete only assets created in EnterpriseView. In order to preserve the integrity of the business model, assets imported from an external asset repository cannot be deleted directly from EnterpriseView; they must be deleted in the system from which they originated. When the business model is next synchronized, the change will be displayed in EnterpriseView. If you delete an asset that has children, then the asset is deleted and the children are saved as unattached.<br><br>This button is available in:<br><br>● **Search** tab<br>● **Unattached** tab<br>● **Asset Card** |
|  | **Show in Map**<br><br>Displays the asset in the business model in the map area.<br><br>This button is disabled if the asset is unattached.<br><br>This button is available in:<br><br>● **Search** tab |

| UI Element | Description |
|---|---|
| | **Edit Asset Properties** |
| | Opens the **Edit Asset Properties** dialog box. For more information on asset properties, see "Asset Properties" on page 25. |
| | This button is available in: |
| | • **Search** tab |
| | • **Unattached** tab |
| | • **Asset Card** |
| | **Connect to another asset (mark as source asset)** |
| | Marks an asset as the parent asset when you connect an asset to the business model. A source asset must be attached to the business model. |
| | This button is available in: |
| | • **Search** tab |
| | • **Asset Card** |
| | **Mark as target asset** |
| | Marks an asset as the child asset when you connect it to the business model. A target asset can be unattached or already connected to the business model. |
| | This button is available in: |
| | • **New** tab |
| | • **Unattached** tab |
| | • **Search** tab after the source asset has been defined |
| | • **Asset Card** after the source asset has been defined |
| | **Refresh**<br>Refreshes the business model to display any changes that might have occurred, for example, synchronization with an external asset repository. |
| | Available in all tabs. |
| | **Collapse** |
| | Collapse the left pane. |
| | **Expand** |
| | Expand the left pane. |

## Asset Card

You can open the asset card by clicking on the asset in the business model map.

The asset card includes the asset name, category and type. The following table includes the functionality available from the asset card.

| UI Element | Description |
|---|---|
| 🗑 | See "Delete" on page 28. |
| ⬉ | See "Connect to another asset (mark as source asset)" on previous page |
| ⬈ | See "Mark as target asset" on previous page. |
| ⛬ | See "Edit Asset Properties" on previous page. |
| **Expand** | Show the direct children of the asset in the business model map. |
| | Click **More > Expand**. |
| | If the asset has more than 20 children, then the assets are not displayed automatically in order not to overload the business model. In this case, the **Show Children on Map for Asset** dialog box is displayed, enabling you to select the children you want to display. The number of direct children that an asset has is displayed in the business model map by the asset name. |
| | You can also expand by double-clicking the asset. |
| **Collapse** | Hide the direct children of the asset in the business model map. |
| | Click **More > Collapse**. |
| | You can also collapse by double-clicking the asset. |
| **Show Parents** | Show the parent assets of the asset in the business model map. |
| | Click **More > Show Parents**. |
| **Hide Parents** | Hide the parent assets of the asset in the business model map. |
| | Click **More > Hide Parents**. |
| ⌄ | **Open Properties** |
| | View properties in read-only mode. For more information on asset properties, see "Asset Properties" on page 25. |
| ⌃ | **Close Properties** |
| | Close properties view. |

## Mini-map

When the business model is expanded to a larger size than the map area, you can navigate it by clicking and dragging in the mini-map area.

To expand or collapse the mini-map, click the **Expand/Collapse**  button.

# Chapter 6

# Policy and Compliance

Organizations must fulfill a set of legal, statutory, regulatory, and contractual requirements in order to satisfy their trading partners, contractors, service providers and socio-cultural environment. These requirements are bound in policies. EnterpriseView provides a set of integrated components that create a complete security policy compliance management framework.

The following components comprise the stages of policy management:

- **Policy creation and library**

  The EnterpriseView policy library includes out-of-the-box policies, such as NIST800-53, PCI DSS v2.0, and HIPAA Security Rule (NIST), in addition to a Unified Compliance Framework (UCF) policy. UCF contains a comprehensive set of IT regulatory compliance controls compiled from hundreds of industry standard polices such as PCI, HIPPA ,and ISO/IEC 27001, allowing you to assess once and comply with many. For more information, see "About Unified Compliance Framework" on page 34.

  EnterpriseView Policy Builder includes a highly configurable policy template for defining in-house policies, as described in "How to Create a Policy" on page 37. The policy template can be easily simplified or enhanced. It can be configured to include basic control definitions, blocks of text for emulating the different parts of traditional industry standard policy books (such as sections and chapters on various levels) or it can be more comprehensive, including parameters such as auditing attributes (for example: priority, GRC designation, type, and purpose).

  Control maturity and compliance acceptance levels are derived from the maturity and compliance score ranges, defined, and can be edited in the Policy Builder. For more information, see "Configure Compliance and Maturity Score Ranges" on page 49.

- **Policy Mapping**

  EnterpriseView policy mapping capability enables you to perform policy compliance assessments on assets for a single policy and create compliance reports for multiple policies, saving you the effort of assessing the compliance for each policy to which your organization is obligated. For more information, see "Policy Mapping" on page 45.

- **Setting Statements of Applicability (SoA)**

  The SoA identifies the controls chosen for the assets in the organization. The SoA is derived from the output of the risk assessment and directly relates the selected controls back to the original risks they are intended to mitigate. Both industry standard and in-house controls can be applied, as described in "Set Statement of Applicability" on page 41. Applied controls are trickled down to lower-level assets and can be viewed at any point on the business model hierarchy, but can also be overridden for specific assets. Controls that are not applicable are also defined, complying with industry best practices.

- **Auditing**

EnterpriseView enables you to assess policy compliance and control maturity for all assets that comprise your organization's business model, as described in "Audit Assets" on page 42.

EnterpriseView applies a Control Maturity Model, which is aligned primarily with the widely adopted Capability Maturity Model (CMM), in order to benchmark IT processes, performance, and capability, performed via the Policy Assessment module. The Control Maturity Model is implemented by a scoring method that is based on five factors that make up the overall control score. This scoring method results in a higher level of quality in the deployment of a security control on an asset. For more information, see "P5 Control Maturity Model Guidelines" on page 60.

The policy assessment module also supports control audit annotation and attachments.

- **Assessment Aggregation**

Policy audits can be performed on lower-level assets and then trickled up and aggregated to top-level assets, providing a business centric analysis of security risk and policy compliance. For more information, see "Control Scores Aggregation Mechanism" on page 61. Assessments can also be overridden for specific assets, as described in "Apply Aggregated Scores" on page 44.

# About Unified Compliance Framework

Unified Compliance Framework (UCF) is an industry-vetted compliance database that includes a comprehensive set of IT regulatory compliance controls from hundreds authority documents, such as PCI, HIPPA, and ISO/IEC 27001. UCF eliminates overlapping controls and bridges the gaps between the different authority documents, providing you with a harmonized list of controls.

In EnterpriseView, UCF is portrayed as a single policy, allowing you to assess one policy while complying with the many policies to which your organization is obligated.

The structure of the UCF policy in EnterpriseView is a simplified version of the original framework, which includes main security categories containing a flat list of controls. The controls are grouped according to main security categories (known as Impact Zones in UCF) and include their control ID.

The following table includes the mapping between EnterpriseView policy elements and their corresponding elements in UCF.

| EnterpriseView | UCF | Additional Information |
|---|---|---|
| **Policy** | **Authority Document** | In the original framework, every control includes Citations. Each citation includes a reference to an authority document that has this control or a similar, corresponding control. |
| | | In EnterpriseView, UCF is represented as a policy entity. The various authority documents, such as PCI, HIPPA, and ISO/IEC 27001, are not represented as standalone policies. Instead, they are used to filter controls when creating the Statement of Applicability, as described in "Set Statement of Applicability" on page 41 and for reporting purposes. |

| EnterpriseView | UCF | Additional Information |
|---|---|---|
| **Main Security Category** | **Impact Zone** | UCF includes impact zones, such as:<br><br>• Leadership and High Level objectives<br><br>• Audit and Risk Management<br><br>• Product Design and Development<br><br>• Acquisition of Technology<br><br>• Operational Management<br><br>• Human Resources Management<br><br>• Records Management<br><br>• Technical Security<br><br>• Physical Security<br><br>• Systems Continuity<br><br>• Monitoring and Reporting<br><br>• Privacy<br><br>• System Hardening Through Configuration Management |
| **Control Text** | **Control Statement** | In some cases when a Control Statement does not exist, then the control text reflects the Policy Statement. |
| **Title** | **Control Title** | |

# Using Vulnerabilities to Refine the Compliance Score

There is an inherent correlation between vulnerabilities and policy controls. Vulnerabilities are a factors throughout the life cycle of a control. A vulnerability may be the primary cause for defining a control, its existence or lack of it may affect the organization's decision of applying a control, and its persistence affects the level of compliance of a control.

EnterpriseView includes out-of-the-box mappings between vulnerabilities defined in the vulnerability dictionary and the policies provided with EnterpriseView. These mappings represent the correlation between controls and vulnerabilities.

Vulnerabilities automatically affect the compliance score of a control when the following conditions occur:

• The vulnerability is mapped to the control

• The control is applied to an asset

• The vulnerability is attached to the asset

The compliance score is affected as follows:

- If the control is manually assessed or if it's assessment was imported from an external system, then the vulnerability lowers the control's compliance score. The following indication is displayed on the screen below the compliance score.

  "Score is affected by <n> vulnerabilities. Reduced by m%."

  You can click the "n vulnerabilities" link to view the details of the vulnerabilities that are mapped to the control. For more information, see "Score is affected by <n> vulnerabilities " on page 58.

- If the control is not assessed, then its compliance score is changed from Not Assessed to "0".

> **Note:** This feature can be disabled for each control by selecting the **Ignore Vulnerabilities** check box in the Policy Assessment window, as described in "Policy Assessment Window" on page 55.

Most mappings are between a control and a group of vulnerabilities rather than between a control and an individual vulnerability. Vulnerabilities are grouped according to different vulnerability types. EnterpriseView adopted the Common Weakness Enumeration (CWE) system for identifying most vulnerability groups. Other vulnerability groups are internal and can be identified by an "EVG" prefix.

The formula that is used to determine the impact of vulnerabilities on a control's compliance score considers the following variables:

- The vulnerability score. For more information on the vulnerability score, see "Vulnerability Properties" on page 150.

  There is a negative correlation between the vulnerability score and the control's compliance score; the higher the vulnerability score, the lower the compliance score will be.

- The number of vulnerabilities that are mapped to the control.

- The weight of the vulnerability with the highest score.

You can search for specific mappings using free text. To access the **Policy Vulnerability Mapping** window, click **Policy and Compliance > Policy Vulnerability Mapping**.

> **Note:** You can perform wildcard searches. For example, if you type **ser\***, the results will contain words beginning with ser (such as server and service). An asterisk cannot be placed before a string (*ser).

# How to Create a Policy

EnterpriseView includes the Unified Compliance Framework, as described in "About Unified Compliance Framework" on page 34. You can also create your own policies. When you create a new policy, you can decide on the complexity of its format and you can configure the control template to suit the needs of your organization and the specific policy.

Creating the policy is a two-step process:

1. Create the policy and configuring the policy template. It is recommended that you plan the policy template in advance. However, you can modify the template at any time.

2. Add content to the policy.

After you have created a new policy, if you want to begin working with the policy, you need to activate it, as described in "Activate a Policy" on next page.

You can fully modify policies that you created in EnterpriseView. For out-of-the-box policies or imported policies, you can modify the control template and add guidelines to controls, but you cannot modify the content of the policy.

## To create a new policy and configure the policy template

1. Click **Policy and Compliance > Policy Builder**.

2. On the **Policy Builder** page, click **Create Policy**.

3. On the **Template** page, do the following, and then click **Save** or **Save and Activate**:

   a. In the **Policy Name** box, enter a name for the policy that you are creating.

   b. In the **Policy Description** box, enter a description for the policy.

   c. In the **Control Template** area, select the attributes relevant for this policy according to the information available in the Template tab, as described in "Template Tab" on page 52.

## To add content to the policy

1. In EnterpriseView, click **Policy and Compliance > Policy Builder**.

2. On the **Policy Builder** page, in the left pane, click the **Content** tab. In the left pane, from the policy drop-down list, select the policy to which you want to add content.

3. Follow these steps to add a Main Security Category. For more information on policy attributes, see "Template Tab" on page 52.

   a. In the left pane, click the **New Main Security Category** button.

   b. In the right pane, enter the following information, and then click **Save**:

      ○ **Paragraph Number**: Can be any alphanumeric string, up to 255 characters

      ○ **Title**: Of the security category

      ○ **Text**: Any additional text explaining this security category

4. Add more security category levels, if required.

a. In the left pane, click the security category to which you want to add another level, and then click the **New Security Category** button.

b. In the right pane, enter the required information, as described in the previous step. Click **Save**.

5. Add controls to the security categories, as required.

a. In the left pane, click the security category to which you want to add the control, and then click the **New Control** button.

b. In the left pane, enter control information, as described in "Template Tab" on page 52. Click **Save**.

6. Repeat steps 3 through 5 to complete the policy content.

# Activate a Policy

You must activate a policy before you can start working with it. Policies that you do not activate are not displayed in any of the pages that belong to the Policy and Compliance module, except for the Policy Builder.

There are two ways to activate a policy:

- Through the policy builder. This option is recommended when you want to create a policy and immediately activate it.

- Through the EnterpriseView **Settings** dialog box. This option is recommended for managing the state of all the policies in EnterpriseView.

### To activate a policy through the Policy Builder

1. If you have not just created the policy, click **Policy and Compliance > Policy Builder** and from the top left pane, select the policy that you want to activate.

2. Click the **Settings** tab, and then select the **Activate Policy** check box.

3. Click **Save**.

### To activate a policy through the EnterpriseView Settings dialog box

1. On the EnterpriseView toolbar, click **Settings**.

2. In the **Settings** dialog box, click **Policy and Compliance > Policy Administration**.

3. On the **Policy Administration** page, select the check boxes of the policies that you want to work with.

   If you selected the **Unified Compliance Framework** check box, then from the **Available Authority Documents** list, click the authority document that you want to view, and then click the **Add** button. Repeat this for all required authority documents. To remove an authority document, click the authority document from the Selected Authority Documents list, and then click the **Remove** button.

4. Click **Save**.

# Import a Policy

You can import policies in XML format from your local computer into EnterpriseView. The XML file must match the XML Schema Definition (XSD), which you can find in the following location:

**<server_URL>/redcat/content/policy.xsd**

> **Note:**
>
> - The paragraph numbers of all the policy elements in the XML must be unique.
>
> - Policy names in EnterpriseView are unique; you cannot import a policy that already exists.

## To import a policy

1. Click **Policy and Compliance > Policy Builder**, and then click **Import Policy**.

2. On the **Select file to upload by** dialog box, navigate to the location of the file, select the file, and then click **Open**.

3. After the policy is imported, you are prompted to activate the policy.

# Delete a Policy

**Note:** You cannot restore a deleted policy.

Out-of-the-box policies and policies that are in an assessment process cannot be deleted. If you delete a policy that is mapped to another policy, then these mappings are deleted.

## To delete a policy

1. Click **Policy and Compliance > Policy Builder**.

2. In the left pane, from the policy list, select the policy that you want to delete, and then, on the top right-hand side, in the Policy Toolbar, click **Delete Policy**.

3. A confirmation message is displayed. Click **OK** to confirm this action.

# Set Statement of Applicability

You can apply controls to assets, which will be assessed during the auditing phase. Once applied, controls are automatically trickled down to all lower-level (children) assets. You can override these settings and reapply controls to the lower-level assets.

> **Note:** After an asset has entered the assessment process (meaning that at least one control that is applied to the asset is already assessed for a specific policy), then none of the controls that are applied to this asset can be removed. However, controls that are not applied to this asset can be applied at any time.

To comply with industry best practices, it is recommended that you explicitly identify controls that are not applicable to the asset.

## To apply controls to assets

1. Click **Policy and Compliance > Statement of Applicability**.

2. On the **Statement of Applicability** page, in the left pane, in the **Organization** tab, expand the business model tree and locate the asset for which you want to set applicability. You can also search for an asset, as described in "Search for an Asset" on page 22.

3. In the **Unassigned Controls** pane, from the policy drop-down list, select the required policy.

   All of the controls that belong to this policy but have not yet been assigned to the asset that you have selected are displayed below the policy. The controls are grouped according to their security category.

4. Click [ ] next to the security category to expand and display the controls. The number of unassigned controls in the security category is displayed. For example, (12/12) means that 12 out of 12 controls that belong to the security category are not yet assigned to the asset that you have selected.

5. If you select the Unified Compliance Framework policy, then you can filter the results according to a specific authority document or policy in EnterpriseView. For more information, see "About Unified Compliance Framework" on page 34. Enter the name of the authority document in the **Filter by authority document** box. The results are filtered accordingly.

6. From the list of controls, do the following:

   a. Drag the controls that you want to apply to the asset to the **Applied to Asset** area. You can drag an entire security category or a main security category.

   b. Drag the controls that are not applied to the asset to the **Not Applied to Asset** area.

   c. Drag controls or security categories between the **Applied to Asset** area and the **Not Applied to Asset** area, as needed.

   The controls that you applied to the asset are automatically applied to all the assets that are contained in the asset. All controls that inherit their applicability from their parent asset are marked with the **Inherited from: <asset>** [ ] icon. If you decide that a policy, a control, or a set of controls are no longer relevant to an asset, then you can return the controls to the **Unassigned Controls** pane. The controls are removed from all children.

You can override these settings and reapply controls to any asset, as described in the following procedure.

### To override control applicability

1. Click **Policy and Compliance > Statement of Applicability**.

2. On the **Statement of Applicability** page, in the left pane, in the **Organization** tab, expand the business model tree and locate the asset for which you want to override applicability. You can also search for an asset, as described in "Search for an Asset" on page 22.

3. Make the necessary changes by dragging the controls from the **Applied to Asset** area to the **Not Applied to Asset** area and vice versa. Controls for which applicability has been overridden are marked with the **Inheritance Exception: <asset>** icon.

# Audit Assets

EnterpriseView enables you to apply a quantitative assessment to assets on two levels:

- **Control Maturity**: Helps identify capability gaps. These gaps can be demonstrated to management, and action plans can then be developed to bring these controls up to the desired capability target level.

- **Asset Compliance**: Helps assess compliance with a policy control.

Both scores are automatically aggregated to higher-level assets. For more information, see "Control Scores Aggregation Mechanism" on page 61. Aggregated scores can be overridden. If you have manually or automatically applied a score, you can restore the aggregated score for a specific control on a specific asset, as described in "Apply Aggregated Scores" on page 44.

If the control that you are assessing is mapped to another control and they are both applied to the asset, then an indication that the control is mapped is displayed, and you can access the mapped control details.

> **Note:** Scores that were applied manually are not overridden by aggregation.

Assets are assessed in the Policy Assessment window. For more information, see "Policy Assessment Window" on page 55.

When assessments are obsolete, you can clear them, as described in "Clear Assessment on Assets" on next page.

### To audit an asset

1. Click **Policy and Compliance > Assessment**.

2. In the left pane, click **Select an Asset**, expand the asset tree, and click the asset that you want to assess. Alternatively, search for the asset by entering its name. Click **OK**.

   The policies that are relevant to this asset (those that have at least one control assigned to the asset) are displayed in the left pane.

3. From the left pane, select the required policy. Expand the policy, and then click the control that you want to assess.

The **Assessment** tab opens in the right pane.

4. Review the P5 Control Maturity Model Guidelines, as described in "P5 Control Maturity Model Guidelines" on page 60 in order to determine the appropriate control maturity score to apply to each maturity factor. Apply a maturity score for all relevant factors by using the slider.

   The **Maturity Score** is a weighted average of all maturity factors. Maturity factor weights are defined in the policy template. For more information, see "P5 Applicability Weights" on page 52.

5. Use the **Compliance Score** slider to select a score between 0 and 100.

6. Click **Save**.

   If there are vulnerabilities mapped to the control, then the compliance score is automatically recalculated (reduced) to include the impact of the vulnerabilities. For more information, see "Using Vulnerabilities to Refine the Compliance Score" on page 35.

   The maturity score is calculated, in addition to the maturity assessment progress, which reflects how many maturity factors have been assessed. Each maturity factor counts for a percentage of the overall score, depending on the number of maturity factors employed. For example, if all maturity factors are employed, then each factor counts for 20% of the overall score. If two out of the five maturity factors have been assessed, then the maturity assessment progress will be 40%. The scores and progress are displayed in the Control Data area. For more information, see "Policy Assessment Window" on page 55.

   The **Maturity Score**, **Compliance Score** and the **Maturity Progress** are trickled up and aggregated to higher-level assets for every applied control. Their values are displayed in the left pane in the asset tree. For more information, see "Control Scores Aggregation Mechanism" on page 61.

   The date and time of this assessment is updated in the **Last Updated On** field.

# Clear Assessment on Assets

You can clear assessments on assets for outdated audits. This action is performed on the entire business model, meaning that the assessments on all assets are cleared for the policies that you select. This action invokes the Archive Trend Data Job. For more information on this job, see the *Archive Trend Data* section in the *HP EnterpriseView Administration Guide*.

> **Note:** The assessments for the policies that you selected will be permanently deleted. Notes or attachments connected to these assessments are also deleted. This action cannot be reversed.

### To clear assessments

1. Click **Policy and Compliance > Assessment**.

2. On the **Policy and Compliance Assessment** window, click **Clear Assessment**.

3. On the **Clear Assessment** dialog box, select the policies for which you want to clear assessments, and then click **OK**.

   This action might take a few minutes. Refresh the page to see the changes.

# Apply Aggregated Scores

If you applied a compliance score or a control maturity score, either manually or automatically, then you can override these scores with scores aggregated from lower-level assets. The score is aggregated according to the logic described in "Control Scores Aggregation Mechanism" on page 61.

### To apply aggregated scores

1. Click **Policy and Compliance > Assessment**.

2. In the left pane, click **Select an Asset**, expand the asset tree, click the asset that you want to assess, and then click **OK**.

   The policies that are relevant to this asset (those that have at least one control assigned to the asset) are displayed in the left pane.

3. From the left pane, select the required policy. Expand the policy, and then click the control that you want to assess.

   The **Assessment** tab opens in the right pane.

4. Click **Apply Aggregation**, and then click **Save**.

# Policy Mapping

EnterpriseView policy mapping capabilities allow you to perform policy compliance assessments on assets for a single policy and create compliance reports for multiple policies, saving you the effort of assessing the compliance for each and every policy to which your organization is obligated.

EnterpriseView includes mappings between controls in the Unified Compliance Framework (UCF) policy and the controls of the rest of the policies provided with EnterpriseView. You can import mappings between UCF and policies that are not included in your EnterpriseView package, such as ISO/IEC 27001 and ISO/IEC 27002. For more information on obtaining this content, contact your EnterpriseView representative. For more information on importing UCF mappings, see "Import UCF Mappings" below.

You can also map controls between polices. For more information on mapping policy controls, see "Map Controls" on next page.

When assets are being assessed by auditors, if a control is mapped to another control and both controls are applied to the asset, then the auditor can access the details of the mapped control (for both source controls and target controls) from the Policy Assessment window.

## About the Policy Mappings Import Job

The Policy Mappings Import Job imports mappings between UCF controls and controls of other policies into the EnterpriseView database, as follows:

> **Note:** The job can import multiple files. Each file is handled separately. As such, it is possible for one file to be imported successfully, while another import fails. To verify the status of each file, refer to the following log:
>
> **<EnterpriseView Installation Folder>/logs/redcat.log**

1.  The process opens the first file from the following location:

    **<EnterpriseView Installation Folder>/content/policyMapping**

2.  The process identifies the policy that is mapped to UCF. The name of the policy in the file must match the name of the policy in EnterpriseView.

3.  The process copies all the mappings into the EnterpriseView database. The control data in the file must be identical to the control data in EnterpriseView. If it is not identical, the import of the file fails.

4.  If there is another mappings file, the process proceeds to the next file.

## Import UCF Mappings

You can import mappings between UCF and policies that are not included in your EnterpriseView package, such as ISO/IEC 27001 and ISO/IEC 27002. For more information on obtaining this content, contact your EnterpriseView representative.

Before you begin, make sure that the policies for which you are importing mappings, are in EnterpriseView. For information on importing policies, see "Import a Policy" on page 39.

### To import UCF mappings

1. Copy the mapping files to the following location:

   **<EnterpriseView Installation Folder>/content/policyMapping**

2. Run the **PolicyMappingsImportJob** from the Job Management module, as described in the *Launch Batch Jobs Manually* section in the *HP EnterpriseView Administration Guide*.

   For more information on the Policy Mappings Import Job, see "About the Policy Mappings Import Job" on previous page.

# Map Controls

When you map controls between polices, you need to select a source policy and a target policy. Control mapping is a two-way mapping; target controls are mapped to source controls and vice versa. This means that mapped policies can serve as either a source or a target. Assessments can be done on a source policy, but compliance reports are generated for a target policy and vice versa.

### To map controls between policies

1. Click  **Policy and Compliance > Policy Mapping**.

2. In the **Source Policy** pane, from the **Select a policy** drop-down list, select a source policy.

   The security categories of the policies are displayed. Expand the security categories to display their controls. Controls in the source policy that are not mapped appear in bold.

3. In the **Target Policy** pane, from the **Select a policy** drop-down list, select a target policy.

   The security categories of the policies are displayed . Expand the security categories to display their controls.
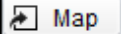
4. From the **Source Policy** pane, from the list of controls, select the control that you want to

   map, and drag it to the **Source** column in the **Mapped Controls** table or click the [↪ Map] button.

   The control that you added to the mapping is displayed in a regular font style (not bold) in the policy tree in the **Source Policy** pane.

   > **Note:** You cannot add controls to the **Mapped Controls** table until both **Source Policy** and **Target Policy** are selected.

5. From the **Target Policy** pane, from the list of controls, select the control that you want to map, and drag it to the **Target**  column in the **Mapped Controls** table that reads "**Drag here**". Or

   click the [↪ Map] button.

   The **Mapped Controls** table displays only the paragraph number of the control; it does not display the control title.

6. Repeat steps 4 and 5 until all of the required controls are mapped.

A source control is displayed only once in the **Mapped Controls** table, even if it is mapped to more than one target control. However, if more than one target control is mapped to the same source control, then all of the target controls are displayed in the same table cell.
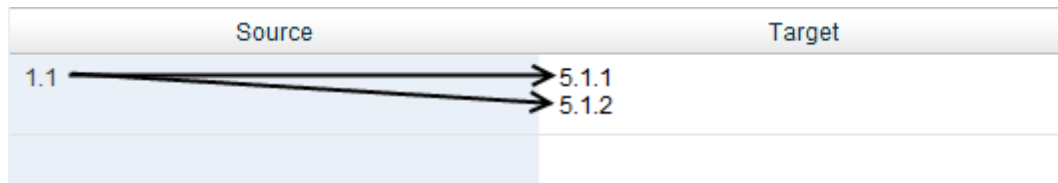


# Search for Controls

You can search for mapped or unmapped controls.

## To search for controls

1. Click **Policy and Compliance > Policy Mapping**.

2. You can search for source controls or target controls. Do one of the following:

   a. In the **Source Policy** pane, from the **Select a policy** drop-down list, select a source policy. In the **Search Source Controls** box, enter the control paragraph number, title or both. You can also enter a partial search string.

   b. In the **Target Policy** pane, from the **Select a policy** drop-down list, select a target policy. In the **Search Target Controls** box, enter the control paragraph number, title, or both. You can also enter a partial search string.

## To search for mapped controls

1. Click **Policy and Compliance > Policy Mapping**.

2. In the **Source Policy** pane, from the **Select a policy** drop-down list, select a source policy, and in the **Target Policy** pane, from the **Select a policy** drop-down list, select a target policy.

   All of the control mappings between the two policies that you selected are displayed.

3. In the **Mapped Controls** pane, in the **Search Associated Controls** box, enter the paragraph number of either a source control or a target control. You can also enter a partial search string.

