HP ArcSight EnterpriseView

For the Windows Operating System

Software Version: 1.0

ArcSight EnterpriseView User Guide

Document Release Date: March 2012

Software Release Date: March 2012

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

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

Restricted Rights Legend

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

Copyright Notice

Follow this link to see a complete statement of copyrights and 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

Welcome to This Guide

Welcome to HP ArcSight 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 ArcSight EnterpriseView

HP ArcSight 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.

Chapter 3

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, 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 13).

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.

There are many different types of assets, which are divided into categories. For more information,see "Manage Asset Types" (on page 11).

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**: 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.

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. In EnterpriseView, 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 *ArcSight EnterpriseView Deployment Guide*.

To edit an asset type

1. In EnterpriseView, click the **Configuration** tab.
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 *ArcSight EnterpriseView Deployment Guide*.

To delete an asset type

1. In EnterpriseView, click the **Configuration** tab.
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 *ArcSight 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.
- **Locally**: you can use EnterpriseView as the primary asset management system of your organization and build a business model within EnterpriseView.

To import a business model

1. Follow the instructions in the *Synchronize Assets with External Asset Repository* section in the *ArcSight EnterpriseView Deployment Guide*.
2. During the first import, all imported assets are saved as **Unattached**. Follow the instructions in "Connect an Asset to Business Model" (on page 15). 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. In EnterpriseView, 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 11).
2. Create the business model.
   a. In EnterpriseView, click **Assets > Asset Profiling**.
   b. On the **Asset Profiling** window, click the **New** tab. The predefined **My organization** asset icon is displayed in the graph area.
   c. Click the **My organization** asset, and enter a **Name** and **Description** in the right pane.
   d. Follow the instructions in "Create an Asset" (on page 14) 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.

To create an asset

1. In EnterpriseView, click **Assets > Asset Profiling**, and then, on the left pane, click the **New** tab.
2. Do one of the following:
   - From the left pane, drag the asset type that you want to create and connect to the business model and drop it on the containing asset in the graph area.

     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 graph area. The following business model is created:

   - In the left pane, select the asset that you want to create and connect to the business model. In the business model, select the containing asset to which you want to connect the new asset, and then click the **Create and Connect** button.
3. In the right pane, enter the properties for the asset that you just created, and then click **Save**. For a detailed description on asset properties, see "Asset Properties" (on page 19).

Connect an Asset to Business Model

You can connect assets, both attached and unattached, to the business model. 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.

To connect an asset to the business model

1. In EnterpriseView, click **Assets > Asset Profiling**, and then, on the left pane, click the **Unattached** tab.
2. Do one of the following:
   - In the left pane, from the list of **Unattached** assets, select the asset that you want to connect to the business model. In the business model select the containing asset to which you want to connect the unattached asset, and then click the **Connect**  button.
   - From the left pane, drag the asset that you want to connect to the business model, and drop it on the containing asset to which you want to connect in the graph area.

     You can also search for the asset that you want to connect, as described in "Search for an Asset" (on page 16).

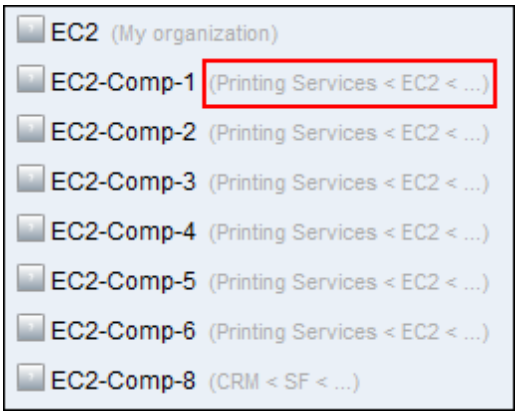
Search for an Asset

You can search for a name or a partial name of any asset.

To search for an asset

1. In EnterpriseView, 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 containing assets are displayed next to each asset that is found.



Disconnect an Asset from the Business Model

When you disconnect an asset from the business model, the relation between the asset and its containing (parent) asset is deleted. Only relations 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 containing asset, then it remains in the business model.) If you disconnect an asset that contains other assets, then that asset and its contained assets remain intact.

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

To disconnect an asset from the business model

1. In EnterpriseView, click **Assets > Asset Profiling**.
2. Search for the asset that you want to disconnect, as described in "Search for an Asset" (on page 16) or, on the left pane, click the **Organization** tab and do one of the following:
   - Expand the business model tree in the left pane to locate the asset that you want to disconnect by clicking the  button.
   - Expand the business model graph to locate the asset that you want to disconnect by double-clicking the assets in the graph.
3. Click the asset that you want to disconnect, and then click the **Disconnect**  button.

   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. In EnterpriseView, click **Assets > Asset Profiling**.
2. Search for the asset that you want to delete, as described in "Search for an Asset" (on page 16) or on the left pane, click the **Organization** tab and do one of the following:
   - Expand the business model graph to locate the asset that you want to delete by double clicking the assets in the graph.
   - Expand the business model tree in the left pane to locate the asset that you want to delete by clicking the  button.
3. Click the asset that you want to delete and then click the **Delete**  button, or select the asset in the graph and press **DELETE**.

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

Asset Properties

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