   **Note:** The search field is not case sensitive.

# Delete Mapping Between Controls

You can delete mappings between the controls of various policies. Deleting a mapping is done on the source control level, meaning that if the source control is mapped to more than one target control, then all of these mappings are deleted. If the source control is mapped to controls in other polices, these mappings are not affected.

   **Note:** Changes made to control mapping might be reflected in policy assessment reports.
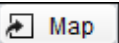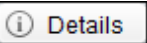
### To delete a mapping between controls

1. Click **Policy and Compliance > Policy Mapping**.

2. In the **Mapped Controls** table, locate the mapping that you want to delete. You can use the **Search Associated Controls** box to filter the mappings. For more information, see "Search for Controls" on previous page.

3. Click the **Delete Mapping** ⊠ button. A confirmation message is displayed. Confirm this action.

   The mapping is deleted from the **Mapped Controls** table.

# Policy Mapping Window

The Policy Mapping window enables you to map controls between a source policy and a target policy. For more information, see "Policy Mapping" on page 45. The different areas and the functionalities available in each are described in the following sections.

| UI Element | Description |
|---|---|
| ⮕ Map | Click this button to add the selected control to the **Associated Control** table. This button is only enabled when both a source policy and a target policy are selected and when an unmapped control in the source policy is selected. You can also drag and drop controls to the **Mapped Controls** table. For more information, see "Map Controls" on page 46. |
| ⓘ Details | Click a control and then click this button to display the control details. |
| <**Search Controls**> | This page provides three different search options: <br><br>● **Search Source Controls**. Search within the list of controls that belong to the source policy, both mapped and not mapped. <br><br>● **Search Target Controls**. Search within the list of controls that belong to the target policy, both mapped and not mapped. <br><br>● **Search Associated Controls**. Search for controls that are already mapped, from the **Mapped Controls** pane. <br><br>For more information, see "Search for Controls" on previous page. |
| ⊠ | Click the control that you want to delete from the **Source** column in the **Mapped Controls** pane, and then click this button. For more information, see "Delete Mapping Between Controls" on previous page. |

| UI Element | Description |
|---|---|
| **<% controls mapped>** | The percentage of controls from the target policy that are mapped to controls in the source policy. Displayed on the bottom of the **Target Policy** pane. |
| **<Controls not mapped:>** | The number of source controls that are displayed in the **Mapped Controls** table, but do not have a target control mapped to them. This indication helps you manage your mappings by filtering controls that are in the process of being mapped and for which mapping has not been completed.<br><br>To the left, you can also see a list of these controls, by control paragraph number. Click in the list, and then select the control to which you want to navigate to in the **Mapped Controls** table. |
| ▲ | **Go to previous unassociated control**<br><br>This button helps you navigate between source controls that are displayed in the **Mapped Controls** table but that do not have a target control mapped to them. |
| ▼ | **Go to next unassociated control**<br><br>This button helps you navigate between source controls that are displayed in the **Mapped Controls** table but do not have a target control mapped to them. |

# Configure Compliance and Maturity Score Ranges

You can configure the ranges for the score severity indication for compliance and maturity scores.

Scores are displayed with one of the following icons:

☑ High score

⚠ Medium score

☒ Low score

This configuration is reflected throughout the application, wherever these scores are displayed. For example, on the Policy and Compliance Assessment page, wherever a compliance score or a maturity score is displayed.

### To configure maturity and compliance score ranges

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Policy and Compliance > Compliance and Maturity Score Ranges**.

3. On the **Compliance and Maturity Score Ranges** page, drag the slider to define the ranges for maturity or compliance score, and then click **Save**.

# Configure Compliance KPI

The compliance KPI is used to determine how close or far the organization is from it's compliance objectives. The KPI indicates the percentage of assets, out of both direct and indirect children, with an aggregated compliance score that is lower than a certain threshold. The higher the percentage the farther the organization is from its compliance objectives.

This KPI reflects the tolerance of your organization to lack of compliance. It is configurable and should be derived from your organization's strategic plans.

The compliance KPI is displayed in the Risk Register page. For more information, see "Risk Register" on page 96.

For more information on KPIs, see "Key Performance Indicators" on page 92.

## To configure compliance KPI

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Policy and Compliance > Compliance KPI**.

3. On the **Compliance KPI** page, do the following:

    a. Under **Compliance Score KPI - Threshold**, enter a number between 0 and 100, inclusive.

    b. Under **Compliance Score KPI - Percentage Ranges**, drag the slider to the define the severity of the percentage ranges.

4. Click **Save**.

# Policy Builder Window

The Policy Builder window enables you to define new policies according to a configurable template, edit existing policies, import policies, create reports, and delete policies. The different areas and the functionalities available in each are described in the following sections.

## Policy Toolbar

| UI Element | Description |
|---|---|
| **<Policy drop-down>** | Select a policy from the drop-down. |
| **Content tab** | See "Content Tab" on page 53. |
| **Template tab** | See "Template Tab" on next page. |
| **Import Policy** | Click this button to import a policy. For more information, see "Import a Policy" on page 39. |
| **Create Policy** | Click this button to create a new policy. For more information, see "How to Create a Policy" on page 37. |
| **Delete Policy** | Click this button to delete a policy.<br><br>This button is disabled if the assessment process has begun (meaning that at least one control that is applied to an asset is assessed).<br><br>**Note:** If you delete a policy that includes controls that are already assigned to an asset, whether the controls are applied to the asset or not, then the assignment and any related assessment are deleted. |
| Reports ⌄ | **Generate Report**<br><br>Click this button and select a report from the list of reports. If you are prompted, select to always allow pop-ups from the EnterpriseView server. You can save the report as a PDF or open it in a separate browser window. |

## Template Tab

Use this screen to configure the control template for each policy that you create.

| UI Element | Description |
|---|---|
| **Control Text**<br><br>**Guideline Introduction**<br><br>**Guidelines**<br><br>**Guideline Additional Text**<br><br>**Additional Information** | The **Basic** attributes include content elements. Selecting an attribute adds a text box to the control in which you can add content. For example, if the control has numerous guidelines, you can select the **Guidelines** attribute.<br><br>If you add Guidelines to your template, when you create the content for the policy, you will have the option of adding tags (short, descriptive text) to the guidelines. You can remove a tag by clicking the X on the right side of the tag. Tag names are limited to 64 characters.<br><br>The **Control Text** attribute is selected by default. |
| **P5 Applicability Weights** | You can apply different weights to the P5 control maturity factors. For example, if the organization business strategy is focused on the human factor, give People a higher weight than the other factors. The weights affect the calculation of the P5 maturity score when a control is assessed.<br><br>By default, all of the P5 control maturity factors are selected. Clearing the check box will remove the specific factor from the control, meaning that the factor is not displayed when the control is assessed.<br><br>You can narrow down the factors for a specific control further when you add content to the policy. For more information, see "How to Create a Policy" on page 37. |
| **Priority** | You can prioritize controls by selecting this check box. The following priorities can be applied:<br><br>• **Low**<br>• **Medium**<br>• **High** |
| **GRC Designation** | You can categorize the controls according to the following criteria:<br><br>• **Regulation**<br>• **Legal Status**<br>• **Standards**<br>• **Threats** |
| **Type** | You can further categorize the controls according to the following criteria:<br><br>• **Management**<br>• **Technical**<br>• **Operations** |

| UI Element | Description |
|---|---|
| **Purpose** | Additional segmentation according to purpose:<br><br>● **Confidentiality**<br><br>● **Integrity**<br><br>● **Availability**<br><br>● **Audit**<br><br>● **Privacy** |
| **Control Weight** | You can apply a weight between 0 and 100 to a control. The control weight affects the aggregation calculation when the policy assessment score is trickled up. For more information, see "Weights and Criticality Level" on page 66.<br><br>If this check box is not selected, then all of the controls will have the same weight. |

## Content Tab

Use this screen to add content to a policy that you created.
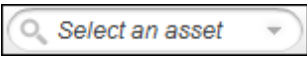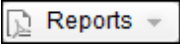
| UI Element | Description |
|---|---|
| ⊡ | **New Main Security Category**<br><br>A Security Category lets you group controls with common characteristics. Examples of security categories in ISO can be: Asset Management, Risk Assessment and Treatment, and Security Policy. Examples of security categories in COBIT can be: Plan and Organize, Acquire and Implement.<br><br>A Main Security Category is the first level in a policy; you cannot add controls to a policy without first defining their security category.<br><br>Click this button to create a new Main Security Category. In the right pane, enter the security category information. |
| ⊡ | **New Security Category**<br><br>A Security Category is optional. It can serve as a subcategory, depending on the format of the policy. You can create as many levels as required.<br><br>Click on the parent category (it may be a Main Security Category or a regular Security Category), and then click this button. In the right pane, enter the security category information. |

| UI Element | Description |
|---|---|
| | **New Control**<br><br>Controls are typically used to make sure that risks are reduced to an acceptable level. Controls are guidelines and rules and are the foundation of any policy; you must define controls in order to assess an asset's compliance with your organization's rules and regulations.<br><br>Click the security category to which the control belongs, and then click this button. In the right pane, enter the control information. |
| | **Delete**<br><br>Deletes a Main Security Category, Security Category, or Control. |
| | **Move Up**<br><br>Changes the order of any one of the following items in the policy tree:<br><br>● **Main Security Category** within a policy<br><br>● **Security Category** within a policy or within another security category<br><br>● **Control** within a security category. In order to move a control between security categories, you need to drag and drop the control. |
| | **Move Down**<br><br>See Move Up. |

# Policy Assessment Window

The Policy Assessment window enables you to audit assets by assessing the control maturity and asset compliance with a control, for each asset. The different areas and the functionalities available in each are described in the following sections.

## Left Pane

| UI Element | Description |
|---|---|
| Select an asset | Select the asset that you want to assess from this drop-down list or search for an asset by entering its name. |
| **Compliance/** **Maturity** tab | Displays information about the asset, for every policy element (controls and security categories). The **Compliance** tab displays compliance information and the **Maturity** tab displays control maturity information. |
| [icon] | Reflects the assessment progress in both **Compliance** and **Maturity** tabs. Provides a visual indication of how much each policy element is assessed. For the exact assessment percentage, hover over the relevant icon. For information on how assessment progress is calculated, see "Control Scores Aggregation Mechanism" on page 61. |
| **<Score Range>** | The score range for a specific policy element is indicated by one of the following icons: [icon] High score [icon] Medium score [icon] Low score The ranges are determined in "Configure Compliance and Maturity Score Ranges" on page 49. The actual score is displayed next to this icon. |
| Reports | **Generate Report** Click this button and select a report from the list of reports. If you are prompted, select to always allow pop-ups from the EnterpriseView server. You can save the report as a PDF or open it in a separate browser window. |
| [icon] | **Refresh** Refreshes the policy and its elements to display assessment changes. |

## Right Pane

### <Control Data>

Information on the control is displayed on each of the tabs.

| UI Element | Description |
|---|---|
| **Inherited from: <asset>** | Indicates from which higher level asset the applicability of this control was inherited. |
| **Maturity Score** | Measured as a score between 0 and 5. |
| | The evolutionary state of a control when it is applied to a specific asset, comprised by the weighted average of five factors: People, Procedure, Process, Product, Proof, also known in EnterpriseView as P5 maturity factors. For example, if the scores are: People=5, Procedure=5, Process=5, Product=3, and Proof=3, then the control maturity score is 4.2. |
| **Maturity Progress** | Measured as a percent. |
| | The maturity assessment progress reflects how many maturity factors have been assessed. Each maturity factor counts for a percentage of the overall score, depending on the number of maturity factors employed. For example, if all maturity factors are employed, then each factor counts for 20% of the overall score, so if two out of five maturity factors have been assessed, then the maturity assessment progress will be 40%. |
| | **Note:** If the control employs fewer than five factors, then the percentage distribution changes accordingly. |
| **Compliance Score** | see "Compliance Score" on next page. |
| **Compliance Progress** | Measured as a percent. |
| | The compliance assessment progress reflects the percentage of overall asset compliance with a policy. |
| **Control Mappings** | Indicates whether the control is mapped to other controls. Is displayed under the following conditions: |
| | • The assessed control is mapped to another control in a different policy. |
| | • The control to which it is mapped is applied to the same asset (SoA). |
| | You can click the "n controls" link to see the details of these controls. For more information on mapping controls between polices, see "Policy Mapping" on page 45. |

**Assessment Tab**
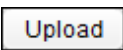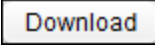
| UI Element | Description |
| --- | --- |
| **Compliance Score** | This number defines how compliant the asset is with the control.<br><br>Use the slider to select a score between 0 and 100. For more information, see "Audit Assets" on page 42.<br><br>When asset compliance is performed on lower level assets it is automatically trickled up and aggregated to higher level assets. You can override the aggregated score for a specific asset by changing it manually. |
| | **Applied Manually**<br><br>This icon indicates that a score was applied manually. It is applied only to the scores that have been changed. |
| | **Aggregated from Children**<br><br>This icon indicates that a score was aggregated from its lower level assets. |
| | **Automatic Assessment**<br><br>This icon indicates that a score was applied automatically by importing the assessment from an external system. It is applied only to the scores that have been changed. |
| **Ignore Vulnerabilities** | Select this check box if you want to disable the affect of vulnerabilities mapped to this control. For information on the correlation between vulnerabilities and controls, see "Using Vulnerabilities to Refine the Compliance Score" on page 35. |
| **Maturity Score** | For each maturity factor, drag the slider to assign a score between 0 and 5. For more information, see "P5 Control Maturity Model Guidelines" on page 60. |

| UI Element | Description |
|---|---|
| **Score is affected by <n> vulnerabilities** | This indication is displayed only if the vulnerabilities that are mapped to the control are also attached to the asset that is being assessed. Click the "n vulnerabilities" link to view information about these vulnerabilities. |
| | **Reduced by m%** |
| | This indication is displayed only if the assessment on the control was saved. |
| | The vulnerabilities reduce the compliance score. The reduction is expressed as a percent and is done automatically when you click **Save**. To override this effect, select the **Manual Assessment Only** check box, but note that selecting this check box also ignores imported automatic assessments. |
| | For more information on the correlation between vulnerabilities and controls, see "Using Vulnerabilities to Refine the Compliance Score" on page 35. |
| **Apply Aggregation** | If the source of some of the compliance or control maturity scores is from an automatic assessment or a manual assessment, click this button to clear the scores and perform score aggregation from lower-level assets. |
| **Last Updated On** | The last date and time that the control was assessed for the specific asset. |

**Details Tab**
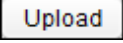
This tab displays information about the control, such as the control text and guidelines. For more information on control details, see "Content Tab" on page 53.

**Attachment Tab**

| UI Element | Description |
|---|---|
| Upload | Click this button to attach a file to this assessment. |
| | The maximum file size is 5.00 MB. |
| Delete | To delete a file from this control assessment, click the file that you want to delete, and then click this button. |
| Download | To download a file to your local computer, click the file that you want to download, and then click this button. |

**Notes Tab**

You can add comments and notes to the assessment.

In the text box, enter the required information, and then click Upload. The information is displayed in a table and includes the creation date and the user name. Click the ▶ icon next to the

date in order to view the entire note. You cannot delete or edit notes.

# P5 Control Maturity Model Guidelines

The P5 Model states that there are five basic factors to every control that must exist in order for that control to perform properly.

The following describes the factors of the P5 Model:

- **P1: People** Assigned staff to oversee and manage controls.

- **P2: Policy/Procedure** Governance documentation used to specify and manage control.

- **P3: Process** Operational sequence of activities designed to reduce risk.

- **P4: Product** Defense-in-depth technologies/solutions to manage/mitigate risk.

- **P5: Proof** Metrics or validation methods used to track control effectiveness.

| Key Performance Indicators | 0 Not Performed | 1 Performed Informally | 2 Planned and Tracked | 3 Well Defined | 4 Quantitatively Controlled | 5 Continuously Improving |
|---|---|---|---|---|---|---|
| P1: People | No personnel assigned to control | Part-time personnel assigned | Full-time personnel assigned | Formally trained personnel assigned | Certified personnel assigned | Back-up personnel assigned |
| P2: Policy & Procedure | No policy for control exists | Assumed policy, not documented or widely known | Formal published policy with acknowledgment | Policy applied to third parties | Policy actively enforced by HR department | Policy externally reviewed |
| P3: Process | No process for control exists | Assumed processes, not documented or widely known | Task list oriented processes | Detailed narrative-based descriptive processes | Processes include evidence of change control | Processes can be used by external personnel to perform control |
| P4: Product | No product for control exists | Default, open source or shareware solution deployed | Standardized point solution (tool) deployed, results monitored | Tool deployed with specific SLA and/or KPI targets tracked | Tool deployed with integrated management, logging and reporting | Multiple layer tools deployed, providing defense in-depth approach |
| P5: Proof | No proof for control exists | Subjective verbal attestation only | Subjective results; however, regularly reported in written format | Results automatically tracked and reviewed by internal audit | Results independently reviewed and/or validated by 3rd party | Formal independent attestations by TOD/TOE (SAS 70, SysTrust etc.) |

# Control Scores Aggregation Mechanism

In EnterpriseView, assessments that are done on lower-level assets, such as servers, are automatically trickled up to higher-level assets, such as a department; this mechanism is called aggregation.

Aggregation is performed on two different levels:

1. Aggregation on the business model level

   First, parent assets get the aggregated compliance score, control maturity score, compliance assessment progress and maturity assessment progress from their children, for each control. This is done for the entire business model hierarchy.

2. Aggregation on the policy level

   After aggregation is done on the business model level, security categories, main security categories and, lastly, the policy inherit the compliance score, control maturity score compliance assessment progress and maturity assessment progress from the controls. This is done separately for each asset in the entire policy hierarchy. If more than one policy is applied to the asset, then the asset receives the lowest compliance and maturity scores.

The following table includes a description of all assessment parameters.

| Parameter | Description |
|-----------|-------------|
| Compliance Score | Measured as a percent. <br><br> The compliance of an asset with a specific control. |
| Control Maturity Score | Measured as a score between 0-5. <br><br> The evolutionary state of a control when it is applied to a specific asset, comprised by the weighted average of five factors: People, Procedure, Process, Product, and Proof (also known in EnterpriseView as P5 maturity factors). For example, if the scores are: People=5, Procedure=5, Process=5, Product=3, and Proof=3, then the control maturity score is 4.2. |

| Parameter | Description |
|---|---|
| Maturity Assessment Progress | Measured as a percent. |
| | The maturity assessment progress reflects the percentage of the overall control maturity within a policy. |
| | Each maturity factor counts for a percentage of the overall score, depending on the number of maturity factors employed. For example, if all maturity factors are employed, then each factor counts for 20% of the overall score, and if out of the five maturity factors two have been assessed, then the maturity assessment progress will be 40%. |
| | **Note:** This parameter is significant only in policy-level aggregation. |
| Compliance Assessment Progress | Measured as a percent. |
| | The compliance assessment progress reflects the percentage of overall asset compliance with a policy. |
| | **Note:** This parameter is significant only in policy-level aggregation. |

**Note:** Any score, both compliance and control maturity factor, that has not yet been assessed (marked as Not Assessed), does not affect the aggregation calculation. For example, if the compliance of asset A is not assessed, but is assessed in asset B, then the parent asset inherits the compliance score of asset B.

# Aggregation on the Business Model Level

The following sections describe the aggregation mechanism for each of the parameters.

**Note:** Scores are aggregated from a child asset to a parent asset only for controls that are applied to both child and parent assets.

## Compliance Score

A parent asset gets the average compliance score of all its children, on a specific control.

$$\frac{\sum(Compliance\ Scores)}{\sum(Children)}$$

For example:

For control X

If

Compliance score for child asset A= **100%**

Compliance score for child asset B=**0%**

Then

Compliance score for parent asset=**50%**
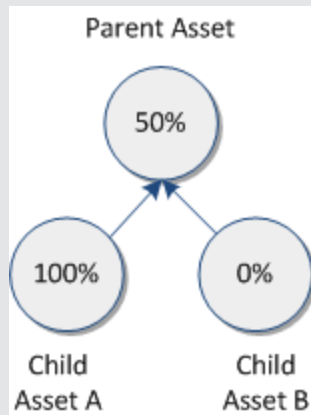


## Control Maturity Score

Aggregation is done in two steps:

1. A parent asset gets the average score for each P5 maturity factor of all its children.

2. The final control maturity score is the weighted average of the P5 maturity factor scores.

For example:

For control X

If

Child asset A has the following scores on its P5 maturity factors:

**People=5, Policy/Procedure=5, Process=5, Product=3, Proof=3**

Child asset B has the following scores on its P5 maturity factors:

**People=5, Policy/Procedure=4, Process=3, Product=3, Proof=5**

Then

The parent asset will inherit the following P5 maturity factor scores:

**People=5, Policy/Procedure=4.5, Process=4, Product=3, Proof=4**

and the overall control maturity score will be **4.1**

Parent Asset

4.1

4.2    4

Asset A
P1=5
P2=5
P3=5
P4=3
P5=3

Asset B
P1=5
P2=4
P3=3
P4=3
P5=5

Calculate P5 maturity
factors for parent asset:
P1: (5+5)/2=5
P2: (4+5)/2=4.5
P3: (5+3)/2=4
P4: (3+3)/2=3
P5: (3+5)/2=4
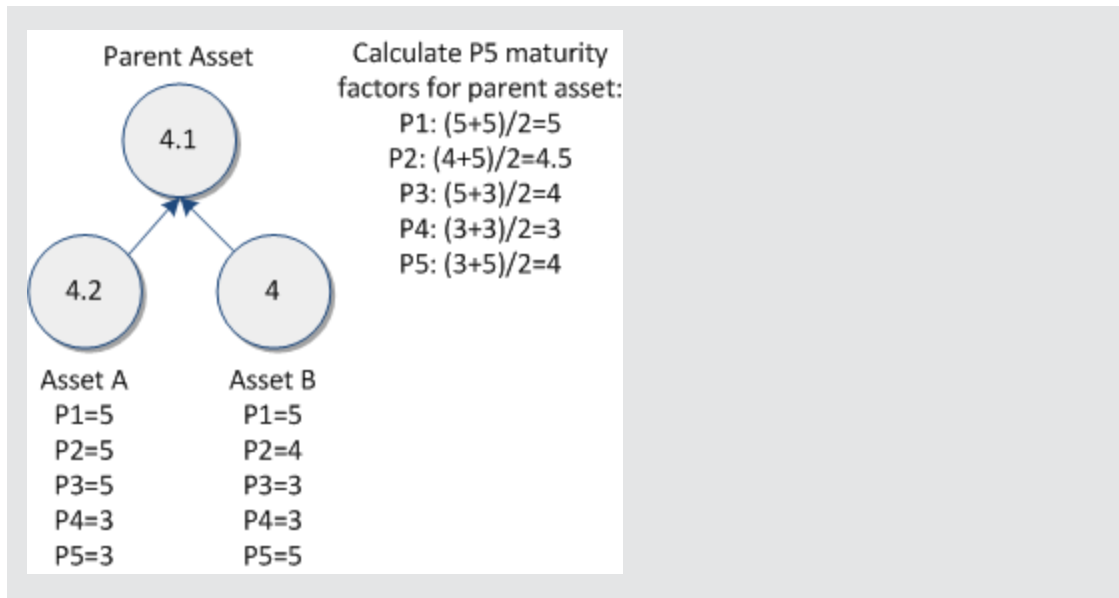
# Aggregation on Policy Level

The following diagram shows the flow of aggregation between policy elements:

Controls → Security Category → Main Security Category → Policy

Meaning:

1. The assessment parameters of all controls under a specific security category are aggregated to that security category.

2. The assessment parameters of all security categories under a specific main security category are aggregated to that main security category.

3. All assessment parameters for the main security categories are aggregated to the policy.

In the following examples, Policy A has the following format:

1 Main Security Category

1.1 Security Category

1.1.1 Control A

1.1.2 Control B

## Compliance Score

A policy element gets the average compliance score of all its contained elements, for a specific asset.

For example:

If

Compliance score for Control A (1.1.1)= **100**

Compliance score for Control B (1.1.2) =**0**

Then

Security Category (1.1), Main Security Category (1) and Policy A inherit the average score of **50**.

## Control Maturity Score

Aggregation is done in two steps:

1. A policy element gets the average score for each P5 maturity factor of all its contained policy elements.

2. The final control maturity score is the weighted average of the P5 maturity factor scores.

For example:

If

Control A (1.1.1) has the following scores on its P5 maturity factors:

**P1=5, P2=5, P3=5, P4=3, P5=3**

Control B (1.1.2) has the following scores on its P5 maturity factors:

**P1=5, P2=4, P3=3, P4=3, P5=5**

Then

Security Category (1.1), Main Security Category (1) and Policy A inherit a control maturity score of **4.1.**

**Note:** Some dashboards display the score on the P5 control maturity factor level. In this example, the following scores will be displayed:

**P1=5, P2=4.5, P3=4, P4=3, P5=4**

## Maturity/Compliance Assessment Progress

A policy element inherits the average maturity/compliance assessment progress of all its contained policy elements, on a specific asset.

For example:

If

Maturity assessment progress
for Control A (1.1.1) = **100%** (fully assessed)

Maturity assessment progress
for Control B (1.1.2)= **0%** (not assessed)

> Then
>
> Security Category (1.1), Main Security Category (1) and Policy A is **50%**

# Weights and Criticality Level

Aggregation of assessment scores is affected by the following factors:

- **Criticality Level**. One of the asset properties; it is determined when an asset is created in the business model, but can be modified at any time. For more information, see "Criticality Level" on page 25.The criticality level determines the weight of an asset's scores when it is aggregated on the business model level; it does not affect aggregation on the policy level.

> For example:
>
> If
>
> For child asset A: Compliance Score= **100**, Criticality Level=**1**
>
> For child asset B: Compliance Score =**10**, Criticality Level=**2**
>
> Then
>
> Compliance Score for parent asset=**40**
>
> Calculation: $\dfrac{(100 * 1) + (10 * 2)}{(1 + 2)}$

- **Control Weight**. One of the policy properties, configurable via the control template. It is determined when a control is defined in a policy. It can be modified until the assessment process on a policy begins. The control weight determines the weight of a specific control in regard to other controls within a specific policy when it is aggregated on the policy level; it does not affect aggregation on the business model level. For more information, see "Control Weight" on page 53.

> For example:
>
> If
>
> Compliance Score for Control A (1.1.1)= **10**, Control Weight=**100**
>
> Compliance Score for Control B (1.1.2) =**100**, Control Weight=**50**
>
> Then
>
> Security Category (1.1), Main Security Category (1) and Policy A inherit the weighted average score of **40**.
>
> Calculation: $\dfrac{(10 * 100) + (100 * 50)}{(100 + 50)}$

# Chapter 7

# Risk Modeling

Assessing risk is one of the ways that an organization identifies its security requirements. Risk assessment directly affects the business strategy and the objectives of the organization. Through a risk assessment, threats to assets are identified and the likelihood of occurrence is evaluated and potential impact is estimated.

EnterpriseView offers self-directed information security risk evaluation that enables organizations to make information protection decisions based on risks to their critical information technology assets.

The foundation of risk modeling is the Threat Library Builder component. The Threat Library Builder offers ready- to-use threats that are common to most organizations. Threats, made up of an initiator (referred to as Actor in EnterpriseView) and the threatening incident (referred to as Operation in EnterpriseView), can be added, modified or deleted, according to the requirements of the organization. An actor can be anything from a hacker to a technical failure and operations may range from natural disasters to malicious actions. EnterpriseView provides simple drag and drop capabilities to create threats, which are displayed as visual threat trees. For more information, see "Create a Threat Library" on page 71.

Risk acceptance levels are derived from the risk score ranges and probability ranges editable via the Threat Library Builder. Relative weights can be ascribed to the different actors or to actor categories, and to the various factors that are affected by the threat (financial, reputation, productivity, fines/legal, safety and health), known in EnterpriseView as impact areas. For more information, see "Configure Risk Assessment Settings" on page 78. EnterpriseView supports risk analysis and evaluation, by applying threats to assets, applying impact value, a qualitative value assigned to describe the extent of impact, to impact areas (low, medium, high) and defining the probability of the threat scenario occurrence. The inherent risk and residual risk scores are calculated from these parameters and are used as a prioritization mechanism designed to highlight risks for remediation. For more information, see "Assess Threat Scenario" on page 74.

Analyzed data is displayed in various dashboards,such as the "Risk Register" on page 96.

# Configure Risk Score Aggregation Method

Before you can begin working with the Risk Modeling module, you need to select a risk score aggregation method. For more information on the risk score aggregation methods and mechanism, see  the *Risk Score Aggregation Mechanism* section in the *HP EnterpriseView User Guide*.

### To configure risk score aggregation method

1.  Click **Administration > Configuration**.

2.  In the **Configuration** module, in the left pane, click the **Risk Aggregation Method** folder, and then click the **Risk Aggregation Method** page.

3. In the right pane, from the **Risk Aggregation Method** drop-down list, select an option:
   - **Average** (default)

   - **Override Children**

   - **Average of Children**

     For more information on the different methods, see "Risk Score Aggregation Mechanism" on page 90.

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

# Risk Mitigation with Policy Controls

There is an inherent correlation between policy controls and risks. A risk management plan should include the appropriate controls for mitigating risk, and, in turn, the process of assessing risk is one of the ways of identifying security requirements or controls.

EnterpriseView includes out-of-the-box mappings between policy controls and threats defined in the threat library.

These polices include:

- PCI DSS 2.0

- HIPAA Security Rule – NIST

- NIST Special Publication (SP) 800 53, Revision 3

- ISO 27002:2005

- UCF Q2 2012

These mappings represent the correlation between controls and risks. Controls automatically affect the probability of a threat scenario when the following conditions occur:

- The control is mapped to the threat

- The control is applied to an asset

- The threat is attached to an asset, creating a threat scenario

- The control has a compliance score resulting from a manual assessment, an automatic assessment, or affecting vulnerabilities

The probability of the risk is affected by the control's compliance score. The direction of the relationship (positive/negative) between the compliance score of the control and the probability of the risk depends on whether the compliance score is higher or lower than the threshold, which is 85:

- If the control's compliance score is higher than the threshold, then the compliance score reduces the probability of the risk

- If the control's compliance score is lower than the threshold, then the compliance score increases the probability of the risk

The formula that is used to determine the new probability depends on whether the compliance score is higher or lower than the threshold.

**If higher than the threshold**

$$NewTempProbability = ManuallySetProbability - \alpha * ManuallySetProbability * \frac{ControlScore - \beta}{100 - \beta}$$

**If lower than the threshold**

$$NewTempProbability = ManuallySetProbability + \alpha * ManuallySetProbability * \left(1 - \frac{ControlScore}{\beta}\right)$$

> **Note:** If the calculation result is higher than 1, then the NewTempProbability will be 1.

If there is more than one control mapped to the threat, the probability for each is calculated separately and then averaged to the final probability. The final probability is:

$$Final\,Probability = \frac{\sum NewTempProbability}{Number\,of\,Controls}$$

You can search for specific mappings by using free text search. To access the **Control to Threat Mapping** window, click **Risk Modeling > Control to Threat Mapping**.

You can add new mappings or edit existing mappings. For more information, see "Map Controls to Threats" below and "Edit Control to Threat Mapping" below.

# Map Controls to Threats

You can add new control to threat mappings.

### To map controls to threats

1. Click **Risk Modeling** > **Control to Threat Mapping**.

2. On the **Control to Threat Mapping** page, click **Add Mapping**.

3. On the **Select a Threat** page, expand the tree and select an operation.

4. On the **Select Controls for Mapping** page, from the **Policy** list, select a policy.

5. From the list of controls, select the controls that you want to map to the threat, and then click the **Add to Mapping** [ > ] button.

   To remove controls from the mapping, click the **Remove from Mapping** [ < ] button.

6. Click **Finish**.

# Edit Control to Threat Mapping

You can edit existing control to threat mappings.

### To edit a mapping

1. Click **Risk Modeling** > **Control to Threat Mapping**.

2. On the **Control to Threat Mapping** page, select the mapping that you want to edit, and then click **Edit Mapping**.

You can search for specific mappings by using free text search.

> **Note:** You can perform wildcard searches. For example, if you type **ser***, the results will contain words beginning with ser (such as server and service). An asterisks cannot be placed before a string (*ser).

3.  To add controls, do the following:

    a.  On the **Edit Mapping** dialog box, click **Add Controls**.

    b.  From the policy list, select a policy.

    c.  From the list of controls, select the controls that you want to map to the threat, and then click the **Add to Mapping** ⟩ button.

    d.  To remove controls from the mapping, click the **Remove from Mapping** ⟨ button.

4.  To remove controls, On the **Edit Mapping** dialog box, from the list of controls, select the control that you want to remove, and then click the **Remove from Mapping** ✕ button.

5.  Click **Finish**.

# Delete Control to Threat Mapping

You can delete both user-created and out-of-the-box mappings.

> **Note:** If you delete a mapping then any affect that control has on a threat scenario is eliminated.

## To delete a mapping

1.  Click **Risk Modeling** > **Control to Threat Mapping**.

2.  On the **Control to Threat Mapping** page, select the mapping that you want to delete, and then click the **Delete Mapping** ✕ button.

    You can search for specific mappings using free text.

3.  Click **Yes** to confirm the action.

# Create a Threat Library

A threat is a potential cause of an unwanted incident which may result in harm to the organization. For example, someone could initiate a denial-of-service attack against an organization's mail server, or a fire or natural disaster could damage an organization's IT hardware. A threat is created when a threat actor exploits a vulnerability.

In EnterpriseView, threats consist of an actor and an operation. The Threat Library Builder offers ready- to-use threats that are common to most organizations. You can add, modify, or delete threats, operations, and actors according to the requirements of your organization. For more information on maintaining threats, actors and operations, see "Threat Library Builder Window" on page 82.

**To create a new threat**

1. If the actor required for this threat does not exist in the threat library, follow the instructions in "Create an Actor" below.

2. If the operation required for this threat does not exist in the threat library, follow the instructions in "Create an Operation" on next page.

3. Connect an actor to an operation, as described in "Connect Actor to Operation" on page 73.

# Create an Actor

An actor is a potential initiator of a violation of the security requirements (confidentiality, integrity, availability) of an asset in your organization.

Actors are divided into categories. EnterpriseView includes the following categories.

| Category | Description |
| --- | --- |
| End Users | This category represents threats to the asset that are caused by users authorized by the organization.<br><br>Threats in this category require direct action by a person and can be deliberate or accidental in nature. |
| External Users | This category represents threats to the asset that result from physical access to the asset.<br><br>Threats in this category require direct action by a person and can be deliberate or accidental in nature. |
| IT Users | This category represents threats to the asset via the organization's technical infrastructure.<br><br>Threats in this category require direct action by a person and can be deliberate or accidental in nature. |

| Category | Description |
|----------|-------------|
| Physical Threats | This category includes problems or situations that are outside the control of an organization. This category of threats includes natural disasters (such as floods or earthquakes) and interdependency risks. Interdependency risks include the unavailability of critical infrastructures (such as power supply). |
| Technical Failures | This category includes problems with an organization's information technology and systems. Examples include hardware defects, software defects, malicious code (such as viruses), and other system-related problems. |

You can create an actor under an existing category or create a new category.

### To create an actor

1. Click **Risk Modeling > Threat Library Builder**.

2. On the **Actors** tab, from the actor tree, click the category to which you want to add a new actor, and then click the **New Actor** button.

3. On the **Actors** dialog box, do the following, and then click **Save**:

    a. **Name**: Enter a unique name for the actor.

    b. **Description**: Enter a description for the actor, which will appear as a tooltip.

    The new actor is displayed in the actor tree.

### To create a new actor category

1. Click **Risk Modeling > Threat Library Builder**.

2. On the **Actors** tab, click the **New Category** button.

3. On the **New Category** dialog box, do the following, and then click **Save**:

    a. **Name**: Enter a unique name for the category.

    b. **Description**: Enter a description for the category, which will appear as a tooltip.

    The new category is displayed in the actor tree.

# Create an Operation

An operation is the violation of the security requirements of an asset performed by an actor.

EnterpriseView includes numerous predefined operations.

### To create an operation

1. Click **Risk Modeling > Threat Library Builder**.

2. On the **Operations** tab, click the **New Operation** button.

3. On the **Operations** dialog box,do the following, and then click **Save**.

   a. **Name**: Enter a unique name for the operation.

   b. **Description**: Enter a description. This description will appear as a tooltip for the operation.

   The new operation is displayed in the operations tree. Operations are sorted alphabetically.

# Connect Actor to Operation

You can create a threat by connecting an actor and an operation.

## To connect an actor and an operation

1. Click **Risk Modeling > Threat Library Builder**.

2. On the **Actors** tab, from the actors tree, locate the required actor. To expand the actors tree, click ▶ next to the category. Drag the actor to which you want to connect an operation to the map area. If the actor already has operations that are connected to it, they are displayed in the map area.

3. Click the **Operations** tab. From the list of operations, locate the operation that you want to attach to the actor, and drag it onto the actor icon in the map area.

   The operation is connected to the actor and is displayed in the **Operations** section in the map area.

4. To disconnect an operation from an actor, click the operation in the graph, and then press **DELETE**.

# Assess Threat Scenario

A threat scenario is a situation in which an asset can be compromised. It generally consists of a threat (an actor and an operation), and an asset. Threat scenarios provide a simple way to determine if a risk exists that could affect your asset. An asset can have many threats associated with it.

The following diagram shows an asset that has several threat scenarios.
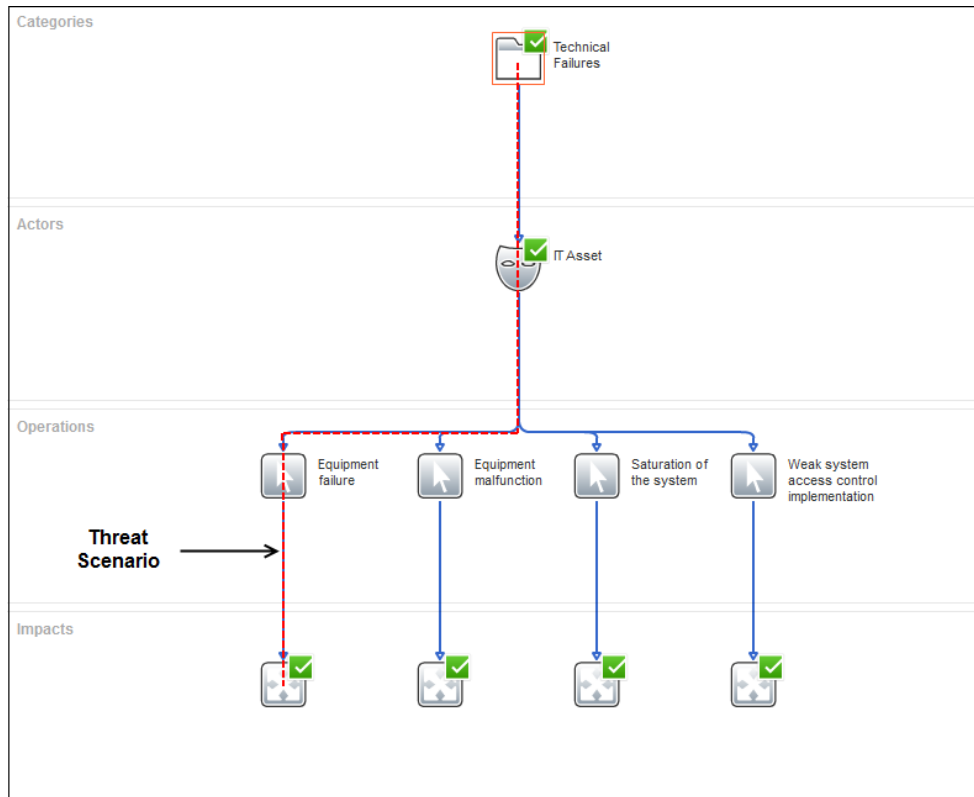


To create and assess a threat scenario, you must first "Assign Threat to Asset" below and then "Apply Risk to Asset" on page 76.

# Assign Threat to Asset

To create a threat scenario, connect a threat to an asset. You can connect threats to assets from both the **Graph** view and the **Table** view.

### To assign a threat to an asset (Graph view)

1. Click  **Risk Modeling > Assessment**.

2. On **Risk Modeling Assessment** window, from the **Asset** drop-down list, select the asset that

   you want to connect to the threat, and then click the Graph  button.

The left pane is divided into two areas:

- **Associated Threats** displays all the threats that are already associated with the asset

- **Unassociated Threats** displays all the threats that are not associated with the asset

All threats are grouped by actor and category.

3. To expand the threats tree, click ▶ next to the category/actor.

4. From the **Unassociated Threats** area, click the threat that you want to assign to the asset. You can also assign an entire group of threats, either grouped by actor or by category, by clicking the category or actor. To multi-select threats, press **CRTL** and click the threats you want to assign. Click the **Add threats to asset** ⬆ button or drag the threat to the map area.

   The threat is displayed in the **Associated Threats** area and in the map area.

5. To disconnect a threat from an asset, from the **Associated Threats** area, click the threat that you want to remove, and then click the **Remove the selected threat from the asset** ⬊ button.

   > **Caution:** If you disconnect a threat that has risk scores applied, then all the data on this threat is deleted and cannot be restored.

   The threat is displayed in the **Unassociated Threats** area and is removed from the map area.

   You can also drag and drop threats between the **Unassociated Threats** and **Associated Threats** areas.

## To assign a threat to an asset (Table view)

1. Click **Risk Modeling > Assessment**.

2. On the **Risk Modeling Assessment** window, from the **Asset** drop-down list, select the asset that you want to connect to the threat.

3. Click the **Table** 🗔 button.

4. From the **Show Threats** drop-down list, select **Unassociated to Asset** or **All Threats**.

5. From the table, select the **Associated** check box for all the relevant threats, and then click **Save**.

6. To disconnect a threat from an asset, from the **Show Threats** drop-down list, select **Associated to Asset** or **All Threats**, from the table, clear the **Associated** check box for all the relevant threats, and then click **Save**.

   > **Caution:** If you disconnect a threat that has risk scores applied, then all the data on this threat is deleted and cannot be restored.

# Apply Risk to Asset

EnterpriseView distinguishes between two types of risks:

- **Inherent Risk**

  The risk to an asset, for a specific threat scenario, in the absence of any actions you might take to alter either the likelihood or impact. The inherent risk is calculated as the weighted average of all impact area values.

- **Residual Risk**

  The risk that remains after you have attempted to mitigate the Inherent Risk. The Residual Risk is calculated as the Inherent Risk multiplied by the probability (Residual Risk = Inherent Risk X Probability).

Each of the threat elements (actor and operation) is applied with an inherent risk and a residual risk. Because the residual risk takes probability into account, it is considered to be the actual risk score. Assets can be part of many threat scenarios, therefore the risk score is applied on the threat scenario level and then aggregated to the asset. For more information on how the risk score is calculated, see "Residual Risk Score Calculation" on page 88.

In addition to the risk score, which is applied manually, each asset also has an Aggregated Risk Score, which is automatically trickled up from lower level assets. This score is not displayed in the Risk Modeling Assessment window, but is one of the parameters in various reports and dashboards, such as the "Risk Register" on page 96. For more information on the risk score aggregation mechanism, see "Risk Score Aggregation Mechanism" on page 90.

## To apply risk to an asset

1. Click **Risk Modeling > Assessment**.

2. On **Risk Modeling Assessment** window, from the **Asset** drop-down list, select the asset that you want to assess.

   All threats assigned to this asset are displayed in the left pane.

3. To display the threats that you want to assess, in the threats tree, click the **Show in graph** button. To expand the threats tree, click ▶ next to the category/actor.

4. In the map area, in the **Impacts** section at the bottom, click the impact icon.

   The risk **Properties** pane is displayed.

5. On the **Properties** pane, do the following:

   a. In the **Probability** box, enter a number between 0 and 1, up to two places after the decimal point. For example, 0.5.

   b. In the **Impact Areas** table, click inside the **Value** cell of each impact area and select **Low**, **Medium** or **High** to represent the impact of each area.

6. Click **Save**.

   The inherent risk and residual risk scores are applied to the operation, actor, and actor category and the residual risk is aggregated to the asset, as described in "Residual Risk Score Calculation" on page 88.

If there are assessed controls mapped to the threat, then the probability score is automatically recalculated to include the affect of the controls. For more information, see "Risk Mitigation with Policy Controls" on page 68.

The date and time of this assessment is updated in the **Last Updated On** field.

# Configure Risk Assessment Settings

You can configure weights of categories and actors and manage impact areas.

### To apply weights to categories and actors

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Risk Modeling > Actor Weights**.

3. On the **Actor Weights** page, locate the category/actor for which you want to change the weight. To expand the category and display actors, click [image] next to the category. Click the weight to make it editable.

4. Enter a weight between 0 and 100.

5. Click **Save**.

> **Note:** You can override these settings for a specific asset, as described in "Configure Asset Risk Settings" on page 80.

### To manage impact area settings

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Risk Modeling > Impact Area**.

3. Do one of the following:

   - To add an impact area, click the **Create new impact area** [image] button. In the **Name** cell, enter a name for the impact area. Click the weight to make it editable and enter a weight between 0 and 100.

   - To delete an impact area, click the **Delete impact area** [image] button.

     A confirmation message is displayed. Click **Yes** to confirm.

     > **Caution:** Deleting an impact area results in the reassessment of all assets.

   - To apply a weight to an impact area, click the weight to make it editable, and enter a weight between 0 and 100.

4. Click **Save**.

# Configure Risk Score Ranges

You can configure the ranges for the score severity indication for risk scores and threat probability.

Risk scores are displayed with one of the following icons:

☑ Low score

⚠ Medium score

❌ High score

This configuration is reflected throughout the application, wherever these measurements are displayed. For example, on the Risk Modeling Assessment page, wherever a residual or an inherent risk score is displayed.

## To configure risk score ranges

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Risk Modeling > Risk Score Ranges**.

3. Under **Risk Score Ranges**, drag the slider to define the inherent and residual score ranges.

4. Click **Save**.

## To define probability ranges

> **Note:** This range affects only the Risk Heat Map dashboard.

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Risk Modeling > Risk Score Ranges**.

3. Under **Probability Ranges**, drag the slider to define the probability ranges.

4. Click **Save**.

# Configure Asset Risk Settings

You can override the default weights applied to categories and actors for a specific asset.

## To override default weights for categories and actors

1. Click **Risk Modeling > Assessment**.

2. On the **Risk Modeling Assessment** window, click the **Asset Risk Settings** button.

3. On the **Asset Risk Settings** dialog box, locate the category/actor for which you want to change the weight. To expand the category and display actors, click ▶ next to the category. Click the weight to make it editable.

4. Enter a weight between 0 and 100.

5. Click **Save**.

# Configure Risk KPIs

The risk KPIs are used to determine how close or far the organization is from it's risk objectives. There are two KPIs:

- **Risk Score KPI**

  Indicates the percentage of assets, out of both direct and indirect children, with an aggregated risk score that is higher than a certain threshold. The higher the percentage the farther the organization is from its risk objectives.

  This KPI reflects the tolerance of your organization to risk. It is configurable and should be derived from your organization's strategic plans.

  The risk score KPI is displayed in the Risk Register page. For more information, see "Risk Register" on page 96.

- **Unassessed Risk KPI**

  Indicates the percentage of assets, out of both direct and indirect children, that have not been assessed. The higher the percentage the farther the organization is from its risk assessment objectives. This KPI reflects your organization's approach to the risk assessment process. It is configurable and should be derived from your organization's strategic plans.

  The risk score KPI is displayed in the Risk Modeling Dashboard page. For more information, see "Risk Modeling Dashboard" on page 102.

For more information on KPIs, see "Key Performance Indicators" on page 92.

## To configure risk score KPI

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Risk Modeling > Risk KPIs**.

3. On the **Risk KPIs** page, do the following:

    a. Under **Risk Score KPI - Threshold**, enter a number between 0 and 100, inclusive.

    b. Under **Risk Score KPI - Percentage Ranges**, drag the slider to the define the severity of the percentage ranges.

4. Click **Save**.

## To configure unassessed risk KPI

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Risk Modeling > Risk KPIs**.

3. On the **Risk KPIs** page, Under **Unassessed Risk KPI - Percentage Ranges** , drag the slider to the define the severity of the percentage ranges.

4. Click **Save**.

# Threat Library Builder Window

The Threat Library Builder enables you to create and manage threats and their building blocks (actors and operations). The different areas and the functionalities available in each are described in the following sections.

## Left Pane

| UI Element | Description |
| --- | --- |
|  | **Search**<br><br>Search for a category, actor, or operation. Enter a name, full or partial. All matches are displayed. |
| **Actors tab** | The Actors tab displays all of the actors that are defined in EnterpriseView in a tree view, grouped by categories. |
|  | **New Category**<br><br>Click this button to create a new actor category. For more information, see "Create an Actor" on page 71. |
|  | **New Actor**<br><br>Click this button to create a new actor. For more information, see "Create an Actor" on page 71. |
|  | **Delete** (category or actor)<br><br>Select the category or actor from the actor tree, and then click this button. Deleting a category automatically deletes all of its actors.<br><br>**Note:** Deleting an actor that is associated with a threat, automatically deletes the threat. Moreover, if the threat is already assessed, then the impact is also deleted. |
|  | **Edit** (category or actor)<br><br>Select the category or actor from the actor tree, and then click this button to edit the name and description of a category or an actor. |

| UI Element | Description |
|---|---|
| | **Copy** and **Paste** (actor)<br><br>You can duplicate actors using the copy/paste functionality.<br><br>Select an actor from the actor tree, and then click the **Copy** button. On the actor tree, click the category to which you want to copy the actor, and then click the **Paste** button. You can copy the actor under the same category. A new actor is created with the following name:<br><br>**Copy of <original actor name>**<br><br>You can rename the actor by clicking the **Edit** button.<br><br>If the actor is connected to operations, then associations are also copied. |
| | **Connect Actor to Operation**<br>Select an actor from the actors tree, click an operation on the graph, and then click this button.<br><br>This button is enabled only when the actor and operation are not yet connected. |
| **Operations tab** | The Operations tab displays a list of all the operations defined in EnterpriseView. |
| | **New Operation**<br><br>Click this button to create a new operation. For more information, see "Create an Operation" on page 72. |
| | **Edit Operation**<br><br>Select the operation from the operation list, and then click this button to edit the name and description of the operation. |
| | **Delete Operation**<br><br>Select the operation from the operation list, and then click this button.<br><br>**Note:** Deleting an operation that is associated with a threat, automatically deletes the threat. Moreover, if the threat is already assessed, then the impact is also deleted. |
| | **Connect Operation to Actor**<br><br>Select an operation or operations (press **CTRL** to multi-select) from the operations list, click the actor in the graph, and then click this button.<br><br>The operation/operations that you selected are connected to the actor and displayed in the map area. |

## Map Area

The map area displays a graphic depiction of the threats in the threats library. You can choose to display one threat or multiple threats.

- To display threats: On the **Actors** tab, open the category, select the actors that you want to display, and drag them to the map area.

- To display a category's actors and their connected operations: On the **Actors** tab, select the categories that you want to display and drag them to the map area.

- To disconnect an operation from an actor, in the map area, click the operation that you want to disconnect, and then press **DELETE**.

## Mini-map

When a threat includes multiple operations and is larger than the map area, you can navigate it by clicking and dragging in the Mini-map area.

To expand or collapse the mini-map, click the **Expand/Collapse**  button.

# Risk Modeling Assessment Window

The Risk Modeling Assessment window enables you to create threat scenarios and assess them. The different areas and the functionalities available in each are described in the following sections.

**Toolbar**

| UI Element | Description |
|---|---|
| 🔍 Select an asset ▾ | Select the asset that you want to assess from this drop-down list or search for an asset by entering its name. |
| 📊 | **Graph** (view) <br><br> In this view, the Risk Modeling Assessment window is divided into the following sections: <br><br> • Left pane <br><br> • Map area <br><br> • Properties pan <br><br> • Mini-map <br><br> This is the default view. |
| ▦ | **Table** (view) <br><br> In this view, all threats are displayed in a table. You can do the following: <br><br> • **Disconnect threats from an asset**. Clear the **Associated** check box. <br><br> • **Edit the threat description**. <br><br> • **Apply risk to an asset**. Edit the **Probability** and impact area fields. |
| 📄 Reports ▾ | **Generate Report** <br><br> Click this button and select a report from the list of reports. If you are prompted, select to always allow pop-ups from the EnterpriseView server. You can save the report as a PDF or open it in a separate browser window. |
| 📋 | **Asset Risk Settings** <br><br> Override the default weights applied to categories and actors for a specific asset. |

## Left Pane

The left pane is divided into two areas:

- **Associated Threats**: The top area displays all the threats that are associated with the asset.

- **Unassociated Threats**: The bottom area displays all the threats that are not associated with the asset.

| UI Element | Description |
|---|---|
| **<Threats tree>** | The threats tree displays all of the actors and their associated operations, grouped by category. The category is the first level, the actor is the second level, and its associated operations is the third level, displayed in alphabetical order. |
| | **Assign Threats to Asset** |
| | From the **Unassociated Threats** area, select the threats that you want to assign to an asset, and then click this button. |
| | The threat scenario is displayed in the map area. For more information, see "Assign Threat to Asset" on page 74. |
| | **Remove the selected threat from the asset** |
| | From the **Associated Threats** area, select the threats that you want to remove from the asset, and then click this button. |
| | The threat scenario is removed from the graph area. For more information, see "Assign Threat to Asset" on page 74. |

## Graph Area

The graph area displays the following information:

- **Asset**: Appears in the upper left side.

- **Residual risk score**: The aggregated residual risk score of all of the asset's threats, displays on the upper right side.

- **Threat scenario graph**: Displays (from top to bottom) the category, actor, operation, and impact elements. Clicking the graph entity displays its properties in the Properties pane on the right.

## Properties Pane

| UI Element | Description |
|---|---|
| **Category Properties** | Includes the name and description of the threat category, in addition to the residual risk score for this specific threat. |
| **Actor Properties** | Includes the name and description of the threat actor, as well as the residual risk score for this specific threat. |
| **Operation Properties** | Includes the name and description of the threat operation. |

| UI Element | Description |
|---|---|
| **Impact Properties** | The impact represents the threat scenario. |
| | • **Description**: You can document the assessment process by adding notes and comments in this text box. |
| | • **Impact Areas**: This table displays all of the impact areas and the weight that each impact area carries. To assign an impact area value, click in the **Value** cell and select **Low**, **Medium**, or **High**. |
| | • **Inherent Score**: The inherent risk score is the risk to an asset in the absence of any actions you might take to alter either the likelihood or impact. The inherent risk is calculated as the weighted average of all impact area values. |
| | • **Probability**: The probability that this threat will occur. Enter a number between zero and one. |
| | • **Residual Score**: The residual risk score is the vulnerability or exposure of the asset; in other words, the risk that remains after you have attempted to mitigate the Inherent Risk. The Residual Risk is calculates as the Inherent Risk multiplied by the probability (Residual Risk = Inherent Risk X Probability). |
| | • **This threat is affected by <n> controls.** |
| | This indication is displayed only if the controls that are mapped to the threat are also attached to the asset that is being assessed. Click the "n controls" link to view information about these controls. |
| | **The probability is reduced/increased by m%.** |
| | This indication is displayed only if the assessment was saved. |
| | • **Last Updated On**: The last date and time on which this threat was assessed. |
| | • ➡ **Next Threat** ⬅ **Previous Threat**: Enabled when more than one threat is displayed in the graph area. Enables you to navigate between threat scenarios and efficiently assess risk. |

## Mini-map

When a threat includes multiple operations and is larger than the map area, you can navigate it by clicking and dragging in the Mini-map area.

# Residual Risk Score Calculation

The residual risk  that is applied to a threat scenario is also calculated and applied separately on the actor, actor category, and asset. For more information on residual risk, see "Residual Risk " on page 76.

The parameters used to calculate risk score and their values are:

- **Impact Area Weight**:  Between 0 and 100. Defined in Settings, as described in "Configure Risk Assessment Settings" on page 78.

- **Impact Area Value**:  **Low**=1, **Medium**=2, **High**=3.

- **Weight**: of actor or category, between 0 and 100. Defined in Settings, as described in "Configure Risk Assessment Settings" on page 78.

- **Probability**: Between 0 and 1.

> **Note:** All scores are normalized to a value between 0 and 100.

The following table describes how the risk scores are calculated for each of these elements.

| Threat Element | Risk score calculation |
|---|---|
| **Threat Scenario** | The Inherent score is the weighted average of the impact areas multiplied by their values.<br><br>The residual score is the inherent score multiplied by probability*100.<br><br>$$\frac{\sum(\textit{Impact Area Value * Impact Area Weight})}{\sum(\textit{Impact Area Weights * 3})} * \left(\textit{Probability} * 100\right)$$ |

| Threat Element | Risk score calculation |
|---|---|
| **Actor** | The actor receives the score of the threat scenario (impact) with the highest risk.  |
| **Actor Category** | The weighted average of all actor scores.<br><br>$$\frac{\sum(\textit{Actor Score} * \textit{Actor Weight})}{\sum(\textit{Actor Weights})}$$ |
| **Asset** | The weighted average of all actor category scores.<br><br>$$\frac{\sum(\textit{Category Score} * \textit{Category Weight})}{\sum(\textit{Category Weights})}$$ |

# Risk Score Aggregation Mechanism

In EnterpriseView, there are two types of risk calculated for an asset:

- **Risk score**. The aggregated residual risk score of all of the threats applied to the asset. Risk scores are applied manually on each threat scenario. For more information on how this score is calculated, see "Residual Risk Score Calculation" on page 88.

- **Aggregated risk score**. Generally defined as the weighted average of aggregated risk scores of the asset's children, but is dependant on the calculation method selected, as described below. This score is applied to an asset automatically. It is not displayed in the Risk Modeling Assessment window, but is one of the parameters in various reports and dashboards, such as the Risk Register. For more information, see "Risk Register" on page 96.

Three methods are available for calculating the aggregated risk score:

> **Note:** If an asset does not have children, then the risk score is used instead of the aggregated risk score.

- **Average**: The weighted average of aggregated risk scores of an asset's children including the risk score of asset itself. This is the default method. The asset's risk score and the aggregated risk score of its children is taken into account.

$$\frac{\sum(Aggregated\ Risk\ Score\ Children * Criticality Level) + Asset\ Risk\ Score * Criticality Level}{\sum(Criticality Level)}$$

- **Override Children**: If the asset already has a risk score, then its aggregated risk score receives the value of the risk score. If the asset does not have a risk score, then its aggregated risk score is calculated according to the Average formula. The asset's risk score takes precedence over its children's aggregated risk score.

Asset risk score or $\frac{\sum(Aggregated\ Risk\ Score\ Children * Criticality Level)}{\sum(Criticality Level)}$

- **Average of Children**: The weighted average of aggregated risk scores of an asset's children, excluding the risk score of the asset itself. The aggregated risk score children takes precedence over the asset's risk score.

$$\frac{\sum(Aggregated\ Risk\ Score\ Children * Criticality Level)}{\sum(Criticality Level)}$$

For instructions on how to configure the risk score aggregation method, see the *Configure Risk Score Aggregation Method* section in the *EnterpriseView Deployment Guide*.

# Chapter 8

# Dashboards and Reports

EnterpriseView comes with a variety of out-of-the-box dashboards and printable reports, based on common needs of specific IT and GRC roles, such as system administrators, auditors, and executives. EnterpriseView administrators can create customized role-based dashboards for different types of users, as described in the *Create a Customized Dashboards Page* in the *EnterpriseView Deployment Guide*. The dashboards can be created from predefined reports or from user-created reports.

There are two types of reports that you can create:

- **Printable**

  These reports are available from the Risk Modeling Assessment, Policy Assessment, Statement of Applicability, and the Vulnerability Management windows. From each window, only reports that are specific to that module are available. These reports are generated as print-friendly PDF documents by clicking the **Generate Report** Reports button. For more information on the reports included in EnterpriseView, see "Printable Reports" on page 139.

- **Dashboard**

  These reports are used as data analysis components and can be grouped together with other components in order to create comprehensive dashboards, such as the Risk Register, for the various roles. For more information, see "Risk Register" on page 96

You can create reports that belong to both categories. For more information on creating reports, see "Create an EnterpriseView Report Using SAP BusinessObjects Web Intelligence" on page 93.

# Root Cause Analysis

Root cause analysis (RCA) is a structured approach for identifying the underlying causes of problems or events. RCA is based on the assumption that problems should be solved by addressing their root causes rather than their obvious symptoms. You can use RCA to mitigate, eliminate, and prevent risk in your organization.

EnterpriseView dashboards support RCA. The dashboards include a drill-down functionality, strategically placed links, allowing you to trace root problems by navigating the various dashboards and EnterpriseView pages. In addition, the EnterpriseView Risk Indicators is an RCA tool that offers you the quickest way to identify risk sources in your organization's business model. It provides you with graphical risk indication on top of your business model map.

There are two main approaches for RCA in EnterpriseView:

- Identifying the underlying asset or assets that are responsible for increasing the overall risk in your organization.

  To follow this approach, you can track the source asset by drilling down in the business model.

> Example:
>
> a. Start by opening the **Risk Register** for your root asset.
>
> b. Identify the asset with the highest risk in the **First-Level Children Summary** component, and click its name.
>
>     The **Risk Register** is updated with information on the asset that you selected.
>
> c. Continue drilling down until you identify the underlying problematic asset.

- Identifying the risk element (vulnerability score, risk score, compliance score, maturity score, and ESM threat score) that is responsible for increasing the overall risk in an asset.

  To follow this approach, you can track the risk element by investigating it specifically.

> Example:
>
> a. Start by opening the **Risk Register** for your root asset.
>
> b. Identify the risk element that appears to be problematic the in the **Asset Summary**, and click its name.
>
>     EnterpriseView navigates to the dashboard that corresponds with the risk element that you chose. For example, if the problematic risk element is the vulnerability score, then when you click **Vulnerability**, the **Vulnerability Dashboard** opens.
>
> c. Continue drilling down until you identify the underlying problematic risk element.

Regardless of the approach you take, after you have identified the problematic asset or risk element, you can navigate to the relevant EnterpriseView page through which you can mitigate the problem.

> Example:
>
> 1. Identify an asset with a high aggregated asset vulnerability score in the **Risk Register**.
>
> 2. Click the **Aggregated Asset Vulnerability Score** label in the **Vulnerability Dashboard**.
>
>     The **Vulnerability Management** page opens with information about the specific asset.
>
> 3. Continue investigating the vulnerabilities using the tools available in the **Vulnerability Management** page. For example, you can filter vulnerabilities according to their score.
>
> 4. Handle the vulnerabilities attached to the asset to lower the asset vulnerability score.

# Key Performance Indicators

EnterpriseView includes key performance indicators (KPIs) that are used to measure the progression of your organization towards its objectives. In EnterpriseView, KPIs are used to monitor and improve upon the different aspects that comprise risk in your organization. EnterpriseView includes quantitative KPIs for risk elements, such as modeled risk, vulnerabilities, ESM threats, policy compliance, and control maturity.

Simple KPIs enable you to define the ranges for the score severity of various risk elements, according to your business needs. For example, asset vulnerability scores are displayed along with an icon that represents a low, medium or high score throughout the application. The color indication is also reflected in the trend charts and heat maps.

More complex KPIs include the percentage of assets with scores that are above or below a certain threshold. For example, the vulnerability KPI indicates the percentage of assets with an aggregated vulnerability score that is higher than a certain threshold. The higher the percentage the farther the organization is from its vulnerability objectives.

A KPI indicates the tolerance of your organization to risk elements. It is configurable and should be derived from your organization's strategy. KPIs are displayed for a specific asset.

All KPI score ranges and threshold parameters can be configured in Settings. For more information, see "Settings" on page 180.

# Create an EnterpriseView Report Using SAP BusinessObjects Web Intelligence

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

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

## General instructions for creating an EnterpriseView report in SAP BusinessObjects Web Intelligence

1. Select **EnterpriseView  Universe** when you create a new document. For detailed information on the classes and objects in the EnterpriseView Universe, see "EnterpriseView Universe" on page 113.

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.

3. The query that you created might be ambiguous. 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 SAP BusinessObjects Web Intelligence User Guide*. The EnterpriseView Universe includes predefined contexts. For information on the contexts, see "EnterpriseView Universe Query Contexts" on page 140.

4. Assign a category to the report when you export the document to the CMS. Select the categories that apply to the report (one or more):

   - EnterpriseView Categories > **Dashboard**

   - EnterpriseView Categories > Printouts > **Policy Assessment**

   - EnterpriseView Categories > Printouts > **Policy SoA**

   - EnterpriseView Categories > Printouts > **Risk Assessment**

   You can also assign a category to a report through SAP BusinessObjects Enterprise CMC.

> **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.

- 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.

## 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.

- 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.

The report that you created is automatically added to EnterpriseView. You can access printable
reports by clicking the **Create Report** ⌐ Reports ▾ button in one of the following windows:

- Risk Assessment

- Policy Assessment

- Statement of Applicability

- Vulnerability Management

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 *EnterpriseView Deployment Guide*.

# Risk Register

The EnterpriseView Risk Register is a comprehensive dashboard that provides you with all the risk-related information identified by your organization.

To open the Risk Register, click **Executive View > Risk Register**.

The Risk Register includes the following components:

- **Asset Selector**

  This component enables you to select the asset that you want to display in the Risk Register.

  The **Organization** tab displays the EnterpriseView business model. Expand the business model to select the asset that you want to display.

  The **Search** tab enables you to search for a name or a partial name of any asset connected to the business model.

  After you have selected the asset, you can collapse the **Asset Selector** by clicking the **Collapse** button. To expand the Asset Selector, click the **Expand Asset Selector** button.

  The asset that you selected is saved for when you next log on.

- **Asset Summary**

  This component displays the overall asset score, which is comprised of the following aggregated data:

  - **Risk**: The aggregated risk score of the asset. For more information on how this score is calculated, see "Risk Score Aggregation Mechanism" on page 90.

  - **Compliance**: The aggregated compliance score of the asset. For more information on how this score is calculated, see "Control Scores Aggregation Mechanism" on page 61.

  - **Maturity**: The aggregated control maturity score of the asset. For more information on how this score is calculated, see "Control Scores Aggregation Mechanism" on page 61.

  - **Vulnerability**: The aggregated asset vulnerability score of the asset. For more information on how this score is calculated, see "Asset Vulnerability Score Aggregation Mechanism" on page 156.

  - **ESM Threat**: The aggregated ESM threat score of the asset. This score is calculated as the highest score out of all the asset's children and the asset itself.

    For more information on how the ESM threat score is calculated, see the *Apply Weighting Scheme to Priority Factors* section in the *HP EnterpriseView Deployment Guide*.

  The following formula is used for calculating the asset overall score:

$$\frac{Risk * weight + (100 - Maturity * 20) * weight + (100 - Compliance) * weight + ESM * 10 * weight + Vulnerabilty * 10 * weight}{\sum weights}$$

> **Note:** You can edit the weights of these scores in **Settings > Asset Overall Score**

> **Formula**. For more information, see "Configure Asset Overall Score Formula" on page 182.

To analyze the scores, click on the label of the score that you want to analyze. You will be redirected to the corresponding page:

- Risk: Risk Modeling Dashboard

- Compliance: Compliance Dashboard

- Maturity: Compliance Dashboard

- Vulnerability: Vulnerability Dashboard

- ESM Threat: ESM Threat View

- **First-Level Children Summary**

This component displays the information provided in the **Asset Summary** for the highest risk, first level children of the asset that you selected (up to five are displayed).

To analyze a specific child asset, click the asset in the **Asset Name** column. The page is reloaded with information on the asset that you chose.

- **Asset Overall Score Over Time**

This component displays the asset overall score over time. Asset overall scores are archived on a weekly basis. These scores, as well as the most updated score, are displayed in a graph in order to reveal trends in the overall score. If you hover over the round icons in the graph, you can see the exact score and the date on which it was calculated.

- **Risk Score KPI**

This component displays a Key Performance Indicator (KPI) that indicates the percentage of assets, out of both direct and indirect children, with an aggregated risk score that is higher than the KPI threshold. The higher the percentage the farther the organization is from its business objectives.

The KPI threshold is dynamic and is displayed in this component below the gauge. It is defined in Settings, along with the percentage ranges for the severity color indication, as described in "Configure Risk KPIs" on page 80.

- **Vulnerability Score KPI**

This component displays a KPI that indicates the percentage of assets, out of both direct and indirect children, with an aggregated vulnerability score that is higher than the KPI threshold. The higher the percentage the farther the organization is from its business objectives.

The KPI threshold is dynamic and is displayed in this component below the gauge. It is defined in Settings, along with the percentage ranges for the severity color indication, as described in "Configure Vulnerability KPI" on page 149.

- **Compliance Score KPI**

This component displays a KPI that indicates the percentage of assets, out of both direct and indirect children, with an aggregated compliance score that is lower than the KPI threshold. The higher the percentage the farther the organization is from its business objectives.

The KPI threshold is dynamic and is displayed in this component below the gauge. It is defined in Settings, along with the percentage ranges for the severity color indication, as described in "Configure Compliance KPI" on page 50.

- **ESM Threat Score KPI**

This component displays a KPI that indicates the percentage of assets, out of both direct and indirect children, with an aggregated ESM threat score that is higher than the KPI threshold. The higher the percentage the farther the organization is from its objectives.

The KPI threshold is dynamic and is displayed in this component below the gauge. It is defined in Settings, along with the percentage ranges for the severity color indication, as described in "Configure ESM Threat KPI" on page 184.

# Overall Score Heat Map

The Overall Score Heat Map enables you to view the overall score of Business and Location assets according to their criticality level.

To open the Overall Score Heat Map, click **Executive View > Overall Score Heat Map**.

The colors in the heat map reflect the severity of the scores, as follows:

- Low = green
- Medium = yellow
- High = red

The criticality level ranges are configurable. For more information, see "Configure Criticality Level Ranges" on page 183.

The overall score is comprised of the aggregated scores of the following: risk, compliance, control maturity, vulnerability, and ESM threat. For more information on the how this score is calculated, see "Configure Asset Overall Score Formula" on page 182.

The assets displayed in the graph are first and second level children of the asset that you select. If the asset that you select does not contain Business or Location assets, the graph remains empty.

The Overall Score Heat Map includes the following components:

- **Asset Selector**

  The **Organization** tab displays the EnterpriseView business model. Expand the business model to select the asset that you want to analyze.

  The **Search** tab enables you to search for a name or a partial name of any asset connected to the business model.

  After you have selected the asset, you can collapse the **Asset Selector** by clicking the **Collapse** [«] button. To expand the Asset Selector, click the **Expand Asset Selector** [»] button.

- **Overall Score Heat Map**

  The name of the asset that you selected is displayed above the graph along with its overall asset score and its criticality level, if it is defined.

  **Note:** Only assets that have been assessed are displayed on the graph.

  The assets that are displayed in the legend are sorted alphabetically and are numbered accordingly. Hover over the asset on the graph to display the name of the asset, the criticality level and the overall asset score. Click the icon of the asset in the graph to highlight the asset in the legend and vice versa. If two or more assets have the same criticality level and overall asset score, then they both appear as a single point on the graph and the icon is displayed with an ellipsis (...). Hover over the ellipsis icon to display information on all the assets that have the same overall asset score and criticality level.

# Risk Indicators

The Risk Indicators page is a root cause analysis tool that helps you identify risk sources in your organization's business model. It provides you with graphical risk indication on top of your business model map.

There are five quantitative factors that comprise the overall risk to your organization's assets. These factors include the policy compliance score, the control maturity score, the risk score, the asset vulnerability score, and the ESM threat score. These scores are formulated into the overall score of the asset.These factors, together with the asset overall score, are risk indicators. For more information on how the asset overall score is calculated, see "Configure Asset Overall Score Formula" on page 182.

You can select the risk indicator that you want to display on the business model map from the indicator menu. When you select an indicator from the indicator menu, information is updated in the business model map, in the asset card, and in the search pane. The name of the indicator that you selected appears at the top of the indicator menu. For example, if you chose the Overall indicator then the indicator menu appears as follows:
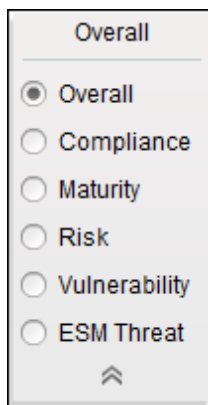


Every asset in the map has an icon that depicts the severity of the indicator score that you chose to display. The severity ranges for these scores are defined in Settings. For more information, see "Settings" on page 180. In the following example My organization has a low severity score.



If you click an asset in the map, the asset card opens displaying information on the asset,including the scores for all the indicators. For more information, see "Asset Card" on next page.

The Risk Indicators page includes the following areas:

- **Left Pane**

  - **Search**. You can search for a name or a partial name of any asset connected to the business model. You can also search by asset category or type by clicking **Advanced**. Click the **Show in Map**  button to display the asset in the business model map.

- **Toolbar**. The toolbar includes map-related actions that are similar to the Asset Profiling page, such as changing the map layout. All actions are view-only. For more information on these actions, see "Map Area" on page 27.

- **Map Area**

  The map area provides a graphical display of the business model. The indicator menu can be found in the upper right side of the map area. You can select a risk indicator to display in the business model map.

- **Asset Card**

  You can open the asset card by clicking on the asset in the business model map.

  Example:
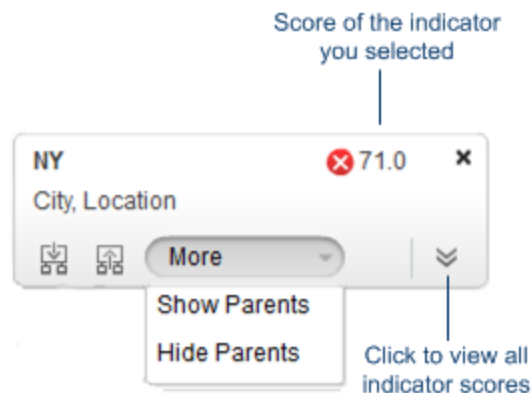


**Note:** The My Organization asset does not include the **Show Parents** and **Hide Parents** options because it is the root asset in the business model.

The following table includes the functionality available from the asset card.

| UI Element | Description |
|---|---|
| | **Expand** |
| | Show the direct children of the asset in the business model map. |
| | If the asset has more than 20 children, then the assets are not displayed automatically in order not to overload the business model. In this case, the **Show Children on Map for Asset** dialog box is displayed, enabling you to select the children you want to display. The number of direct children that an asset has is displayed in the business model map by the asset name. |
| | You can also expand by double-clicking the asset. |
| | **Collapse** |
| | Hide the direct children of the asset in the business model map. |
| | You can also collapse by double-clicking the asset. |

| UI Element | Description |
|---|---|
| **Show Parents** | Show the parent assets of the asset in the business model map. Click **More > Show Parents**. |
| **Hide Parents** | Hide the parent assets of the asset in the business model map. Click **More > Hide Parents**. |
| ⩒ | **Open Indicator Scores** Click to view all indicator scores. |
| ⩘ | **Close Indicator Scores** Close indicator scores. |

- **Mini-Map**

  When the business model is expanded to a larger size than the map area, you can navigate it by clicking and dragging in the mini-map area.

  To expand or collapse the mini-map, click the **Expand/Collapse** 🖥 button.

  High-risk assets that are displayed with a red severity indication in the map are also marked in red in the mini-map.

# Risk Modeling Dashboard

The Risk Modeling Dashboard is a comprehensive dashboard that provides you with general information on modeled risk for a specific asset.

To open the Risk Modeling Dashboard page, click **Risk Modeling > Risk Modeling Dashboard**.

Risk Modeling Dashboard includes the following components:

- **Asset Selector**

  The **Organization** tab displays the EnterpriseView business model. Expand the business model to select the asset that you want to analyze.

  The **Search** tab enables you to search for a name or a partial name of any asset in EnterpriseView, connected to the business model.

  After you have selected the asset, you can collapse the **Asset Selector** by clicking the

  **Collapse** ⪡ button. To expand the Asset Selector, click the **Expand Asset Selector** ⪢ button.

- **Risk Scores**

  This component displays the residual risk and aggregates risk scores for the asset that you have selected. For more information on how these scores are calculated, see "Residual Risk Score Calculation" on page 88 and "Risk Score Aggregation Mechanism" on page 90.

To analyze the residual risk, click on **Residual Risk**. The Risk Modeling Assessment page opens, displaying risk information for the asset that you have chosen.

- **First-Level Children Summary**

  This component displays the information provided in the **Risk Scores** component for the least compliant first-level children of the asset that you selected (up to five are displayed).

  To analyze a specific child asset, click the asset in the **Asset Name** column. The page is reloaded with information on the asset that you chose.

- **Children Risk Breakdown**

  This component displays the breakdown of risk severity (high, medium, low) of all the children of the asset that you selected, both direct and indirect. Only children that have a risk assessment are included in this breakdown.

- **Aggregated Risk Score Over Time**

  Asset aggregated risk scores are archived on a weekly basis. These scores, as well as the most updated score, are displayed in a graph in order to reveal trends in risk. Hover over the round icons in the graph to see the exact risk score and the date on which it was calculated.

- **Unassessed Risk KPI**

  A Key Performance Indicator (KPI) that indicates the percentage of business-critical assets (Business and Location assets), out of both direct and indirect children, that have not been assessed. The higher the percentage the farther the organization is from its objectives.

  The percentage ranges for the severity color indication is defined in Settings, as described in "Configure Risk KPIs" on page 80.

# Risk Scorecard and Heat Map

The Risk Scorecard and Heat Map includes information on risk assessment that is performed on a specific asset.

To open the Risk Scorecard and Heat Map page, click **Risk Modeling > Risk Scorecard and Heat Map**.

Risk Scorecard and Heat Map includes the following components:

- **Asset Selector**

  The **Organization** tab displays the EnterpriseView business model. Expand the business model to select the asset that you want to analyze.

  The **Search** tab enables you to search for a name or a partial name of any asset connected to the business model.

  After you have selected the asset, you can collapse the **Asset Selector** by clicking the **Collapse** ⟪ button. To expand the Asset Selector, click the **Expand Asset Selector** ⟫ button.

- **Risk Heat Map**

  The Risk Heat Map displays threat scenarios according to their inherent risk scores and probability. If the asset that you select does not have any threats attached to it, then the graph remains empty. The colors in the heat map reflect the severity of the scores.

  Hover over the threat on the graph to display the probability, inherent risk score, operation, and actor. Clicking the icon in the graph selects the threat in the legend and vice versa. If two or more threats have the same probability and inherent risk score, then they both appear as a single point on the graph and the icon is displayed with an ellipsis (…). Hover over this icon to display information on all the threats that have the same probability and inherent risk score.

- **Risk Scorecard**

  The Risk Scorecard table includes detailed information on the risk assessment of each threat attached to the asset that you have selected.

  The name of the asset that you selected is displayed above the table along with its residual score.

# Compliance Dashboard

The Compliance Dashboard is a comprehensive dashboard that provides you with general compliance information identified by your organization for a specific asset. If there is more than one policy that applies to the asset, then information is displayed for the least compliant policy (based on the aggregated compliance score on the policy level). For more in-depth information on compliance of a specific policy, see "Compliance by Policy Dashboard" on next page.

To open the Compliance Dashboard, click **Policy and Compliance > Compliance Dashboard**.

The Compliance Dashboard includes the following components:

- **Asset Selector**

  This component enables you to select an asset and display compliance information on that asset and its children.

  The **Organization** tab displays the EnterpriseView business model. Expand the business model to select the asset that you want to display.

  The **Search** tab enables you to search for a name or a partial name of any asset connected to the business model.

  After you have selected the asset, you can collapse the **Asset Selector** by clicking the **Collapse** ⟪ button. To expand the **Asset Selector**, click the **Expand Asset Selector** ⟫ button.

- **Compliance Summary**

  This component includes the aggregated compliance score and progress, in addition to the maturity assessment score and progress for the asset that you have selected. For more information on the aggregation mechanism, see "Control Scores Aggregation Mechanism" on page 61.

- **First-Level Children Summary**

  Displays the information provided in the **Compliance Summary** for the least compliant first level children of the asset that you selected (up to five are displayed).

  To analyze a specific child asset, click the asset in the **Asset Name** column. The page is reloaded with information on the asset that you chose.

- **Compliance Score Over Time**

  Asset compliance scores are archived on a weekly basis and when a clear assessment has been performed. These scores, as well as the most updated score, are displayed in a graph in order to reveal trends in compliance. If you hover over the round icons in the graph, you can see the exact compliance score, the assessment progress, and the date on which it was calculated. If the scores were archived due to a clear assessment, then the tooltip includes an "Audit Complete" indication.

- **Maturity Score Over Time**

  Control maturity scores are archived on a weekly basis and when a clear assessment has been performed. These scores are displayed in a graph in order to reveal trends in compliance. If you hover over the round icons in the graph, you can see the exact maturity score, the assessment

progress, and the date on which it was calculated. If the scores were archived due to a clear assessment, then the tooltip includes an "Audit Complete" indication.

- **Policy Compliance**

  Includes the aggregated score and assessment progress for both asset compliance and control maturity for each policy that is applied to the asset that you selected.

  To analyze a specific policy, click the policy in the **Policy Name** column. The **Compliance by Policy Dashboard** opens and displays information about the policy that you chose.

# Compliance by Policy Dashboard

The Compliance by Policy Dashboard is a comprehensive dashboard that provides you with all the compliance-related information identified by your organization for each policy associated with a specific asset.

To open the Compliance by Policy Dashboard, click **Policy and Compliance >  Compliance by Policy Dashboard**.

The Compliance by Policy Dashboard includes the following components:

- **Policy and Asset Selector**

  This component enables you to select an asset and one of the policies that applies to it and display compliance information on that asset and its children.

  You must first select a policy from the policy drop-down.

  The **Organization** tab displays the EnterpriseView business model. Expand the business model to select the asset that you want to display.

  The **Search** tab enables you to search for a name or a partial name of any asset connected to the business model.

  After you have selected the asset, you can collapse the **Policy and Asset Selector** by clicking the **Collapse** [«] button. To expand the Policy and Asset Selector, click the **Expand Policy and Asset Selector** [»] button.

- **Compliance Summary**

  This component includes the aggregated compliance score and progress,and the maturity assessment score and progress for the asset that you have selected, in relationship to the policy that you have selected.

  To analyze the policy assessment of specific asset, click **Compliance** or **Maturity**. The **Policy Assessment** page opens and displays information on the compliance assessment or maturity assessment of the asset that you selected.

  For more information on the aggregation mechanism, see "Control Scores Aggregation Mechanism" on page 61.

- **First-Level Children Summary**

Displays the information provided in the **Compliance Summary** for the least compliant first level children of the asset that you selected (up to five are displayed).

To analyze a specific child asset, click the asset in the **Asset Name** column. The page is reloaded with information on the asset that you chose.

- **P5 Score Breakdown**

A breakdown of the aggregated score of P5 control maturity factors of the asset and the policy that you selected.

- **Maturity Score Over Time**

Control maturity scores are archived on a weekly basis and when a clear assessment has been performed. These scores are displayed in a graph in order to reveal trends in compliance. If you hover over the round icons in the graph, you can see the exact maturity score, the assessment progress, and the date on which it was calculated. If the scores were archived due to a clear assessment, then the tooltip includes an "Audit Complete" indication.

- **Compliance Score Over Time**

Asset compliance scores are archived on a weekly basis and when a clear assessment has been performed. These scores, as well as the most updated score, are displayed in a graph in order to reveal trends in compliance. If you hover over the round icons in the graph, you can see the exact compliance score, the assessment progress, and the date on which it was calculated. If the scores were archived due to a clear assessment, then the tooltip includes an "Audit Complete" indication.

- **Score Details**

The aggregated maturity and compliance scores on the security category level. For more information on the aggregation mechanism, see "Control Scores Aggregation Mechanism" on page 61.

# Policy Compliance Map

The Policy Compliance Map enables you to view all of the policies and their security categories that are applied to a specific asset along with their assessment information, in a graphic view.

To open the Policy Compliance Map, click **Policy and Compliance > Compliance Map**. The different areas and the functionalities available in each are described in the following sections.

## Left Pane (Asset Selector)

| UI Element | Description |
|---|---|
| **Organization tab** | The Organization tab displays the EnterpriseView business model. Expand the business model and select the asset that you want to view. |
| **Search tab** | You can search for a name or a partial name of any asset connected to the business model. |

## Map Area

The Policy Compliance Map area has two tabs. The **Compliance** tab displays compliance assessment information and the **Maturity** tab displays control maturity information. Select that tab that has the information you require.

The policy and security categories are displayed according to their hierarchy, in a circular layout, each represented by an icon. Each icon includes the following information:

- Policy or security category name
- Control maturity/compliance score
- Assessment progress (provides a visual indication of how much the policy element is assessed)
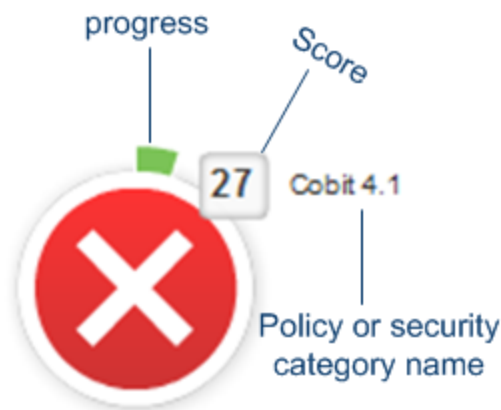
The graph area also includes the following functionality and information.

| UI Element | Description |
|---|---|
|  | **Optimize Layout**<br><br>Refreshes the layout of the business model in the graph. |
|  | **Fit to Window**<br><br>Resizes and displays the entire business model in the Graph Area. |
|  | Zoom in/zoom out business model. |
| **<Score Range>** | The score range for a specific policy element:<br><br>✅ High score<br><br>⚠️ Medium score<br><br>❌ Low score<br><br>The ranges are determined in "Configure Compliance and Maturity Score Ranges" on page 49 |

## Mini-map

When an asset has multiple policies/security categories applied to it and is larger than the map area, you can navigate it by clicking and dragging in the Mini-map area. To expand or collapse the mini-map, click the **Expand/Collapse**  button.

# Vulnerability Dashboard

The Vulnerability Dashboard provides you with an overview of your organization's vulnerability state for a specific asset and its children.

To open the Vulnerability Dashboard, click **Vulnerabilities > Vulnerability Dashboard**.

The Vulnerability Dashboard includes the following components:

- **Asset Selector**

  This component enables you to select the asset that you want to display in the Vulnerability Dashboard.

  The **Organization** tab displays the EnterpriseView business model. Expand the business model to select the asset that you want to display.

  The **Search** tab enables you to search for a name or a partial name of any asset in EnterpriseView, connected to the business model.

  After you have selected the asset, you can collapse the **Asset Selector** by clicking the **Collapse** button. To expand the Asset Selector, click the **Expand Asset Selector** button.

  **Vulnerability Summary**

  This component includes the aggregated asset vulnerability score for the asset that you selected. For more information on asset vulnerability score aggregation, see "Asset Vulnerability Score Aggregation Mechanism" on page 156.

  To analyze the aggregated asset vulnerability score, click the score. The Vulnerability Management page opens, displaying vulnerability information for the asset that you have chosen.

- **First-Level Children Summary**

  Displays the following information for the most vulnerable first level children of the asset that you selected (up to five are displayed):

  - Aggregated asset vulnerability score.

  - The number of open vulnerabilities and the percentage of open vulnerabilities that have not been handled yet, meaning, with a remediation status of New or Reopened.

  To analyze a specific child asset, click the asset in the **Asset Name** column. The page is reloaded with information on the asset that you chose.

- **Open Vulnerabilities Remediation Status**

  Displays a breakdown of all the open vulnerabilities that are attached to the asset that you have selected or to any of its children, according to their remediation status.

- **Vulnerabilities with the Highest Scores**

  Displays the vulnerabilities with the highest scores that affect the asset that you have selected, meaning that they are either attached directly to the asset or to the asset's children. Each record

represents a vulnerability (ID).

The **Assets Impacted** column displays the number of assets that this vulnerability (open or closed) affects, either by being directly attached to the asset or by being attached to a child asset. The percentage of open vulnerabilities is displayed in parenthesis.

- **Aggregated Vulnerability Score Over Time**

Aggregated vulnerability scores are archived on a weekly basis. These scores, as well as the most updated score, are displayed in a graph in order to reveal trends in vulnerability scores. If you hover over the round icons in the graph, you can see the exact vulnerability score and the date on which it was calculated.

- **Number of Open Vulnerabilities Over Time**

The number of open vulnerabilities are archived on a weekly basis. These scores, as well as the most updated score, are displayed in a graph in order to reveal trends in risk. If you hover over the round icons in the graph, you can see the exact risk score and the date on which it was calculated.

# ESM Threat View

EnterpriseView enables a periodic import of security threats from a Security Information and Event Management (SIEM) system, providing near real-time monitoring capabilities on the threats imposed on organization assets. For more information on the import process, see the *Import Security Threats from an SIEM System* section in the *EnterpriseView Deployment Guide*.

To open the ESM Threat View, click **ESM Threats > ESM Threat View**.

For each security threat, a score (1-10) depicts the threat level. This information is displayed graphically for individual or multiple assets. It enables you to identify security threat trends over selected time periods.

Two types of scores are calculated:

- **Asset ESM Threat Score**. The weighted average of a security event's priority factors, associated with an asset in a specific time range.

- **Aggregated Asset ESM Threat Score**. The highest Asset ESM Threat Score out of all the asset's children (indirect scores) and the asset itself (direct score).

The score displayed is the Aggregated Asset ESM Threat Score.

The ESM Threat View window includes the following areas:

## Left pane (Multi-asset Selector)

In this area you select the asset or assets for which you want to display threats. To select an asset, from the **Available Assets**, expand the business model tree, click an asset, and then click the **Add Asset** button. Repeat this for all the assets that you want to display. To remove an asset, from the **Selected Assets**, select the asset, and then click the **Remove Asset** button.

## Top pane (Threat Over Criticality)

Displays the asset on the graph according to its threat score and criticality. You can select one of the following time spans: last hour, last day, last 7 days, last 30 days, last year. The difference in the threat score between the current date and the time span that you select is reflected in the size of the asset icon that is displayed; a small icon reflects a small change in the threat score and a large icon reflects a big change in the threat score. Hover over the asset on the graph to display the name of the asset, the criticality level and the exact score for the current date and time, as well as the score for the time span that you selected.

## Bottom pane (Threat Over Time)

Displays a graph of the threat score for each asset that you selected for different time spans. You can select a time span: last hour, last day, last 7 days, last 30 days, last year. Hover over the graph curve to display the name of the asset, the exact threat score for the specific point on the graph, and the exact time that the threat score was imported into EnterpriseView.

# EnterpriseView Universe

In SAP BusinessObjects, a universe is an abstraction of a data source that contains data in non-technical terms with which users can create queries and run them against a database. These queries are then used to perform data analysis and create reports using entities in the universe called objects. For more information, see SAP BusinessObjects documentation. The EnterpriseView system includes an EnterpriseView universe that contains the classes and objects described in the following tables. You can use these objects to create a customized report, as described in "Create an EnterpriseView Report Using SAP BusinessObjects Web Intelligence" on page 93.

## Asset

An asset is an entity that represents a physical or logical resource in the system. For example, assets can represent hardware, software, services, or business units.

| Object | Description |
|---|---|
| Asset ID | The unique ID of the asset. |
| Asset Category | The category of the asset. Includes: Organization, Location, Business, IP, Infrastructure Elements, Running Software. For more information, see "Manage Asset Types" on page 17. |
| Asset Name | The name of the asset. |
| Asset Type | The asset type is a subset of the asset category. |
| Asset Description | Additional information on the asset. |
| Business Value | A numeric, monetary value. |
| Criticality Level | A numeric index, between 0 and 10, indicating the severity of a potential catastrophe and the probability of its occurrence. The default criticality level of all assets is 1. The criticality level of an asset affects the weight of its scores when policy assessment aggregation, risk aggregation and vulnerability score aggregation is done. For more information, see "Weights and Criticality Level" on page 66. |
| Latitude | Geographical coordinates of the asset's location. |
| Longitude | Geographical coordinates of the asset's location. |
| Address | Street address of the asset. |
| ZIP Code | Asset location ZIP code. |
| City | City of the asset. |
| State | State of the asset. |

| Object | Description |
|---|---|
| Country | Country of the asset. |
| OS Name | The operating system that is installed on the infrastructure element. |
| OS Version | The version of the operating system that is installed on the infrastructure element. |
| Application Name | The name of the application. |
| Application Version | The version of the application. |
| DNS Name | The server name as defined in the network DNS. |
| MAC Address | The server MAC address. |
| IP Address | The server IP address. |
| Role | The role of the person or the group in the organization. |
| Version | The version of the document. |
| Purpose | The purpose for which the document was created. |
| Classification | The type of document, such as legal or technical. |
| Release Date | The date on which the document was published. |
| Is Attached | Indicates whether the asset is attached to the business model. |

## Asset Source (subclass of Asset)

The origin of the asset.

| Object | Description |
|---|---|
| Source ID | The unique ID of the source. |
| Source Name | • If assets are created in EnterpriseView, then the source name is empty.<br><br>• If assets are imported from an external asset repository, then the source name is the same as the connector name defined in the **Configuration** module.<br><br>• For the Organization asset the source name is **System**. |
| External ID | The ID of the asset in the source (such as UCMDB and ArcSight ESM). |

## Overall Asset Score (subclass of Asset)

| Object | Description |
|---|---|
| Overall Asset Score | The overall asset score is comprised of the aggregated scores of the following: risk, compliance, control maturity, vulnerability, and ESM threat. <br><br> The following formula is used for calculating the overall asset score: <br><br> $$\frac{Risk * weight + (100 - Maturity * 20) * weight + (100 - Compliance) * weight + ESM * 10 * weight + Vulnerability * 10 * weight}{\sum weights}$$ |

## Risk Assessment (subclass of Asset)

The process of attaching threats to assets, evaluating the likelihood of their occurrence, and estimating the potential impact.

| Object | Description |
|---|---|
| Asset Risk Score | The aggregated residual risk score of all of the threats applied to the asset. |
| Asset Risk Score Severity | The severity level of the risk on an asset, expressed as one of the following values:  Low, Medium, or High. This value depends on the risk score ranges defined. |
| Aggregated Asset Risk Score | Generally defined as the weighted average of aggregated risk scores of the children of an asset, but depends on the calculation method configured. For more information, see "Risk Score Aggregation Mechanism" on page 90. |

## Associated Category (subclass of Risk Assessment)

An associated category is a category in a threat that is applied to an asset.

| Object | Description |
|---|---|
| Category ID | The unique ID of the category. |
| Category Weight | A numeric value between 0 and 100, associated with a specific asset. Is used when calculating the asset risk score. |
| Category Risk Score | The weighted average of all actor scores. <br><br> $$\frac{\sum(Actor\ Score\ *\ Actor\ Weight)}{\sum(Actor\ Weights)}$$ <br><br> For more information, see "Residual Risk Score Calculation" on page 88. |

## Associated Actor (subclass of Associated Category)

An associated actor is an actor in a threat that is applied to an asset.

An actor is a potential initiator of a violation of the security requirements (confidentiality, integrity, availability) of an asset in your organization.

| Object | Description |
|---|---|
| Actor ID | The unique ID of the actor. |
| Actor Weight | A numeric value between 0 and 100, associated with a specific asset. Is used when calculating the category risk score. |
| Actor Risk Score | The actor receives the score of the threat scenario (impact) with the highest risk.<br><br>For more information, see "Residual Risk Score Calculation" on page 88. |

### Impact (subclass of Associated Actor)

The element that represents the threat scenario.

| Object | Description |
|---|---|
| Operation ID | The unique ID of the operation. |
| Impact Description | Notes and comments used to document the risk assessment process. |
| Impact Inherent Score | The risk to an asset, for a specific threat scenario, in the absence of any actions you might take to alter either the likelihood or impact. The inherent risk is calculated as the weighted average of all impact area values. |
| Impact Residual Score | The risk that remains after you have attempted to mitigate the Inherent Risk. The Residual Risk is calculated as the Inherent Risk multiplied by the probability (*Residual Risk=Inherent Risk * Probability*). |
| Impact Probability | The probability that a threat will occur on a specific asset. A number between 0 and 1. |
| Last Updated | The last date and time on which the probability values, impact area values, or both were updated. |

### Impact Value (subclass of Impact)

An impact value can be **Low**, **Medium**, or **High**.

| Object | Description |
|---|---|
| Impact Area ID | The unique ID of the impact area. |
| Impact value | Low, Medium, or High |

### SoA (subclass of Asset)

The Statement of Applicability (SoA) identifies the controls chosen for the assets in the organization.

## Policy - SoA (subclass of SoA)

The policies that include controls are applied to an asset.

| Object | Description |
|--------|-------------|
| Policy ID | The unique ID of the policy. |

## Policy Security Category - SoA (subclass of Policy - SoA)

The policy security categories that include controls that are applied to an asset.

| Object | Description |
|--------|-------------|
| Policy Security Category ID | The unique ID of the policy security category. |
| Not Applied Controls Count | The number of controls for a specific security category that are not applied to an asset. |
| Applied Controls Count | The number of controls for a specific security category that are applied to an asset. |

## Control - SoA (subclass of Policy Security Category - SoA)

The controls that are applied to an asset.

| Object | Description |
|--------|-------------|
| Control ID | The unique ID of the control. |
| Is Control Applied | Indicates whether the control is applied to an asset. |
| Assignment Type | Indicates one of the following values for a control that is applied to an asset:<br><br>• **Inherited**: From a parent asset.<br><br>• **Inheritance Exception**: Control applicability has been overridden.<br><br>• **Applied Manually**: A regular control assignment. |

## Inherited From Asset (subclass of Control - SoA)

Controls that are inherited from a parent asset.

| Object | Description |
|--------|-------------|
| Asset ID | The unique ID of the parent asset. |
| Asset Category | The category of the parent asset. |
| Asset Name | The name of the parent asset. |
| Asset Type | The type of the parent asset. |

## Policy Assessment (subclass of Asset)

The process of assessing policy compliance and control maturity for all assets that comprise your organization's business model.

## Asset Scores (subclass of Policy Assessment)

Scores of assets that have been assessed.

| Object | Description |
|---|---|
| Compliance Score | Indicates how compliant the asset is with the control. Measured as a percent. |
| Compliance Progress | The percentage of overall asset compliance with a policy. |
| Maturity Score | The evolutionary state of a control when it is applied to a specific asset, comprised by the weighted average of five factors: People, Procedure, Process, Product, and Proof (also known in EnterpriseView as P5 maturity factors). |
| Maturity Progress | The percentage of the overall control maturity within a policy, for a specific asset. |

## Policy Scores (subclass of Asset Scores)

Scores of an asset that has been assessed for a specific policy.

| Object | Description |
|---|---|
| Policy ID | The unique ID of the policy. |
| Compliance Score | Indicates how compliant the asset is with the policy. Measured as a percent. |
| Compliance Score Severity | Low, Medium or High, depending on the score range, determined in Settings. |
| Compliance Progress | The percentage of overall asset compliance with a policy. |
| Maturity Score | The evolutionary state of a policy when it is applied to a specific asset, comprised by the weighted average of five factors: People, Procedure, Process, Product, and Proof (also known in EnterpriseView as P5 maturity factors). |
| Maturity Score Severity | Low, Medium or High, depending on the score range, determined in Settings. |
| Maturity Progress | The percentage of the overall control maturity within a policy, for a specific asset. |

## Policy P5 Scores (subclass of Policy Scores)

Assessment scores on specific control maturity factors aggregated to the policy.

| Object | Description |
| --- | --- |
| People Score | Maturity score for People factor. |
| Procedure Score | Maturity score for Procedure factor. |
| Process Score | Maturity score for Process factor. |
| Product Score | Maturity score for Product factor. |
| Proof Score | Maturity score for Proof factor. |

## Policy Security Category Scores (subclass of Policy Scores)

Scores of an asset that has been assessed for a specific security category.

| Object | Description |
| --- | --- |
| Policy Security Category ID | The unique ID of the policy security category. |
| Compliance Score | Indicates how compliant the asset is with the security category.<br><br>Measured as a percent. |
| Compliance Progress | The percentage of overall asset compliance with a policy. |
| Maturity Score | The evolutionary state of a control when it is applied to a specific asset, comprised by the weighted average of five factors: People, Procedure, Process, Product, and Proof (also known in EnterpriseView as P5 maturity factors). |
| Maturity Progress | The percentage of the overall control maturity within a policy, for a specific asset. |

## Policy Security Category P5 Scores (subclass of Policy Security Category Scores)

Assessment scores on specific control maturity factors aggregated to the security category.

| Object | Description |
| --- | --- |
| People Score | Maturity score for People factor. |
| Procedure Score | Maturity score for Procedure factor. |
| Process Score | Maturity score for Process factor. |
| Product Score | Maturity score for Product factor. |
| Proof Score | Maturity score for Proof factor. |

### Control Audit Data (subclass of Policy Security Category Scores)

Information on a specific assessment.

| Object | Description |
|---|---|
| Control ID | The unique ID of the control. |

### Control Notes (subclass of Control Audit Data)

| Object | Description |
|---|---|
| Note ID | The unique ID of the note. |
| Note Time | The date and time on which the note was created. |
| Note Text | Any type of additional information related to the assessment. |

### Control Scores (subclass of Control Audit Data)

Assessment scores on a specific control.

| Object | Description |
|---|---|
| Compliance Score | Indicates how compliant the asset is with the control. Measured as a percent. |
| Compliance Score Severity | Low, Medium or High, depending on the score range, determined in Settings. |
| Compliance Progress | The percentage of overall asset compliance with a policy. |
| Maturity Score | The evolutionary state of a control when it is applied to a specific asset, comprised by the weighted average of five factors: People, Procedure, Process, Product, and Proof (also known in EnterpriseView as P5 maturity factors). |
| Maturity Score Severity | Low, Medium or High, depending on the score range, determined in Settings. |
| Maturity Progress | The percentage of the overall control maturity within a policy, for a specific asset. |
| Compliance Applied Manually | Indicates that a score was applied manually. It is applied only to the specific scores that have been changed. |
| Last Updated | The last date and time on which the control compliance and/or maturity score was updated. |

### Control P5 Scores (subclass of Control Scores)

Assessment scores on specific control maturity factors.

| Object | Description |
|---|---|
| People Score | Maturity score for People factor. |
| People Applied Manually | Score for People factor applied manually. |
| Procedure Score | Maturity score for Procedure factor. |
| Procedure Applied Manually | Score for Procedure factor applied manually. |
| Process Score | Maturity score for Process factor. |
| Process Applied Manually | Score for Process factor applied manually. |
| Product Score | Maturity score for Product factor. |
| Product Applied Manually | Score for Product factor applied manually. |
| Proof Score | Maturity score for Proof factor. |
| Proof Applied Manually | Score for Proof factor applied manually. |

## Policy Compliance (subclass of Asset)

This class enables you to create a policy compliance report for assets on a policy that has not been directly assessed (Compliant Policy), but are mapped in EnterpriseView to a policy that has been assessed (Assessed Policy). For more information, see "Policy Mapping" on page 45.

| Object | Description |
|---|---|
| Assessed Policy ID | The unique ID of the assessed policy. |
| Assessed Policy Name | The unique name of the assessed policy. |
| Compliant Policy ID | The unique ID of the compliant policy. |
| Compliant Policy Name | The unique name of the compliant policy. |

## Mapped Controls (subclass of Policy Compliance)

This class includes information on mapped control parameters.

| Object | Description |
|---|---|
| Assessed Control ID | The unique ID of the assessed control. |
| Assessed Policy Security Category Paragraph Number | An alphanumeric string that indicates the paragraph number. |
| Assessed Policy Security Category Title | The title of the policy security category. |
| Compliant Control ID | The unique ID of the compliant control. |

| Object | Description |
|---|---|
| Compliant Policy Security Category Title | The title of the policy security category. |
| Compliant Policy Security Category Paragraph Number | An alphanumeric string. |
| Compliant Policy Security Category Order Key | Used to display the policy security categories according to their order in the policy. |

## Mapped Control Scores (subclass of Mapped Controls)

This class includes information on mapped control scores.

| Object | Description |
|---|---|
| Compliance Score | Indicates how compliant is the asset with the control. Measured as a percent. |
| Compliance Progress | The percentage of overall asset compliance with a policy. |
| Maturity Score | The evolutionary state of a control when it is applied to a specific asset, comprised by the weighted average of five factors: People, Procedure, Process, Product, and Proof (also known in EnterpriseView as P5 maturity factors). |
| Maturity Progress | The percentage of the overall control maturity within a policy, for a specific asset. |

## Mapped Control P5 Scores (subclass of Mapped Control Scores)

Assessment scores on specific control maturity factors that belong to a mapped control.

| Object | Description |
|---|---|
| People Score | The maturity score for People factor. |
| Procedure Score | The maturity score for Procedure factor. |
| Process Score | The maturity score for Process factor. |
| Product Score | The maturity score for Product factor. |
| Proof Score | The maturity score for Proof factor. |

## Asset ESM Threats (subclass of Asset)

A security event associated with a certain asset that poses a threat on that asset.

| Object | Description |
|---|---|
| Asset ESM Threat Score | The weighted average of a security event's priority factors, associated with an asset in a specific time range.<br><br>A numeric value between 0 and 10. |
| Aggregated Asset ESM Threat Score | The highest threat score out of all the asset's children (indirect scores) and the asset itself (direct score). |

## Asset Vulnerability (subclass of Asset)

This class includes different types of asset vulnerability scores.

| Object | Description |
|---|---|
| Asset Vulnerability Score | The highest score out of all the vulnerability scores of open vulnerabilities that are associated with the asset. |
| Aggregated Asset Vulnerability Score | The highest score of the following:<br><br>Asset vulnerability score<br><br>Or<br><br>$$m * \frac{\sum(Aggregated\ Asset\ Vulnerability\ Score\ *\ Criticality\ Level)\ of\ top\ \mathbf{n}\ Children}{\sum(Criticality\ Level)}$$<br><br>*m=Children Multiplier*<br><br>*n=Maximum Children in Calculation. Sorted primarily by aggregated asset vulnerability score and secondarily by criticality level.* |

## Asset Children

Use this class to create reports on an asset's children.

| Object | Description |
|---|---|
| Parent Asset ID | Parent asset unique ID. This asset is the starting point for the asset hierarchy. |

## Children (subclass of Asset Children)

Use this class to create reports on an asset's children.

| Object | Description |
|---|---|
| Child Asset ID | Child asset unique ID. |
| Hierarchy Level | The position of the asset in the hierarchical tree, in reference to the parent asset (Parent Asset ID object). |

## Archived Data (subclass of Asset)

This class includes information about scores that are archived in EnterpriseView. A dedicated job is

run periodically to extract and store a snapshot of these scores in the database. This data is used to create history and trend reports.

### Overall Score Archive (subclass of Archived Data)

This class includes archived data about the overall score of the asset.

| Object | Description |
|--------|-------------|
| Overall Score | The overall score of the asset. For more information on how this score is calculated, see "Configure Asset Overall Score Formula" on page 182 |
| Snapshot Time | The date and time that the overall score was archived. |

### Asset Vulnerability Archive (subclass of Archived Data)

This class includes archived data on asset vulnerabilities and aggregated asset vulnerability scores.

| Object | Description |
|--------|-------------|
| Aggregated Open Vulnerability Count | The number of all open vulnerabilities that are attached to an asset and its direct and indirect children. |
| Aggregated Asset Vulnerability Score | See "Aggregated Asset Vulnerability Score" on previous page. |
| Snapshot Time | The date and time that the aggregated asset vulnerability score was archived. |

### Risk Assessment Archive (subclass of Archived Data)

This class includes archived data on the risk score of an asset.

### Aggregated Score (subclass of Risk Assessment Archive)

This class includes archived data on the aggregated risk score of an asset.

| Object | Description |
|--------|-------------|
| Aggregated Asset Risk Score | See "Aggregated Asset Risk Score" on page 115. |
| Snapshot Time | The date and time that the aggregated risk score was archived. |

### Residual Score (subclass of Risk Assessment Archive)

This class includes archived data on the residual risk score of an asset.

| Object | Description |
|--------|-------------|
| Asset Risk Score | The aggregated residual risk score of all of the threats applied to the asset. |
| Snapshot Time | The date and time that the residual risk score was archived. |

### Policy Assessment Archive (subclass of Archived Data)

This class includes archived data on the maturity and compliance score of an asset.

### Asset Score Archive (subclass of Policy Assessment Archive)

This class includes archived data on the aggregated maturity and compliance score of an asset on the business model level.

| Object | Description |
| --- | --- |
| Snapshot Time | The date and time that the maturity and compliance data were archived. |
| Compliance Score | Indicates how compliant the asset is with the control. Measured as a percent. |
| Compliance Score Severity | Low, Medium or High, depending on the score range. |
| Compliance Progress | The percentage of overall asset compliance with a policy. |
| Maturity Score | The evolutionary state of a control when it is applied to a specific asset, comprised by the weighted average of five factors: People, Procedure, Process, Product, and Proof (also known in EnterpriseView as P5 maturity factors). |
| Maturity Score Severity | Low, Medium or High, depending on the score range. |
| Maturity Progress | The percentage of the overall control maturity within a policy, for a specific asset. |

### Policy Score Archive (subclass of Policy Assessment Archive)

This class includes archived data on the aggregated maturity and compliance score of an asset on the policy level.

| Object | Description |
| --- | --- |
| Snapshot Time | The date and time that the maturity and compliance data were archived. |
| Compliance Score | Indicates how compliant the asset is with the control. Measured as a percent. |
| Compliance Score Severity | Low, Medium or High, depending on the score range. |
| Compliance Progress | The percentage of overall asset compliance with a policy. |
| Maturity Score | The evolutionary state of a control when it is applied to a specific asset, comprised by the weighted average of five factors: People, Procedure, Process, Product, and Proof (also known in EnterpriseView as P5 maturity factors). |

| Object | Description |
|---|---|
| Maturity Score Severity | Low, Medium or High, depending on the score range. |
| Maturity Progress | The percentage of the overall control maturity within a policy, for a specific asset. |

### Policy P5 Score Archive (subclass of Policy Score Archive)

Aggregated assessment scores on specific control maturity factors.

| Object | Description |
|---|---|
| People Score | The aggregated maturity score for People factor. |
| Procedure Score | The aggregated maturity score for Procedure factor. |
| Process Score | The aggregated maturity score for Process factor. |
| Product Score | The aggregated maturity score for Product factor. |
| Proof Score | The aggregated maturity score for Proof factor. |

### Asset Profiling

This class includes information that is relevant to asset properties.

### Criticality Level Ranges (subclass of Asset profiling)

This class includes color indication for the criticality level ranges.

| Object | Description |
|---|---|
| Medium | Criticality level within a medium range is displayed in yellow. Score below the medium range is displayed in green. |
| High | Criticality level within the high range is displayed in red. |

### Policies

This class includes all the information that is relevant to active policies.

### General Policy Settings (subclass of Policies)

This class includes information on policy settings that is relevant to all policies.

### Maturity Score Range (subclass of General Policy Settings)

This class includes color indication for the maturity score ranges.

| Object | Description |
|---|---|
| Medium | Scores within a medium range are displayed in yellow. Scores below the medium range are displayed in green. |
| High | Scores within the high range are displayed in red. |

## Compliance Score Range (subclass of General Policy Settings)

This class includes color indication for the compliance score ranges.

| Object | Description |
|--------|-------------|
| Medium | Scores within a medium range are displayed in yellow. Scores below the medium range are displayed in green. |
| High | Scores within the high range are displayed in red. |

## Policy (subclass of Policies)

This class includes information that is specific to a policy.

A policy includes legal, statutory, regulatory, and contractual requirements to which the organization is bound.

| Object | Description |
|--------|-------------|
| Policy ID | The unique ID of the policy. |
| Policy Name | The name of the policy. |
| Policy Description | A description of the policy. |

## Policy Security Category (subclass of Policy)

A policy security category is group of controls with common characteristics.

| Object | Description |
|--------|-------------|
| Policy Security Category ID | The unique ID of the policy security category. |
| Policy Security Category Paragraph Number | An alphanumeric string. |
| Policy Security Category Title | The title of the policy security category. |
| Policy Security Category Text | Any additional text explaining the policy security category. |
| Policy Security Category Level | Policy security categories can be nested. This object indicates the level of the policy security category in the policy security category hierarchy. |
| Policy Security Category Order Key | Used to display the policy security categories according to their order in the policy. |
| Policy Security Category Controls Count | The number of controls under a specific policy security category. |

## Policy Security Category Hierarchy (subclass of Policy Security Category)

This class enables you to create a report for a specific security category and is generally used for

drill-down capability.

| Object | Description |
|---|---|
| Policy Security Category Parent ID | The ID of the security category that contains the policy elements that you want to display. |
| Policy Security Category Grandparent ID | The ID of the security category that contains the security category that contains the policy elements that you want to display. |
| Has Children | Indicates whether the policy element is the last level in the policy hierarchy. |

## Control (subclass of Policy Security Category)

Controls are the guidelines and rules that form the foundation of a policy.

| Object | Description |
|---|---|
| Control ID | The unique ID of the control. |
| Control Text | Control text. |
| Control Additional Information | Control additional information. |
| Guideline Introduction | Guideline introduction. |
| Guideline Additional Text | Guideline additional text. |
| Control Type | One of the following values: **Management**, **Technical**, or **Operations**. |
| Control GRC Designation | One of the following values: **Regulation**, **Legal Status**, **Standards** or **Threats**. |
| Control Purpose | One of the following values: **Confidentiality**, **Integrity**, **Availability**, **Audit**, or **Privacy**. |
| Control Weight | A numeric value between 0 and 100. The control weight affects the aggregation calculation on the policy level. For more information, see "Weights and Criticality Level" on page 66. |
| Control Priority | One of the following values: **Low**, **Medium**, or **High**. |
| People Applicable to Control | Indicates whether the People control maturity factor is applicable to a specific control. |
| Procedure Applicable to Control | Indicates whether the Procedure control maturity factor is applicable to a specific control. |
| Process Applicable to Control | Indicates whether the Process control maturity factor is applicable to a specific control. |

| Object | Description |
|--------|-------------|
| Product Applicable to Control | Indicates whether the Product control maturity factor is applicable to a specific control. |
| Proof Applicable to Control | Indicates whether the Proof control maturity factor is applicable to a specific control. |

### Control Guidelines (subclass of Control)

Guidelines or rules of the control.

| Object | Description |
|--------|-------------|
| Guideline ID | The unique ID of the guideline. |
| Guideline Text | Guideline text. |
| Guideline Order ID | Used to display the guidelines according to their order in the control. |

### Tag (subclass of Controls Guidelines)

Short descriptive texts that are applied to guidelines.

| Object | Description |
|--------|-------------|
| Tag ID | The unique ID of the tag. |
| Tag Name | The tag name. |

### Policy Settings (subclass of Policy)

Includes global policy settings.

### Control Template (subclass of Policy Settings)

This class enables you to create a report that displays only the objects that are in the control template.

| Object | Description |
|--------|-------------|
| Control Text in Template | Indicates whether this parameter is in the template. |
| Control Additional Information in Template | Indicates whether this parameter is in the template. |
| Guideline Introduction in Template | Indicates whether this parameter is in the template. |
| Guideline Additional Text in Template | Indicates whether this parameter is in the template. |
| Control Type in Template | Indicates whether this parameter is in the template. |

| Object | Description |
|---|---|
| Control GRC Designation in Template | Indicates whether this parameter is in the template. |
| Control Purpose in Template | Indicates whether this parameter is in the template. |
| Control Weight in Template | Indicates whether this parameter is in the template. |
| Control Priority in Template | Indicates whether this parameter is in the template. |
| People Weight | The weight applied to this maturity factor. |
| Procedure Weight | The weight applied to this maturity factor. |
| Process Weight | The weight applied to this maturity factor. |
| Product Weight | The weight applied to this maturity factor. |
| Proof Weight | The weight applied to this maturity factor. |

## Policy Mapping

This class enables you to create a report that displays mappings between policies.

| Object | Description |
|---|---|
| Source Policy ID | The unique ID of the source policy. |
| Source Policy Name | The name of the source policy. |
| Target Policy ID | The unique ID of the target policy. |
| Target Policy Name | The name of the target policy. |
| Is Target policy Active | Indicates whether the target policy is active in EnterpriseView. For more information, see "Activate a Policy" on page 38. |

## Policy Mapped Controls (subclass of Policies)

This class includes information on the mapped source and target controls.

| Object | Description |
|---|---|
| Source Control ID | The unique ID of the control in the source policy. |
| Source Policy Security Category Paragraph Number | The source policy security category paragraph number. |
| Source Policy Security Category Title | The source policy security category title. |
| Target Control ID | The unique ID of the control in the target policy. |
| Target Control Text | The control text in the target control. |

| Object | Description |
|---|---|
| Target Policy Security Category Paragraph Number | The target policy security category paragraph number. |
| Target Policy Security Category Title | The target policy security category title. |

## Vulnerability

A vulnerability is a flaw or a weakness in the software (in the network layer or the application layer) or a system configuration issue that can be exploited by an attacker and used to gain access to a system or a network.

| Object | Description |
|---|---|
| Vulnerability ID | The unique ID of the vulnerability. |
| Vulnerability Name | A descriptive name of the vulnerability. |
| Vulnerability Type | **Network** |
| Vulnerability Score | The severity level of the vulnerability expressed as a number (x.y) between 1 and 10. |
| Vulnerability Location | <hostname>:<port> |
| Vulnerability Number of Times Reported | The number of times that a specific vulnerability is reported from various sources. |
| Vulnerability First Reported On | The date and time of the first report of the vulnerability, as recorded by the external source from which the vulnerability was imported. |
| Vulnerability Last Reported On | The date and time of the last report of the vulnerability, as recorded by the external source from which the vulnerability was imported. |

### Vulnerability Unhandled Percentage Ranges (subclass of Vulnerability)

This class includes color indication for percentage ranges of vulnerabilities that have not been handled, meaning vulnerabilities with remediation status New and Reopened.

| Object | Description |
|---|---|
| Medium | A percentage within a medium range is displayed in yellow. A percentage below the medium range is displayed in green. |
| High | A percentage within the high range is displayed in red. |

### Vulnerability Statuses (subclass of Vulnerability)

This class includes the names and ID of all types of vulnerability statuses.

## Vulnerability Status (subclass of Vulnerability Statuses)

This class includes the names and ID for all vulnerability statuses.

| Object | Description |
|---|---|
| Vulnerability Status ID | The unique ID of the vulnerability status. |
| Vulnerability Status Name | Indicates the values **Open** or **Closed**. |

## Remediation Status (subclass of Vulnerability Statuses)

This class includes the names and ID for all remediation statuses.

| Object | Description |
|---|---|
| Vulnerability Remediation Status ID | The unique ID of the vulnerability remediation status. |
| Vulnerability Remediation Status Name | Indicates the values **New**, **Reopened**, **Assigned**, **Awaiting Remediation**, **Not an Issue**, **Awaiting Verification**, **Resolved**, or **Automatically Closed**. |

## Vulnerability Score Ranges (subclass of Vulnerability)

This class includes color indication for the vulnerability score ranges.

| Object | Description |
|---|---|
| Medium | Scores within a medium range are displayed in yellow. Scores below the medium range are displayed in green. |
| High | Scores within the high range are displayed in red. |

## Vulnerability Open Percentage Ranges (subclass of Vulnerability)

This class includes color indication for percentage ranges of vulnerabilities that have a status of Open.

| Object | Description |
|---|---|
| Medium | A percentage within a medium range is displayed in yellow. A percentage below the medium range is displayed in green. |
| High | A percentage within the high range is displayed in red. |

## Threat Library

The threat library includes predefined threats, common to most organizations, in addition to user-defined threats.

## Threat Library Settings (subclass of Threat Library)

This class includes information on threat library settings that are relevant to all threat scenarios.

## Probability Ranges (subclass of Threat Library Settings)

This class includes color indication for the probability ranges.

| Object | Description |
|--------|-------------|
| Medium | Scores within a medium range are displayed in yellow. Scores below the medium range are displayed in green. |
| High | Scores within the high range are displayed in red. |

## Risk Score Ranges (subclass of Threat Library Settings)

This class includes color indication for the risk score ranges.

| Object | Description |
|--------|-------------|
| Medium | Scores within a medium range are displayed in yellow. Scores below the medium range are displayed in green. |
| High | Scores within the high range are displayed in red. |

## Impact Area (subclass of Threat Library)

The area or areas in the organization that are affected by a threat on an asset.

| Object | Description |
|--------|-------------|
| Impact Area ID | The unique ID of the impact area. |
| Impact Area Name | The name of the impact area. |
| Impact Area Weight | A numeric value between 0 and 100. |

## Category (subclass of Threat Library)

The category of an actor.

| Object | Description |
|--------|-------------|
| Category ID | The unique ID of the category. |
| Category Default Weight | A numeric value between 0 and 100. The weight of a category defined on the threat library level. |
| Category Description | Category description. |
| Category Name | Category name. |

## Actor (subclass of Category)

An actor in the threat library.

An actor is a potential initiator of a violation of the security requirements (confidentiality, integrity, availability) of an asset in your organization.

| Object | Description |
|---|---|
| Actor ID | The unique ID of the actor. |
| Actor Default Weight | A numeric value between 0 and 100. The weight of an actor defined on the threat library level. |
| Actor Description | Actor description. |
| Actor Name | Actor name. |

## Operation (subclass of Actor)

An operation in the threat library.

An operation is the violation of the security requirements of an asset preformed by an actor.

| Object | Description |
|---|---|
| Operation ID | The unique ID of the operation. |
| Operation Description | Operation description. |
| Operation Name | Operation name. |

## Overall Score

This class includes overall score settings.

## Overall Score Ranges (subclass of Overall Score)

This class includes color indication for the overall score ranges.

| Object | Description |
|---|---|
| Medium | Scores within a medium range are displayed in yellow. Scores below the medium range are displayed in green. |
| High | Scores within the high range are displayed in red. |

## Overall Score Weights (subclass of Overall Score)

This class includes the weights for all the factors used to calculate the overall asset score. This value can be edited in the EnterpriseView universe.

| Object | Description |
|---|---|
| Risk Weight | The weight applied to an asset's aggregated risk score when calculating the asset's overall score. |
| Compliance Weight | The weight applied to an asset's aggregated compliance score when calculating the asset's overall score. |

| Object | Description |
|---|---|
| Maturity Weight | The weight applied to an asset's aggregated control maturity score when calculating the asset's overall score. |
| Vulnerability Weight | The weight applied to an asset's aggregated vulnerability score when calculating the asset's overall score. |
| ESM Weight | The weight applied to an asset's aggregated ESM threat score when calculating the asset's overall score. |

## ESM Threats

This class includes ESM threat settings.

## ESM Threat Score Ranges (subclass of ESM Threats)

This class includes color indication for the ESM threat score ranges.

| Object | Description |
|---|---|
| Medium | Scores within a medium range are displayed in yellow. Score below the medium range are displayed in green. |
| High | Scores within the high range are displayed in red. |

## KPIs

This class includes information about key performance indicators (KPIs).

## Risk Score KPI (subclass of KPIs)

This class includes the KPI parameter and indication, such as a different color for each range, for percentage ranges.

| Object | Description |
|---|---|
| Risk Score KPI Threshold | This threshold is used for measuring how many assets have a score that is higher or lower from it. This threshold is configured in Settings and is measured as a percent. |
| Medium | A percentage within a medium range is displayed in yellow. A percentage below the medium range is displayed in green. |
| High | A percentage within the high range is displayed in red. |

## Compliance Score KPI (subclass of KPIs)

This class includes the KPI parameter and indication, such as a different color for each range, for percentage ranges.

| Object | Description |
|---|---|
| Compliance Score KPI Threshold | This threshold is used for measuring how many assets have a compliance score that is higher or lower from it. This threshold is configured in Settings and is measured as a percent. |
| Medium | A percentage within a medium range is displayed in yellow. A percentage below the medium range is displayed in green. |
| High | A percentage within the high range is displayed in red. |

## Vulnerability Score KPI (subclass of KPIs)

This class includes the KPI parameter and indication, such as a different color for each range, for percentage ranges.

| Object | Description |
|---|---|
| Vulnerability Score KPI Threshold | This threshold is used for measuring how many assets have a vulnerability score that is higher or lower from it. This threshold is configured in Settings and is measured as a percent. |
| Medium | A percentage within a medium range is displayed in yellow. A percentage below the medium range is displayed in green. |
| High | A percentage within the high range is displayed in red. |

## ESM Threat Score KPI (subclass of KPIs)

This class includes the KPI parameter and indication, such as a different color for each range, for percentage ranges.

| Object | Description |
|---|---|
| ESM Threat Score KPI Threshold | This threshold is used for measuring how many assets have an ESM threat score that is higher or lower from it. This threshold is configured in Settings and is measured as a percent. |
| Medium | A percentage within a medium range is displayed in yellow. A percentage below the medium range is displayed in green. |
| High | A percentage within the high range is displayed in red. |

## Risk Assessment KPI (subclass of KPIs)

This class includes indication, such as a different color for each range, for the percentage ranges that are configured for KPI parameter: **No Risk Assessment KPI Threshold**.

| Object | Description |
|---|---|
| Medium | A percentage within a medium range is displayed in yellow. A percentage below the medium range is displayed in green. |
| High | A percentage within the high range is displayed in red. |

## Unhandled Vulnerabilities KPI (subclass of KPIs)

This class includes indication, such as a different color for each range, for the percentage ranges that are configured for KPI parameter: **Open Unhandled Vulnerabilities KPI Threshold**.

| Object | Description |
|--------|-------------|
| Medium | A percentage within a medium range is displayed in yellow. A percentage below the medium range is displayed in green. |
| High | A percentage within the high range is displayed in red. |

## Generic Prompts

This class can be used to easily create a query filter without inputting the prompt value.

| Object | Description |
|--------|-------------|
| @AssetPrompt | Can be used to create a query filter without the need to input the value "assetId". |
| @PolicyPrompt | Can be used to create a query filter without the need to input the value "policyId". |

## Generic Objects

This class includes miscellaneous classes and objects.

## Score Severity (subclass of Generic Objects)

This class includes the values for score severity.

| Object | Description |
|--------|-------------|
| Score Severity | Displays one of the following values: Low, Medium, or High. |

## Scores Rank (subclass of Generic Objects)

The objects in this class are used to rank asset scores using a weighted average in order to display "top #" assets in reports. The rank itself is not displayed in the report.

| Object | Description |
|--------|-------------|
| Asset Risk Score Rank | Used for ranking risk scores. |
| Aggregated Asset Risk Score Rank | Used for ranking aggregated risk scores. |
| Aggregated Asset Vulnerability Score Rank | Used for ranking aggregated vulnerability scores. |
| Asset Compliance Score Rank | Used for ranking compliance scores. |
| Asset Maturity Score Rank | Used for ranking P5 maturity factor scores. |

| Object | Description |
|---|---|
| Overall Asset Score Rank | Used for ranking the overall asset score. |
| Asset Vulnerability Score Rank | Used for ranking the direct asset vulnerability scores. |
| Vulnerability Score Rank | Used for ranking the vulnerability scores. |

## P5 Names (subclass of Generic Objects)

Use the objects in this class to return the names of the P5 maturity factors to be displayed in a report.

| Object | Description |
|---|---|
| People | Indicates that the maturity factor name "People" should be displayed in the report. |
| Procedure | Indicates that the maturity factor name "Procedure" should be displayed in the report. |
| Process | Indicates that the maturity factor name "Process" should be displayed in the report. |
| Product | Indicates that the maturity factor name "Product" should be displayed in the report. |
| Proof | Indicates that the maturity factor name "Proof" should be displayed in the report. |

# Printable Reports

Printable reports are available from the Risk Modeling Assessment, Policy Assessment, Statement of Applicability, and Vulnerability Management windows. From each window, only reports that are specific to that module are available. These reports are generated as print-friendly PDF documents by clicking the **Generate Report** [Reports ▾] button.

In addition to the various reports provided by EnterpriseView, you can create your own customized reports using SAP BusinessObjects Web Intelligence, as described in "Create an EnterpriseView Report Using SAP BusinessObjects Web Intelligence" on page 93.

The following table includes all of the out-of-the-box reports in EnterpriseView.

| Type | Report Name | Description |
|---|---|---|
| Risk Modeling | Risk Score Summary | This report includes the selected asset's risk score and aggregated risk score, as well as risk information for each threat imposed on a selected asset. |
| | Risk Score Details | This report includes risk score information on all actors and operations that comprise the threats that are posed on a selected asset, in conjunction with their name and description. |
| Statement of Applicability | Statement of Applicability Details | This report includes all the controls from policies that are applied to a selected asset and their details. |
| Policy Assessment | Policy Compliance Summary | This report includes compliance scores, control maturity scores and assessment progress information on controls, security categories the policy applied to a selected asset. |
| | Policy Compliance Details | This report includes compliance scores, control maturity scores and assessment progress information on all policy elements (security categories and controls) that are applied to a selected asset, in conjunction with the policy content. |
| Policy Builder | Activated Mapped Controls | This report includes mappings between a source policy and a target policy for all controls in policies that are activated, for a selected policy. |
| | Policy Details | This report includes the policy content for a selected policy. |
| Vulnerability | Open Vulnerabilities Summary | This report includes the vulnerability score and the number of locations that the vulnerability was found for all open vulnerabilities for a selected asset and all of its children. |
| | Open Vulnerability Details | This report includes the vulnerability score and the number of locations that the vulnerability was found, as well as information on each of the assets to which it is attached, for all open vulnerabilities for a selected asset and all of its children. |

# EnterpriseView 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 SAP 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. |
| 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 ESM Threat Context | Defines the group of objects with which you can create a report that provides ESM threat information on an asset. |
| Asset Scores Context | Defines the group of objects with which you can create a report that includes the various aggregated scores on an asset: compliance, maturity, risk, vulnerability, ESM threat, and the overall asset score. For example, the Policies Compliance dashboard report and the Policy Children Asset Summary dashboard report utilize the Asset Scores Context. |
| 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. |

| Context Name | Description |
|---|---|
| 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 aggregated scores. |
| Asset Risk Context | Defines the group of objects with which you can create a report on risk modeling assessments on an asset. |

# Chapter 9

# Vulnerability Management

In EnterpriseView, a vulnerability is a flaw or a weakness in a software application or a system configuration issue that can be exploited by an attacker and used to gain access to a system or a network or impact the confidentiality, integrity, and availability of a system or a network. For example, a user account that does not have a password, or an input validation error, such as SQL injection.

The Vulnerabilities module enables you to manage the life cycle of vulnerabilities in your organization including collection, aggregation, prioritization, and remediation. The Vulnerabilities module enables you to view vulnerabilities that affect an asset and its children in a summarized view or a detailed view. Both views offer filtering capabilities so that, for example, vulnerabilities can be viewed within a specific score range or a specific location.

EnterpriseView assigns vulnerabilities to specific assets in your business model. Vulnerabilities can be attached to assets or removed from assets manually. Asset vulnerability scores are derived from vulnerability scores (see "Common Vulnerability Scoring System" on page 144) and the asset's criticality level (see "Criticality Level" on page 25) and are trickled up and aggregated to top-level assets, providing business context to the state of your organization's security.

In addition, you can manage the vulnerability's life cycle by applying statuses aiding you in managing remediation.

EnterpriseView imports vulnerability information from vulnerability scanner output generated by the following vulnerability assessment tools:

- Tenable Nessus Vulnerability Scanner

- McAfee Vulnerability Manager (Foundscan)

- Qualys Guard

- HP Webinspect

The vulnerability information is imported into EnterpriseView using ArcSight SmartConnectors. For information on deploying ArcSight SmartConnectors, see the *Import Vulnerabilities From Vulnerability Assessment Tools* section in the *EnterpriseView Deployment Guide*.

EnterpriseView is CVE (Common Vulnerabilities and Exposures) compliant, aligned with most established dictionary of common names for publicly known information security vulnerabilities. However, EnterpriseView also supports management of vulnerabilities from sources that do not have a CVE classification.

The same vulnerability can be reported numerous times and by numerous vulnerability assessment tools. EnterpriseView aggregates these reports into a single vulnerability, in order to eliminate duplication of data, allowing you to manage the vulnerability only once.

# About the Vulnerability Life Cycle

In EnterpriseView, the vulnerability life cycle is managed by using the vulnerability's status (see "Status" on page 150) and the vulnerability's remediation status (see "Remediation Status" on page 151). Vulnerability remediation has both manual and automatic aspects. For more information on the automatic aspects, see the *About the Vulnerability Import Job* section in the *EnterpriseView Deployment Guide*.

The following example outlines how to manage the vulnerability life cycle:

1. When a vulnerability occurrence is first imported into EnterpriseView, it has an **Open** status and a **New** remediation status. Remediation status **Reopened** is handled the same as remediation status **New**.

2. A user with an appropriate role assigns **New** and **Reopened** vulnerabilities to users for handling.

   > **Note:** Users can use the **Notes** parameter in order to communicate information to one another or for any other comments that the user wants to document.

3. The user to whom the vulnerability is assigned must first determine whether the vulnerability is an actual problem.

   - If the vulnerability is not found to be significant, then the user can close it, and change its remediation status to **Not an Issue**. Cases in which vulnerabilities are identified as non-issues include vulnerabilities that have very low scores, when the organization uses security tools that provide virtual patching to solve security issues in the network, and any other case in which insignificant reports unnecessarily overload the system.

   - If the vulnerability is found to be significant, then the user investigates methods for solving the problem. The user can use the Solution parameter (see "Solution" on page 154 to help solve the problem. When the solution is found, the user changes the remediation status to **Awaiting Remediation**.

4. After the vulnerability is fixed, the user changes the vulnerability's remediation status to **Awaiting Verification**.

5. The user verifies that the vulnerability is fixed by rescanning the network.

6. If the vulnerability is not reported, then the user changes the vulnerability status to **Closed** and the remediation status to **Resolved**.

7. If a new vulnerability instance is reported for a closed and resolved vulnerability, then the vulnerability status is changed to **Open** and the remediation status is changed to **Reopened**, automatically.

The following flowchart depicts the process described above.
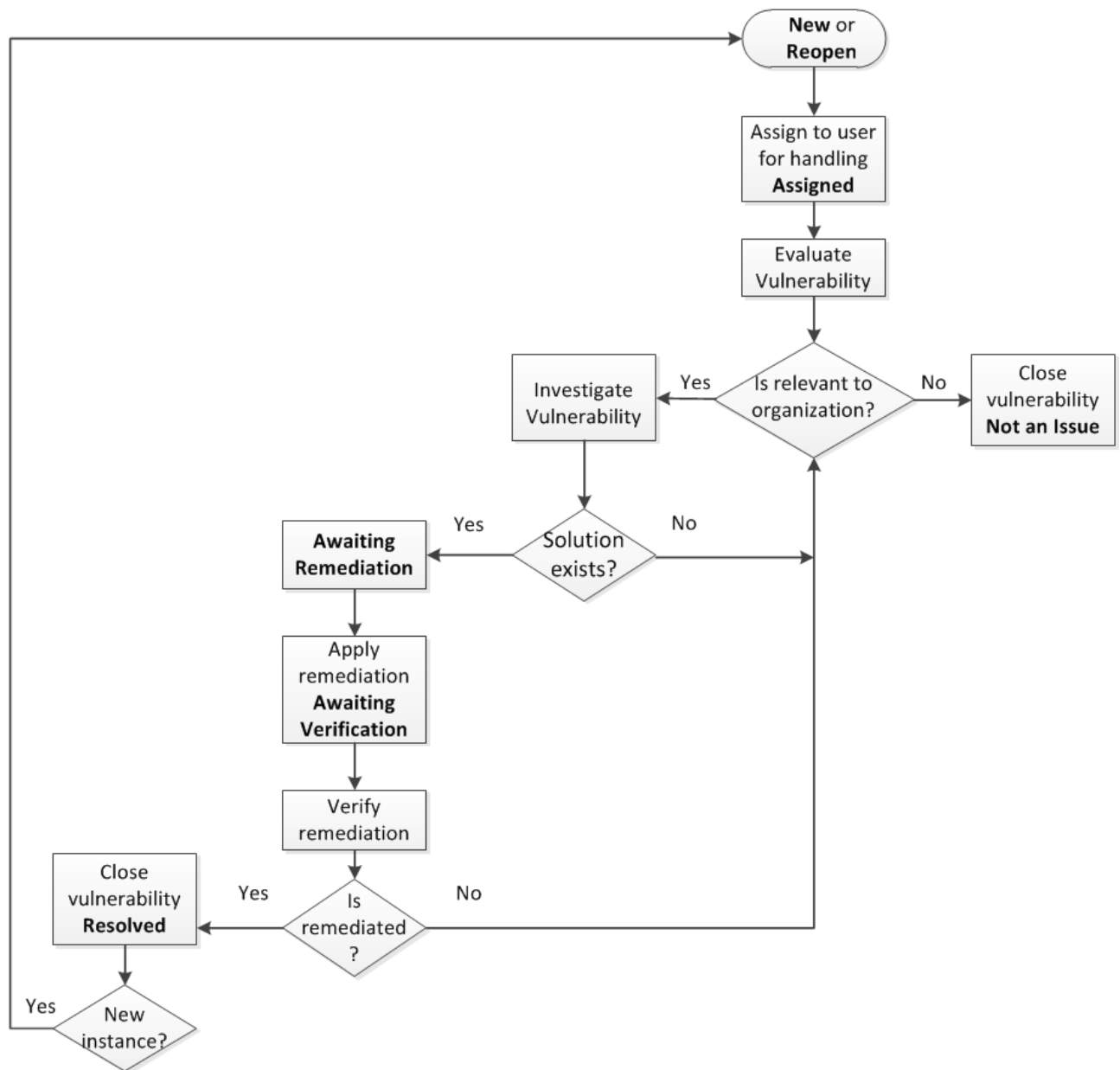


# Common Vulnerability Scoring System

The Common Vulnerability Scoring System (CVSS) is an industry standard vulnerability scoring system for assessing the severity IT vulnerabilities. It is widely adopted by commercial and open-source products, such as McAfee, National Vulnerability Database, Qualys, and Tenable network Security.

EnterpriseView uses CVSS v2 as the scoring system for the vulnerabilities defined in the vulnerability dictionary. For more information on the vulnerability dictionary, see"Vulnerability Dictionary" on page 164.

The score defined in the vulnerability dictionary is based on the following metrics:

- Base: Represent the intrinsic qualities of a vulnerability.

- Temporal: Represent the characteristics of a vulnerability that change over time but are not related to your organization's environment.

Because temporal metrics are dynamic by nature, the vulnerability score is regularly updated by EnterpriseView labs. Every time you update the vulnerability dictionary in EnterpriseView, you receive the most updated vulnerability scores. In addition to the vulnerability score, EnterpriseView displays the scoring vector, providing you a breakdown of the score calculation. For more information on the vulnerability score, see "Vulnerability Properties" on page 150.

After a vulnerability is attached to an asset, the vulnerability score on that asset is recalculated to include environmental metrics. Therefore, the vulnerability score defined in the vulnerability dictionary will usually be different than the vulnerability score on a specific asset.

# Manage the Vulnerability Life Cycle

You can change vulnerability statuses, as described in the following procedure. For information on the vulnerability life cycle, see "About the Vulnerability Life Cycle" on page 143.

### To manage the vulnerability life cycle

1. Click **Vulnerabilities > Management**.

2. From the grid, select the relevant vulnerability, and then click the **Details View** button.

3. In the **Status Management**, perform the following steps, and then click **Save**:

   a. If required, change the **Status** field.

   b. From the **Remediation Status** drop-down list, select the relevant status.

   c. If required, use the **Notes** parameter to communicate information with other users or for any other comments that you want to document.

# Attach a Vulnerability to an Asset

During the Vulnerability Import Job, vulnerabilities are mapped and attached to assets. For more information, see the *About the Vulnerability Import Job* section in the *EnterpriseView Deployment Guide*. In some cases, vulnerabilities cannot be mapped to assets, which results in unattached vulnerabilities. You can manually attach vulnerabilities to assets via the Vulnerability Assignment window. You can also detach vulnerabilities from one asset and reattach them to a another asset.

**Note:** In order to put vulnerabilities in a business context, it is important to attach all vulnerabilities to assets. The more vulnerabilities are attached to assets the more accurate the overall asset risk  score will be.

## To attach a vulnerability to an asset

1. Click  **Vulnerabilities > Assignment**.

2. On the **Vulnerability Assignment** window, in the **Assets** pane, select the asset to which you want to attach a vulnerability/vulnerabilities using either of the following methods:

   ▪ In the **Organization** tab, expand the organization tree.

   ▪ In the **Search** tab, enter the asset name or a partial name.

   The **Unattached Vulnerabilities** pane displays all the vulnerabilities that have been imported into EnterpriseView that are not currently attached to an asset.

3. If necessary, you can filter the vulnerabilities according to the vulnerability score or status, or by clicking **More Filters**. For more information on the vulnerability properties in the **Filter Vulnerabilities** dialog box, see "Summary View Grid" on page 150.

4. From the **Unattached Vulnerabilities**, select the vulnerability that you want to attach to the asset, and then click <  Attach . You can also select multiple vulnerabilities by pressing CTRL and selecting the vulnerabilities from the list.

   The vulnerability/vulnerabilities are displayed in the **Attached Vulnerabilities** pane.

## To detach a vulnerability from an asset

1. Click  **Vulnerabilities > Assignment**.

2. On the **Vulnerability Assignment** window, in the **Assets** pane, select the asset from which you want to detach the vulnerabilities.

3. From the **Attached Vulnerabilities** pane, select the vulnerability or vulnerabilities that you want to detach from the asset, and then click Detach > .

   The vulnerability/vulnerabilities are displayed in the **Unattached Vulnerabilities** pane.

# Configure Asset Vulnerability Score Aggregation Parameters

You can configure the asset vulnerability score aggregation parameters to better suit your business needs and your organization's structure. For more information on these parameters, see the *Asset Vulnerability Score Aggregation Mechanism* section in the *HP EnterpriseView User Guide*.

### To configure asset vulnerability score aggregation parameters

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Vulnerabilities > Asset Vulnerability Score Aggregation**.

3. On the  **Asset Vulnerability Score Aggregation** page, enter the following information:

   - **Maximum Children in Calculation**. Decrease the impact of the children severity on the score.

   - **Children Multiplier**. Decrease the impact of the children on the score.

   > **Note:** This change recalculates scores for the entire business model, therefore it might take some time until the updated scores are apparent.

4. Click **Save**.

# Configure Vulnerability Score Ranges

You can configure the ranges for the score severity indication for vulnerability scores.

Vulnerability scores are displayed with one of the following icons:

Low score

Medium score

High score

This configuration is reflected throughout the application, wherever these scores are displayed. For example, on the Vulnerability Management page, in the Score column in the grid.

### To configure vulnerability score ranges

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Vulnerabilities > Vulnerability Ranges**.

3. Under **Vulnerability Score Ranges**, drag the slider to define the score ranges.

4. Click **Save**.

# Configure Vulnerability Dashboard Settings

The Vulnerability Dashboard provides comprehensive information about the vulnerabilities in your organization. You can configure the severity of the statistics that are displayed in the Vulnerability Dashboard according to your organization's business preferences. This data includes:

- The percentage of assets with open vulnerabilities attached. This data is displayed in the Vulnerabilities with the Highest Scores component. You can configure high, medium, and low ranges for this data.

- The percentage of unhandled vulnerabilities (vulnerabilities that have a remediation status of New or Reopened). This data is displayed in the First-Level Children Summary component. You can configure high, medium, and low ranges for this data.

### To configure vulnerability dashboard settings

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Vulnerabilities > Vulnerability Ranges**.

3. Under **Ranges for Impacted Assets with Open Vulnerabilities**, drag the slider to define the percentage ranges.

4. Under **Ranges for Vulnerability Remediation Status New and Reopened**, drag the slider to define the percentage ranges.

5. Click **Save**.

# Configure Vulnerability KPI

The vulnerability KPI is used to determine how close or far the organization is from it's vulnerability objectives. The KPI indicates the percentage of assets, out of both direct and indirect children, with an aggregated vulnerability score that is higher than a certain threshold. The higher the percentage the farther the organization is from its vulnerability objectives.

This KPI reflects the tolerance of your organization to vulnerabilities. It is configurable and should be derived from your organization's strategic plans.

The vulnerability KPI is displayed in the Risk Register page. For more information, see "Risk Register" on page 96.

For more information on KPIs, see "Key Performance Indicators" on page 92.

### To configure vulnerability KPI

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Vulnerabilities > Vulnerability KPI**.

3. On the **Vulnerability KPI** page, do the following:

   a. Under **Threshold**, enter a number between 0 and 10, inclusive.

   b. Under **Percentage Ranges**, drag the slider to the define the severity of the percentage ranges.

4. Click **Save**.

# Vulnerability Properties

The following tables describe all the vulnerability properties according to where they are displayed in the Vulnerabilities module.

**Summary View Grid**

The Summary View is available from the Vulnerability Management window.

Each record in the summary view grid is an occurrence of a vulnerability in a specific location.

| Property | Description |
|---|---|
| **ID** | A common classification ID. This ID can be defined in the vulnerability dictionary or not. |
| **Score** | The vulnerability score is the severity level of the vulnerability expressed as a number between 0 and 10.<br><br>The score of a vulnerability is calculated by EnterpriseView labs. It is CVSS version 2.0 compliant. For more information, see "Common Vulnerability Scoring System" on page 144. Scores of new vulnerabilities that do not exist in the dictionary are imported from the scanner and are normalized to the EnterpriseView scoring system. |
| **Status** | The following options are available:<br><br>● **Open**: The default status of all vulnerabilities that are imported into EnterpriseView. As long as the vulnerability exists, its status is open. A vulnerability can be reopened automatically by EnterpriseView if a new instance of the same vulnerability occurrence is found.<br><br>● **Closed**: You can manually change the status to Closed. Open vulnerabilities are automatically closed by EnterpriseView if they have been open for more than N days. The number of days is configurable in the Configuration module. For more information, see the *Schedule and Activate Vulnerabilities Import Job* section in the *EnterpriseView Deployment Guide*.<br><br>Closed vulnerabilities do not affect the vulnerability scores of assets in the business model. |

| Property | Description |
|---|---|
| **Remediation Status** | The remediation status depends on the vulnerability status, meaning that a vulnerability with status Open has different remediation status options than a vulnerability with status Closed. Some statuses can be applied manually and some are applied automatically by EnterpriseView. |
| | The following options are available: |
| | ● **New**: The default remediation status for open vulnerabilities. |
| | ● **Reopened**: A closed vulnerability can be automatically reopened by EnterpriseView if a new instance of the same vulnerability occurrence is found. |
| | ● **Assigned**: An open vulnerability is assigned to a system user. |
| | ● **Awaiting Remediation**: Remediation for an open vulnerability was found, but has not been applied. |
| | ● **Not an Issue**: A closed vulnerability that was identified as irrelevant to the organization, due to its severity, to the probability of an attack using this vulnerability or for any other reason defined by the organization. A vulnerability with this status will not be reopened. |
| | ● **Awaiting Verification**: Remediation was applied to a vulnerability, but was not verified. |
| | ● **Resolved**: The vulnerability was fixed. |
| | ● **automatically closed**: This status is assigned automatically when a vulnerability has been open for more than N days. The number of days is configurable in the Configuration module. For more information, see the *Schedule and Activate Vulnerabilities Import Job* section in the *EnterpriseView Deployment Guide*. |
| **Attached to Asset** | The asset name in the EnterpriseView business model to which the vulnerability is attached. Vulnerabilities can be attached automatically to IP assets according to their host, IP address or MAC address. Vulnerabilities can also be attached manually to assets. If a vulnerability is not attached to an asset, then this field is empty. For more information, see "Attach a Vulnerability to an Asset" on page 147. |
| **Times Reported** | The number of instances of a vulnerability occurrence. |
| | Imported vulnerabilities can be reported more than once, either by different vulnerability assessment tools or due to multiple scans from the same tool. |

| Property | Description |
|---|---|
| **Location** | The location displayed depends on the type of the vulnerability. Each type has the following location formats:<br><br>• Network: **<Hostname>:<Network Port>**.<br><br>• Application: **<Normalized URI>:<Vulnerable Parameter>**.<br><br>The original URI indicating the location of the vulnerability is normalized by the Vulnerability Import Job. The vulnerable parameter is isolated from the query string passed in the original URI. |
| **First Reported On** | The date that the vulnerability occurrence was first reported, as recorded by the external source from which the vulnerability was imported.<br><br>Format: Mon Day, Year<br><br>Example: Jan 16, 1970 |
| **Last Reported On** | The date that the vulnerability occurrence was last reported, as recorded by the external source from which the vulnerability was imported. |
| **Title** | A short description of the vulnerability. |

**Details View**

The Details View is available from the Vulnerability Management window. The Details View displays information on a single vulnerability occurrence.

| Category | Property | Description |
|----------|----------|-------------|
| **General** | **ID** | See "ID" on page 150 |
| | **Score** | See "Score" on page 150. |
| | **Related CVEs** | The CVE identifiers of related vulnerabilities. Defined by EnterpriseView labs. |
| | **References** | The identifiers defined by various sources for vulnerabilities that are similar or related to the vulnerability defined in the EnterpriseView vulnerability dictionary. |
| | **Details** | A detailed description of the vulnerability. |
| | **Location** | See "Location" on previous page. |
| | **Attached to Asset** | See "Attached to Asset" on page 151 |
| | **Times Reported** | See "Times Reported" on page 151. |
| | **First Reported On** | See "First Reported On" on previous page |
| | **Last Reported On** | See "Last Reported On" on previous page. |
| | **Host** | The host where the vulnerability was found. |
| | **Port** | Relevant only for network scanners. The port where the vulnerability was found. |
| | **Vulnerable Parameter** | The parameter from the URI that is used to exploit the vulnerability. For example, User ID can be the vulnerable parameter in case of an SQL injection vulnerability. This property is displayed only for records originating from application scanners. |

| Category | Property | Description |
|---|---|---|
| **CVSS** | **Base Score** | Represents the intrinsic qualities of a vulnerability. This score is static. For more information on CVSS, see "Common Vulnerability Scoring System" on page 144. |
| | **Temporal Score** | Represent the characteristics of a vulnerability that change over time but are not related to the organization's environment. This score is updated when the vulnerability dictionary content is updated, as described in the *About the Dictionary Information Import Job* section in the HP EnterpriseView Administration Guide. For more information on CVSS, see "Common Vulnerability Scoring System" on page 144. |
| | **Vector** | The components from which the score was calculated and their values. Both base and temporal metrics. Click the **Show** link to see how the score was derived. |
| **Remediation** | **Solution** | A recommended solution for fixing the vulnerability, as provided from the vulnerability assessment tool. |
| | **Filter (TippingPoint)** | The signature number of the TippingPoint filter. |

**Instances**

The Instances tab is available from the Details View page.

The Instances tab includes all the instances reported for a single vulnerability occurrence. The data displayed is provided by the connectors.

| Property | Description |
|---|---|
| **Reported On** | The date and time that the vulnerability instance was reported by the connector. |
| **Source Rule ID** | The identifier of the rule that corresponds to the vulnerability defined in the vulnerability assessment tool. |
| **CVEs** | A list of CVEs that correspond to the scanner rule, as provided by the connector. |
| **Scanner** | The name of the vulnerability assessment tool. |

| Property | Description |
|----------|-------------|
| **Origin** | Information on the instance origin. A concatenation of the following parameters separated by a dash: <br><br> • Source name: Nessus, Qualys, McAfee, or WebInspect. <br><br> • The output of the scanner, either file name or URL <br><br> • CSV file name (connector output) <br><br> • The line number where the vulnerability was reported in the CSV file <br><br> Example, Nessus-/home/Credit Card Vulns/Visa/nessus_report_ WebTrends.nessus- 2011-09-06-17-42-19.done.csv-555 |
| **Scanner Type** | Network or Application. |
| **Scanner Version** | The version of the vulnerability assessment tool. |
| **IP** | Relevant only for network scanners. <br><br> IP address where the vulnerability was found. |
| **MAC** | Relevant only for network scanners. <br><br> MAC address where the vulnerability was found. |
| **Method** | Relevant only for application scanners. <br><br> The HTTP method used by the scanner for finding the vulnerability. |
| **Scheme** | Relevant only for application scanners. <br><br> HTTP, HTTPS, or FTP |
| **Original URI** | Relevant only for application scanners. <br><br> The query string from the original URI. |

# Asset Vulnerability Score Aggregation Mechanism

The aggregated asset vulnerability score is calculated as the higher score out of the following:

- The direct asset vulnerability score, which is the highest score out of all the vulnerability scores of open vulnerabilities that are associated with the asset.

- $$m * \frac{\sum(Aggregated\ Asset\ Vulnerability\ Score\ *\ Criticality\ Level)\ of\ top\ n\ Children}{\sum(Criticality\ Level)}$$

  - **m=Children Multiplier**: This variable is a number between 0 and 1 (inclusive) that is typically used to decrease the impact of the children on the aggregated asset vulnerability score; the lower the number, the smaller the effect. Consider the structure of your business model when configuring this variable. For example, if you have a flat organizational structure, then the children will have a bigger impact then if you have a structure with many levels of hierarchy.

  - **n=Maximum Children in Calculation**: Sorted primarily by aggregated asset vulnerability score and secondarily by criticality level. This variable is used to decrease the impact of the children severity on the aggregated asset vulnerability score; the higher the number, the smaller the impact. Consider the structure of your business model when configuring this variable. For example, if assets in your business model have a maximum of five children each, then it would be meaningless if this variable is configured to six.

  For more information on configuring these variables, see the *Configure Vulnerability Score Aggregation Parameters* section in the *EnterpriseView Deployment Guide*.

The aggregated asset vulnerability score is calculated when any of the following takes place:

- Any change is made to the Children Multiplier or to the Maximum Children in Calculation. In this case, the scores on the entire business model are recalculated, so it might take some time until the updated scores are apparent.

- An asset is removed from the business model or is moved within the business model.

- The criticality level of an asset is modified.

- A vulnerability is either attached or detached from an asset.

- Any change is made to a vulnerability's status.

# Vulnerability Error Handling

Vulnerability assessment tools generate reports in a variety of formats, such as an XML file or into a database. The information is converted to CSV format using connectors. The Vulnerability Import Job retrieves the CSV files, processes the information and writes it to the EnterpriseView database. For more information on the Vulnerability Import Job, see the *About the Vulnerability Import Job* section in the *EnterpriseView Deployment Guide*.

The connectors write the CSV file to the **<EnterpriseView Installation folder>/vm/import/pending/<connector ID>** folder. The Vulnerability Import Job processes the files and does the following:

- Successfully processed files are moved to the **<EnterpriseView Installation folder>/vm/import/done/<connector ID>** folder. When vulnerabilities are not defined in the vulnerability dictionary, their records might contain data that was not fully imported into EnterpriseView due to format constraints. In these cases, the data is truncate, and only partial information is displayed.

  For example,the **Description** field in EnterpriseView can be a maximum of 4000 characters, but the field in the file holds a value of 5000 characters. In this case, only the first 4000 characters are imported and displayed.

  If a record is modified then a notification, indicated by "INFO", is entered into the redcat-vulnerability-admin.log file that is located in the <**EnterpriseView** Installation folder>/logs folder.

- Files containing erroneous records are moved to the **<EnterpriseView Installation folder>/vm/import/errors/<connector ID>** folder. If an erroneous record exists, then the record is skipped and an error message is entered into the redcat-vulnerability-admin.log file that is located in the <**EnterpriseView** Installation folder>/logs folder.

In either case, vulnerability information is displayed in the Vulnerability Management window. The **Last Imported On** field on the top left side of the Vulnerability Management window displays the date and time of the most recent import update. If there are any ERROR or INFO messages in the redcat-vulnerability-admin.log file, an icon informing the user of errors or notifications is displayed right next to the **Last Imported On** field.

The redcat-vulnerability-admin.log file is updated with each import. The maximum size of this file is 4MB. When the maximum size is reached, a backup copy of the file is created with the following suffix:

redcat-vulnerability-admin.log **.1**

Whenever a new backup file is created, the suffix is incremented by 1. Up to 19 backup files can be created. After the maximum number of files is reached, the oldest file is deleted.

Because the log file generally includes multiple imports, you can use the Job Execution ID to locate the latest job. Check the Job Management module for the last job executed. For more information, see the *Troubleshoot Batch Jobs* section in the *HP EnterpriseView Administration Guide*.

**File Format**

Following is the format of a log file record:

<timestamp> ERROR/INFO "The file <file name> for job execution ID <ID> has the following issues in line number <line number>

<error/info message1>

<error/info message2>"

Example:

```
2012-01-31 18:07:43,801 ERROR The file '6_error-handling.done.csv'
for job execution ID '36' has the following issues in line number 3

The values in the following fields exceed the maximum length:

Description (event.flexString1),  maximum length: 4000

These fields were truncated to the maximum length.

The following fields are mandatory and are missing from the record:

Host (event.destinationHostName)

This record was skipped.
```

# Vulnerability Management Window

The Vulnerability Management window enables you to filter the vulnerabilities found in your organization's network using various criteria, creating views that help you manage the vulnerability life cycle. The different areas and the functionalities available in each are described in the following sections.

## Toolbar

| UI Element | Description |
| --- | --- |
| **Vulnerabilities Affecting Asset** | Filter the vulnerabilities in the grid using one of the following options:<br><br>• **All Vulnerabilities**: View all vulnerabilities, both attached to assets and unattached assets.<br><br>• **Unattached Vulnerabilities**: Select this option to view vulnerabilities that are not attached to an asset.<br><br>• **My Organization**: Expand the business model and select an asset. View all vulnerabilities that affect this asset; meaning all vulnerabilities that are directly attached to this asset or that are attached to any of its children. |
| ▦ | **Summary View**<br><br>This is the default view. For more information, see "Summary View" on next page.<br><br>Filters are retained when passing from one view to another. |
| ▤ | **Details View**<br><br>To open this view, select a vulnerability from the grid, and then select this view. For more information, see "Details View" on next page.<br><br>Filters are retained when passing from one view to another. |
| Reports ▾ | **Generate Report**<br><br>Click this button and select a report from the list of reports. If you are prompted, select to always allow pop-ups from the EnterpriseView server. You can save the report as a PDF or open it in a separate browser window.<br><br>You can generate a report for an asset or for an asset and its children. |

| UI Element | Description |
|---|---|
| **Last Imported On** | Displays the date of the most recent import update. If any ERROR or INFO messages are in the redcat-vulnerability-admin.log file, one of the following icons is displayed:<br><br>❌ Errors. Hovering over this icon displays the following message:<br><br>"The last update was completed with errors. For more information, see the redcat-vulnerability-admin.log file or contact your Administrator."<br><br>ⓘ Notifications (INFO). Hovering over this icon displays the following message:<br><br>"The last update was completed successfully. Some notifications exist for this update. For more information, see the redcat-vulnerability-admin.log file or contact your Administrator."<br><br>For more information or error handling, see "Vulnerability Error Handling" on page 157. |
| **Aggregated Asset Vulnerability Score For \<asset\>** | For more information on how this score is calculated, see "Asset Vulnerability Score Aggregation Mechanism" on page 156. |
| ▼ | **Filter Vulnerabilities**<br><br>Click this button to open the **Filter Vulnerabilities** dialog box. You can filter the vulnerabilities in the grid according to the vulnerability properties that are displayed in the grid, described in "Summary View Grid" on page 150. To remove a filter, you can either open the **Filter Vulnerabilities** dialog box and change the filter, or you can close the filter indicators that display on the toolbar. |
| ▼ | **Clear Filter**<br><br>Click this button to clear all the filters that you set through the **Filter Vulnerabilities** dialog box. |

## Summary View

Each record in the summary view grid is an occurrence of a vulnerability in a specific location.

You can filter vulnerabilities using the grid column headers. If the filter string that you enter exceeds 200 characters, only the first 200 characters are used.

The Summary View includes the vulnerability properties describes in "Summary View Grid" on page 150.

## Details View

The Details View includes the following areas:

### Left Pane

This area displays a minimized version of the vulnerabilities grid that is displayed in the Summary View. It includes the vulnerability ID, Location and Title. Clicking on a vulnerability in this grid

**User Guide**
Chapter 9: Vulnerability Management

displays its details in the other panes,allowing you to navigate through the vulnerabilities without changing the view. Vulnerabilities can be filtered using the grid column headers.

**Details (middle pane)**

This area displays the vulnerability properties described in "Details View" on page 153.

**Instances (tab)**

This tab displays the vulnerability properties described in "Instances " on page 154.

**Status Management**

| UI Element | Description |
| --- | --- |
| **Status** | Filter according to the vulnerability's status (**Open** or **Closed**). |
| **Remediation Status** | Filter according to the vulnerability's remediation status. For more information on the different statuses, see "Remediation Status" on page 151. |
| **Notes** | Use Notes to communicate with other users that are involved in remediating the vulnerability and to document anything regarding the vulnerability. Notes cannot be deleted or edited. |
| **Save** | Click to save changes. |
| **Cancel** | Click to clear changes. Reverts any change that you have made to the statuses. |

# Vulnerability Assignment Window

The Vulnerability Assignment window enables you to attach vulnerabilities to assets or detach vulnerabilities from assets. The different areas and the functionalities available in each are described in the following sections.

## Assets

This pane enables you to select the asset to which you want to attach a vulnerability.

| UI Element | Description |
|---|---|
| **Organization tab** | Displays the EnterpriseView business model. Expand the business model to select the asset that you want to display. |
| **Search tab** | Enables you to search for a name or a partial name of any asset in EnterpriseView, connected to the business model. |

## Attached Vulnerabilities

This pane displays all the vulnerabilities that are attached to a selected asset. When an asset is selected, the title of this pane displays the asset name.

| UI Element | Description |
|---|---|
| ‹ Attach | **Attach Vulnerabilities to Asset**<br><br>Select a vulnerability from the grid, and then click this button. For more information, see "To detach a vulnerability from an asset" on page 147. |
| Detach › | **Detach Vulnerabilities from Asset**<br><br>From the grid, select or multi-select (CTRL+click) the vulnerabilities that you want to attach to the asset, and then click this button. For more information, see "Attach a Vulnerability to an Asset" on page 147. |
| **<Vulnerability Grid>** | A grid with the details of the vulnerabilities that are directly attached to the asset in the **Assets** pane. |

## Unattached Vulnerabilities

This pane displays vulnerabilities that are not attached to an asset. It includes the following methods for filtering unattached vulnerabilities:

- Quick filters accessible from the screen
- Header filters
- The Filter Vulnerabilities dialog box

| UI Element | Description |
|---|---|
| **Score** | Filter according to the vulnerability score severity:<br><br>☑ Low<br><br>⚠ Medium<br><br>❌ High<br><br>The ranges are determined in the *Configure Vulnerability Score Ranges* section in the *EnterpriseView Deployment Guide*. |
| **Status** | Filter according to **Open** or **Closed**. |
| More Filters... | **Filter Vulnerabilities**<br><br>Click this button to open the **Filter Vulnerabilities** dialog box. You can filter the vulnerabilities in the grid according to the vulnerability properties that are displayed in the grid, described in "Summary View Grid" on page 150. To remove a filter, click More Filters to open the **Filter Vulnerabilities** dialog box and change the filter. |
| 🔽 | **Clear Filter**<br><br>Click this button to clear all the filters that you set through the **Filter Vulnerabilities** dialog box. |
| **<Vulnerability Grid>** | A minimized version of the vulnerabilities grid that is displayed in the Summary View. It includes the vulnerability ID, Location, Title, and Score. You can filter vulnerabilities using the grid column headers. |

# Vulnerability Dictionary

Many information security tools and sources, both commercial and non-commercial, include a vulnerability database. Each has a different methodology for naming and identifying vulnerabilities. This means that the same vulnerability can be defined differently in each of these sources. Because the Vulnerabilities module receives vulnerability information from various sources, the disparity would make it difficult to identify duplicate reports, provide additional information about the vulnerabilities, and efficiently associate them with remediation actions.

To solve this problem, EnterpriseView labs created and maintains a comprehensive vulnerability dictionary that includes all vulnerabilities, regardless of whether they have been recognized by an industry standard source. EnterpriseView labs compiles, correlates, processes and enriches these vulnerabilities, and creates a single point of reference for each vulnerability.

The EnterpriseView vulnerability dictionary is continually expanded.

EnterpriseView labs sources are varied. Some of the leading industry standard sources from which information is derived are:

- MITRE, Common Vulnerabilities and Exposures (CVE)

- Open Source Vulnerability Database (OSVDB)

- BugTraq

You can view the vulnerabilities in the dictionary via the EnterpriseView user interface. To access the vulnerability dictionary, click **Vulnerabilities > Dictionary**.

The Vulnerability Dictionary window includes three panes:

- **Left pane**: Displays the number of vulnerabilities released each month for the past 24 months. This information is read-only.

- **Middle pane**: Displays the vulnerabilities (ID, title, score, and the date it was added to the dictionary).

- **Right pane**: Displays the properties of the vulnerability that is selected. To view the properties of a vulnerability, click the vulnerability record in the middle pane.

You can search for vulnerabilities using their ID, title, details, or group or partial strings from these properties.

> **Note:** You can perform wildcard searches. For example, if you type **ser\***, the results will contain words beginning with ser (such as server and service). An asterisks cannot be placed before a string (*ser).

# Chapter 10

# Task Management

A workflow is a sequence of connected tasks that produce a final outcome. Tasks are consecutive creating a flow in the work process. Each task in the workflow is assigned to the individual who is most suitable to perform the task. After a task is complete, the individual responsible for the next task is notified. For more information on managing tasks, see "Manage Your Tasks" on page 172.

The Workflow module enables managers to oversee, approve, and follow up on tasks that were not completed. EnterpriseView provides you with a graphic display of each workflow. The status and due date of each task are visible on the workflow map. Overdue tasks include explicit indication.

Example:
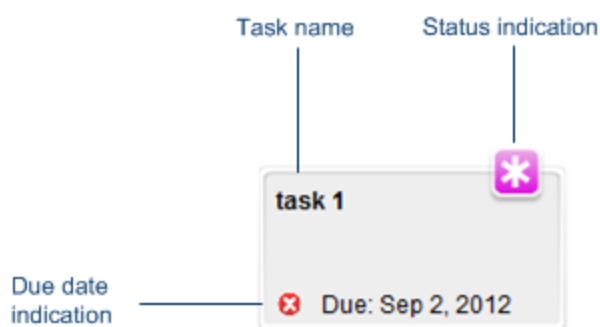


Workflows are based on templates. EnterpriseView includes out-of-the-box workflow templates, such as EnterpriseView Vulnerability Assessment for New Asset. You can create additional templates that represent the workflows in your organization. For more information on creating templates, see "Create a Workflow Template" on next page. You can also edit and delete workflow templates, as described in "Edit a Workflow Template" on page 169 and "Delete a Workflow Template from EnterpriseView" on page 170, respectively.

Each workflow has an owner, but any user with suitable permissions can create, edit, or delete workflows. For more information on how to create, edit, or delete a workflow, see "Create a New Workflow" on page 170, "Edit Workflow Properties" on page 172, and "Delete a Workflow" on page 171, respectively.

The workflow life cycle consists of three modes: Draft, In Progress, and Completed. Workflows are created in a draft mode (**Draft** status). After they are published, their status changes to **In Progress** and after the last active task in the workflow is completed, their status changes to **Completed**.

The Workflow module includes filtering capabilities to help you locate your workflows quickly. For more information on filtering, see "Filter Workflows" on page 176. All completed workflows are displayed at the end of the list. Workflows that are in draft or in progress are sorted by due date; Workflows with an earlier due date are displayed first.

# Manage Workflow Templates

EnterpriseView includes out-of-the-box workflow templates, such as EnterpriseView Vulnerability Assessment for New Asset. You can create additional templates that represent the workflows in your organization.

This section includes information on managing workflow templates. It includes the following topics:

# Create a Workflow Template

EnterpriseView includes out-of-the-box workflow templates, such as EnterpriseView Vulnerability Assessment for New Asset. You can create additional templates that represent the workflows in your organization.

All workflow templates must fulfill the following conditions:

- A template must have a name.

- Begin with a start event and end with an end event.

- The first task after the start event must have the name "Initialize". There can be only one Initialize task.

- There can be only one outbound sequence flow from the start event; meaning that it can be connected only to the Initialize task.

- There can be only one inbound sequence flow to the Initialize task.

- All tasks must be of type **User**.

- All tasks must be assigned to an EnterpriseView page. When the task is ready to be carried out by the user, it is displayed on the Home page and on the page assigned to it in the template.

The following diagram is an example of a workflow template.
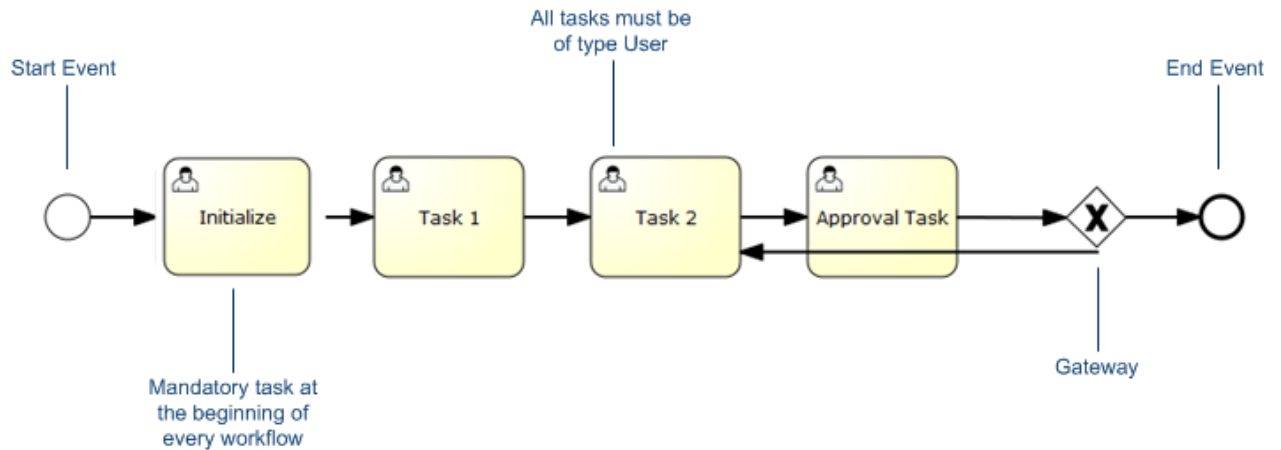
After you create a template you need to upload it to EnterpriseView in order to use it. For more information, see "Upload a Workflow Template to EnterpriseView" on page 169.

## To create a workflow template

1. Access Activiti Modeler using the following URL:

   **http://<EnterpriseView Fully Qualified Domain Name>:<EnterpriseView Port>/activiti-modeler**

2. On **Activiti Modeler**, click **New > Business Process Diagram (BPMN 2.0)**.

3. On the **New Process** window, **under Shape Repository**, expand the list and select **BPMN (Activiti)**.

   > **Note:** EnterpriseView supports only **BPMN (Activiti)**; it does not support **BPMN (Complete)**.

4. On the right, expand the **Attributes** pane.

5. On the **Properties** pane, under **Main Attributes**, click in the **Name** field, and enter a name for the template.

   > **Note:** The template name must be unique.

6. On the **New Process** window, in the **Shape Repository**, expand the **Start Events**. Drag a **Start Event** to the canvas.

7. Click the start event in the canvas, and then, on the floating toolbar, click the **Task** ☐ button.

   A new task is created with a sequence flow from the start event. A sequence flow defines the execution order of the activities.

8. Click the task that you just created. On the **Properties** pane, do the following:

   - Click in the **Name** field, under **Value**, and enter "**Initialize**".

   - Click in the **Tasktype** field, under **Value**, and select **User** from the list.

9. To assign an EnterpriseView page to the task, do the following:

    a. Under **More Attributes**, click in the **Properties** field, in the **Value** column.

    b. On the **Editor for a Complex Type** dialog box, click **Add**.

    c. In the **Name** field, enter **page=n**, where n is the page ID. For example, if you want to assign the task to the Vulnerability Management page, enter **page=4** (case sensitive). For the list of page IDs, see "EnterpriseView Page IDs" on page 178.

    d. Click **OK**.

10. Click the Initialize task in the canvas. Click the **Task** ☐ button to add the next task. For each task that you create, do the following:

    Add as many tasks as you require.

    ■ Change the **Tasktype** to **User**.

    ■ In the **Name** field, enter a name. The name of the task should be short and should reflect the main idea of the task.

    ■ In the **Documentation** field, enter a detailed description of the task.

11. To create an approval task, follow the instruction in "To create an approval task" below.

12. Add an end event or end events to your template (optional). The end event indicates that there are no tasks. To add an end event, after you have added all the required tasks, click on the task in the canvas that does not have any tasks after it, and then, from the floating toolbar, click the

    **End Event** ◯ button.

13. Click **Save**.

14. On the **Save** dialog box, in the **Title** box, enter the file name for the template, and then click **Save**.

    The file name that you enter is the name that will be displayed when you upload the template into EnterpriseView.

## To create an approval task

**Note:** You can create more than one approval task in a workflow template.

1. Create a task with Tasktype **User**, as described in the previous procedure, and give it a meaningful name. For example, "Approve Audit".

2. Click the approval task in the canvas, and then click the **Data-based exclusive (XOR) gateway** button.

3. From the gateway, create two outbound sequence flows:

    ■ One leading to the next task in the flow, in case of approval.

    ■ The second leading to the task that should be redone, in case of rejection.

4. Click the sequence flow that represents the approved flow, and then do the following:

    a. In the **Properties** pane, expand **More Attributes**.

    b. Invent a variable name to use for this specific approval task. The variable must be alpha numeric. You must use the same variable for the approval flow and for the rejection flow.

The rejection flow variable is precedes by an **!**.

> **Note:** You cannot use this variable for another approval task; each approval task must have a unique variable.

    c. Click in the **Condition expression** field, and enter **${<variable>}**.

5. Click the sequence flow that represents the rejection flow, and then do the following:

    a. In the **Properties** pane, expand **More Attributes**.

    b. Click in the **Condition expression** field, and enter **${!<variable>}**.

# Upload a Workflow Template to EnterpriseView

You can upload a template created in Activiti Modeler to EnterpriseView.

For more information on creating a template, see "Create a Workflow Template" on page 166.

## To upload a template

1. Click **Task Management > Workflow Management**.

2. On the **Workflow Management** window, click **Manage Templates**.

3. On the **Manage Workflow Templates** dialog box, click **Upload Template**.

4. On the **Upload Template** dialog box, select the file of the template that you want to upload, and then click **Upload**.

   EnterpriseView validates the template. If the template is not valid, a message is displayed indicating the problem. To create a valid template, see "Create a Workflow Template" on page 166.

   The template is added to the list of templates displayed in the **Manage Workflow Templates** dialog box.

5. On the **Manage Workflow Templates** dialog box, click **Close**.

# Edit a Workflow Template

Editing a workflow template means changing a template in Activiti Modeler, saving it under the same file name, and reloading it to EnterpriseView.

If you created a workflow and then changed the template, the workflow that is based on the previous version does not change.

## To edit a workflow

1. Open **Activiti Modeler**.

2. On the **Workspace**, click the template that you want to edit.

3. Make the required changes and save the template. For more information on how to edit the template, see "Create a Workflow Template" on page 166.

> **Note:** EnterpriseView recognizes the template by its name and not by its file name. If you change the template name, then it will no longer be considered the same template in EnterpriseView. When you edit a template, it is recommended to save it under the same file name.

4. Upload the updated template to EnterpriseView. For more information, see "Upload a Workflow Template to EnterpriseView" on previous page.

# Delete a Workflow Template from EnterpriseView

You can delete a template from EnterpriseView as long as there are no published workflows based on that template. If there are draft workflows (workflows that have not been published), they are deleted along with the template. Workflows can be deleted while they are in draft mode or in progress. For more information, see "Delete a Workflow" on next page.

### To delete a template

1. Click **Task Management > Workflow Management**.

2. On the **Workflow Management** window, click **Manage Templates**.

3. Select the template from the list, and then click **Delete Template**.

   You can reload the template at any time, as described in "Upload a Workflow Template to EnterpriseView" on previous page

# Manage Workflows

This section includes the following topics:

# Create a New Workflow

You can create a workflow based on the templates in EnterpriseView (user-defined or out-of-the-box). When you create a workflow, you assign tasks to users. After you assign all the tasks you can publish the workflow. Publishing the workflow means that users can start carrying out their tasks.

### To create a workflow

1. Click **Task Management > Workflow Management**.

2. On the **Workflow Management** window, click **New**.

3. On the **New Workflow** dialog box, select a template from the list.

4. Enter the following information:

- **Name**: Enter a meaningful name for the workflow. The name of the workflow must be unique.

- **Owner**: Select an owner for the workflow. The owner of the workflow is responsible for the workflow and for carrying out the Initialize task. As long as the workflow is in draft mode, you can change the owner. If you change the owner, then the Initialize task is reassigned accordingly.

- **Due Date**: Select the date on which the workflow should be complete.

- **Description** (optional): Enter additional information.

5. Click **Save**.

    The workflow is created with the status **Draft**. It is displayed in the **Workflows** list on the left pane of the **Workflow Management** window and the workflow diagram in the map area.

    The Initialize task is in status **In Progress** and all the other tasks are in status **New**.

6. You can edit the Initialize task by clicking it in the map area and editing its properties in the **Properties** pane. The default due date for this task is one day after the current date and it is assigned to the workflow owner.

7. Assign tasks to users. Click the task in the map area, and then, in the **Properties** pane, do the following:

    a. In the **Assigned To** box, enter the user name of the person responsible for carrying out the task.

    b. In the **Due Date** box, enter a due date for the task.

    c. Click **Save**.

    Repeat this process for all tasks.

8. In the left pane, click the **Publish** button.

    This action validates that all mandatory information has been entered into all tasks. If mandatory information is missing, then a message is displayed.

    The status of the workflow is changed to **In Progress** and the status of the Initialize task is changed to **Completed**. The tasks after the Initialize task are displayed in the assignee's **My Tasks** list. To manage user tasks, see .

# Delete a Workflow

You can delete a workflow that is either in draft mode or is in progress. When you delete a workflow you delete all of its related tasks.

### To delete a workflow

1. Click **Task Management > Workflow Management**.

2. On the **Workflow Management** window, from the **Workflows** list in the left pane, click the workflow that you want to delete.

3. Click the **Delete** button.

The workflow is removed from the list. All related tasks are deleted.

# Edit Workflow Properties

You can edit the workflow properties when the workflow is either in draft mode or in progress. After you complete a workflow, you cannot edit any of its properties or its task properties.

### To edit workflow properties

1. Click **Task Management > Workflow Management**.

2. On the **Workflow Management** window, from the **Workflows** list in the left pane, click the workflow that you want to edit.

3. Click the **Properties** button.

4. On the **Workflow Properties** dialog box, make the necessary changes, and then click **Save**. For information on workflow properties, see "Workflow Properties" below.

# Manage Your Tasks

All the tasks that you need to perform are displayed in the **My Tasks** pane on the EnterpriseView home page. This includes tasks that have the status In Progress. New tasks are not displayed in My Tasks because they are not active. After they are activated, meaning that their status is In Progress, they are displayed in My Tasks. Completed tasks can only be viewed from the Workflow Management window. For more information, see "Workflow Management Window" on page 176. You can access the page on which you need to perform a task directly from the **My Tasks** pane on the home page, by clicking the task name link.

You can access your tasks by clicking **My Tasks** on the EnterpriseView toolbar. Accessing your tasks from the **My Tasks** pane on the home page while you are on the home page, displays the same list of tasks as in the **My Tasks** pane. If you click **My Tasks** from the toolbar while any other page is open, then only the tasks that are relevant to that page are displayed.

### To manage your tasks

1. After you successfully performed your task, click **My Tasks** on the toolbar.

2. To complete a task, select the **Complete Task** checkbox. If this is an approval task, select either **Approve** or **Reject**.

3. You can also reassign a task to another user, change the task due date, or insert a comment. For more information on the task properties, see "Task Properties" on next page.

4. Click **Save**.

   The task is removed from your task list.

# Workflow Properties

The following table describes all the workflow properties.

| Property | Description |
|----------|-------------|
| **Name** | The name of the workflow must be unique. |
| | You can change the name of a workflow when it is in draft mode or in progress. After it is completed, the name cannot be changed. |
| **Template** | The template on which the workflow is based. |
| | For more information, see "Manage Workflow Templates" on page 166. |
| | You cannot change the template of a workflow. |
| **Owner** | The person responsible for managing the workflow. |
| | When the workflow is created, the owner of the workflow is assigned to the Initialize task. |
| | The owner of the workflow can be changed as long as the workflow is not completed. |
| **Due Date** | The expected completion date of the workflow. |
| | The due date is the date on which the workflow is expected to be completed. It is configured when you create a workflow. |
| | The due date is displayed for workflows that have a **Draft** or **In Progress** status. |
| | The actual date on which the workflow is completed is the due date of the last task. If the last task due date is later than the workflow due date, it means that the workflow is past its due date. The following indication is displayed: |
| | ❌ Past the due date |
| **End Date** | The actual completion date of the workflow. |
| | The date on which the workflow is actually completed, meaning that the last task in the workflow has been completed. |
| | The end date is displayed for workflows that have a **Completed** status. |
| **Last Task Due Date** | The due date of the last task in the workflow. |
| | This date serves as a threshold indicating whether the workflow due date is on schedule or at risk of not being met. |
| **Description** | A general description of the workflow. |

# Task Properties

The following table describes all the task properties.

**Note:**

- You cannot edit task properties that are defined in the workflow template.

- You cannot edit task properties after the task is completed.

| Property | Description |
|---|---|
| **Name** | The name of the task as defined in the template. |
| **Module** | The module to which the task is related.<br><br>The module is inferred from the page selected when the template is created. See "Page " below. |
| **Page** | The page that the task is related to as defined in the template.<br><br>When creating a template, the user must assign the task to a specific page in EnterpriseView. For more information, see "Create a Workflow Template" on page 166. |
| **Assigned To/Assignee** | The user (assignee) to which the task is assigned.<br><br>The assignee is responsible for carrying out the task.<br><br>In My Tasks, this field is referred to as **Assignee**. In the properties pane of the Workflow Management page, this field is referred to as **Assigned To**. |
| **Due Date** | The expected completion date of the task.<br><br>The due date is configured by the workflow owner before the owner publishes the workflow.<br><br>Tasks in the workflow graph in the Workflow Management window includes the following indicators:<br><br>- ❌ Past the due date.<br><br>  This indicator is displayed after the due date passes, meaning on the day after the due date.<br><br>- ⚠️ Approaching the due date.<br><br>  This indicator is displayed on the day before the due date and until the due date is passed. |
| **Description** | A general description of the task as defined in the template. |

| Property | Description |
|---|---|
| **Status** | The status of the task:<br><br>● **New**: The status of a task that is not active after a workflow has been published. At this stage the task is not available to the assignee. New tasks are accessible only from the Task Management page, but are not displayed in My Tasks. There are two possible indicators:<br><br>  ■ **Not initialized**. Not all mandatory fields are configured.<br><br>  ■ **Initialized**. The task is assigned and has a due date.<br><br>● **In Progress**: A task receives this status only after its preceding task is completed. If there is more than one task before it, then at least one of the preceding tasks must be complete. Tasks that are in progress are displayed in My Tasks displayed in the Home page and in the My Tasks dialog box accessible from the EnterpriseView toolbar. These tasks need to be carried out by their assignee.<br><br>● **Completed**: The task status is automatically updated to **Completed** after the user selects the **Complete Task** check box or the **Reject** or **Approve** options (for approval tasks) and clicks **Save**. |
| **Complete Task** | Select this check box if you want to mark the task as completed, and then click **Save**. The status of the task is changed to **Completed** and cannot be changed back to **In Progress**. |
| **Approve/Reject** | Displayed for approval tasks.<br><br>Select one of the options to approve or reject the tasks in the workflow, and then click **Save**. If you approve, then the workflow proceeds to the following task. If you reject, then the workflow returns to a designated task, as defined in the template. A new task of the same type is created. For an example of a rejection flow, see "Rejection flow" on page 177. |
| **Comments** | Comments are shared by all the tasks that are related to a specific workflow. Both the owner and the various task assignees can enter a comment. Use comments to communicate with your colleagues, convey information, and mitigate problems related to the workflow.<br><br>When you enter a comment and click **Save**, all users related to the specific workflow can view your comment. |

# Workflow Management Window

The Workflow Management window enables you manage workflows and workflow templates. For more information, see "Task Management" on page 165. The different areas and the functionalities available in each are described in the following sections.

## Toolbar

The toolbar includes the **Manage Templates** button.

Click this button to open the **Manage Workflow Templates** dialog box.

The **Manage Workflow Templates** dialog box includes all the actions that are related to template:

- Upload template. For more information, see "Upload a Workflow Template to EnterpriseView" on page 169.

- View template. Click the template name to display the workflow graph on the map. You can reset the layout, zoom in/out, or navigate the mini-map to better display the template.

- Delete template. For more information, see "Delete a Workflow Template from EnterpriseView" on page 170.

## Left Pane

The left pane displays all the workflows that are in the system. Completed workflows are displayed at the bottom of the list. Workflows in draft or in progress are sorted by due date; the workflow with the earliest due date is displayed first.

| UI Element | Description |
|---|---|
| **New** | **Create a New Workflow**<br><br>Click this button to create a new workflow. For more information, see "Create a New Workflow" on page 170. |
|  | **Filter Workflows**<br><br>Click this button to open the **Filter Workflows** dialog box. You can filter the workflows that are displayed in the left pane by template name, workflow name, owner, and status.To remove a filter, you can either open the **Filter Workflows** dialog box and change the filter, or you can click the **Clear Filter**  button. |
|  | **Clear Filter**<br><br>Click this button to clear all the filters that you set through the **Filter Workflows** dialog box. |
|  | **Properties**<br><br>Click on this button to edit or view the workflow properties.<br><br>For more information, see "Edit Workflow Properties" on page 172. |

| UI Element | Description |
|---|---|
|  | **Publish**<br><br>Click this button to publish a workflow.<br><br>A workflow can be published only after all tasks are initialized; meaning that they are assigned to users and have a due date. |
|  | **Delete**<br><br>Click this button to delete the workflow. All related tasks are deleted regardless of their status. you cannot delete a workflow that has been completed. For more information, see "Delete a Workflow" on page 171. |
| **<Status>** | One of the following values is displayed:<br><br>• **Draft**: The status of a workflow before it is published. Users have not started working on their tasks.<br><br>• **In Progress**: The status of a workflow after it is published. Users have started working on their tasks.<br><br>• **Completed**: The status of a workflow after all its tasks have been completed. |
| **Due Date** | See "Due Date" on page 173. |
| **End Date** | See "End Date" on page 173. |

## Map Area

The map area includes the workflow graph. The following diagram is an example of a task that has been rejected, meaning that some tasks need to be carried out again.

**Rejection flow**

| UI Element | Description |
|---|---|
|  | **Reset Layout**<br><br>Optimizes the workflow graph in the map area. |
|  | Zoom in/zoom out business model. |

### Properties Pane

The Properties pane displays the properties for a task selected in the map area. For information on task properties, see "Task Properties" on page 173.

| UI Element | Description |
|---|---|
|  | **Next Task**<br><br>This button helps you navigate between tasks of the same type. For example, if a workflow is rejected by the owner, then one or more tasks need to be repeated. In this case, new, duplicate tasks are created for each task that was rejected. You can navigate between these tasks using this button. |
|  | **Previous Task**<br><br>See "Next Task" above. |
| **Save** | Save the changes that you made to the task properties. |
| **Cancel** | Cancel the changes that you made to the task properties. |

### Mini-map

When the workflow is too large to be entirely displayed in the map area, you can navigate it by dragging in the mini-map area.

To expand or collapse the mini-map, click the **Expand/Collapse**  button.

# EnterpriseView Page IDs

The following table includes the page ID for all EnterpriseView pages.

| Page ID | Page Display Name |
|---|---|
| 1 | Risk Indicators |
| 2 | Threat Library Builder |
| 3 | Risk Modeling Assessment |
| 4 | Vulnerability Management |

| Page ID | Page Display Name |
|---------|-------------------|
| 5 | Vulnerability Assignment |
| 6 | Vulnerability Dictionary |
| 7 | Policy Builder |
| 8 | Policy Mapping |
| 9 | Statement of Applicability |
| 10 | Policy and Compliance Assessment |
| 11 | Vulnerability to Control Mapping |
| 12 | Control to Threat Mapping |
| 13 | Asset Profiling |
| 14 | Task Management |
| 15 | Configuration |
| 16 | User Management |
| 17 | Job Management |
| 18 | Audit Log |
| 19 | Dashboard Builder |

HP EnterpriseView (1.5)

# Settings

EnterpriseView includes a centralized Settings module, through which you can configure all internal settings.

To access the settings module, on the EnterpriseView toolbar, click **Settings**. If you open Settings when the home page is open, then the **Settings** dialog box opens on the main page and displays links to the following modules:

- ESM Threat

- Executive View

- Vulnerabilities

- Policy and Compliance

- Risk Modeling

**Note:** You have access only to modules for which you have the required permissions.

Click the module name in order to access the configuration options for that module.

If you open Settings when one of the above mentioned modules is open, then the **Settings** dialog box opens on the page of that module. For example, if the Vulnerability Management page is open, when you click **Settings**, then the **Settings** dialog box opens on the **Vulnerabilities** page. To return to the **Settings** main page, click **Settings** on the title bar.

The following table includes all the configuration options available through the **Settings** dialog box, for each module.

| Module | Setting Page |
| --- | --- |
| ESM Threat | ESM Threat KPI<br><br>For more information, see "Configure ESM Threat KPI" on page 184. |
| | ESM Threat Score Ranges<br><br>For more information, see "Configure ESM Threat Score Ranges" on page 183. |

| Module | Setting Page |
|---|---|
| Executive View | Asset overall Score Formula |
| | For more information, see "Configure Asset Overall Score Formula" on next page. |
| | Asset Overall Score Ranges |
| | For more information, see "Configure Asset Overall Score Ranges" on next page. |
| | Criticality Level Ranges |
| | For more information, see "Configure Criticality Level Ranges" on page 183. |
| Vulnerabilities | Asset Vulnerability Score Aggregation |
| | For more information, see "Configure Asset Vulnerability Score Aggregation Parameters" on page 148. |
| | Vulnerability KPI |
| | For more information, see "Configure Vulnerability KPI" on page 149. |
| | Vulnerability Ranges |
| | For more information, see "Configure Vulnerability Score Ranges" on page 148 and "Configure Vulnerability Dashboard Settings" on page 149. |
| Policy and Compliance | Compliance KPI |
| | For more information, see "Configure Compliance KPI" on page 50. |
| | Compliance and Maturity Score Ranges |
| | For more information, see "Configure Compliance and Maturity Score Ranges" on page 49. |
| | Policy Administration |
| | For more information, see "Activate a Policy" on page 38. |

| Module | Setting Page |
|---|---|
| Risk Modeling | Actor Weights<br><br>For more information, see "Configure Risk Assessment Settings" on page 78. |
| | Impact Area<br><br>For more information, see "Configure Risk Assessment Settings" on page 78. |
| | Risk Score Ranges<br><br>For more information, see "Configure Risk Score Ranges" on page 78. |
| | Risk KPIs<br><br>For more information, see "Configure Risk KPIs" on page 80. |

# Configure Asset Overall Score Formula

There are five quantitative factors that comprise the overall risk to your organization's assets. These factors include the policy compliance score, the control maturity score, the risk score, the asset vulnerability score, and the ESM threat score. The asset overall score is the weighted average of the five factors:

$$\frac{Risk * weight + (100 - Maturity * 20) * weight + (100 - Compliance) * weight + ESM * 10 * weight + Vulnerabilty * 10 * weight}{\sum weights}$$

You can edit the weights of each of the variables in the formula.

### To configure the asset overall score formula:

1.  On the EnterpriseView toolbar, click **Settings**.

2.  On the **Settings** dialog box, click **Executive View > Asset Overall Score Formula**.

3.  On the **Asset Overall Score Formula** page, enter the weight for each variable in the formula.

4.  Click **Save**.

# Configure Asset Overall Score Ranges

You can configure the ranges for the score severity indication for asset overall scores.

Asset overall scores are displayed with one of the following icons:

Low score

Medium score

High score

This configuration is reflected throughout the application, wherever these scores are displayed. For example, on the Risk Register page, in the Asset Summary component and in the Overall Score Heat Map page.

### To configure vulnerability score ranges

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Executive View > Asset Overall Score Ranges**.

3. Under **Asset Overall Score Ranges**, drag the slider to define the score ranges.

4. Click **Save**.

# Configure Criticality Level Ranges

You can configure the ranges for the severity indication for the criticality levels. Severity is indicated by color:

- Low = green

- Medium = yellow

- High = red

This configuration is reflected in the Overall Score Heat Map.

### To configure criticality level ranges

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **Executive View > Criticality Level Ranges**.

3. Under **Criticality Level Ranges**, drag the slider to define the ranges.

4. Click **Save**.

# Configure ESM Threat Score Ranges

You can configure the ranges for the score severity indication for aggregated ESM threats.

Aggregated ESM threats scores are displayed with one of the following icons:

✅ Low score

⚠️ Medium score

❌ High score

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

### To configure ESM threat score ranges

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click **ESM Threat > ESM Threat Ranges**.

3. Under **ESM Threat Ranges**, drag the slider to define the score ranges.

4. Click **Save**.

# Configure ESM Threat KPI

The ESM threat KPI is used to determine how close or far the organization is from it's ESM threat objectives. The KPI indicates the percentage of assets, out of both direct and indirect children, with an aggregated ESM threat score that is higher than a certain threshold. The higher the percentage the farther the organization is from its ESM threat objectives.

This KPI reflects the tolerance of your organization to ESM threats. It is configurable and should be derived from your organization's strategic plans.

The ESM threat KPI is displayed in the Risk Register page. For more information, see "Risk Register" on page 96.

For more information on KPIs, see "Key Performance Indicators" on page 92.

## To configure ESM threat KPI

1. On the EnterpriseView toolbar, click **Settings**.

2. On the **Settings** dialog box, click  **ESM Threat >  ESM Threat KPI**.

3. On the **ESM Threat KPI** page, do the following:

   a. Under **Threshold**, enter a number between 0 and 10, inclusive.

   b. Under **Percentage Ranges**, drag the slider to the define the severity of the percentage ranges.

4. Click **Save**.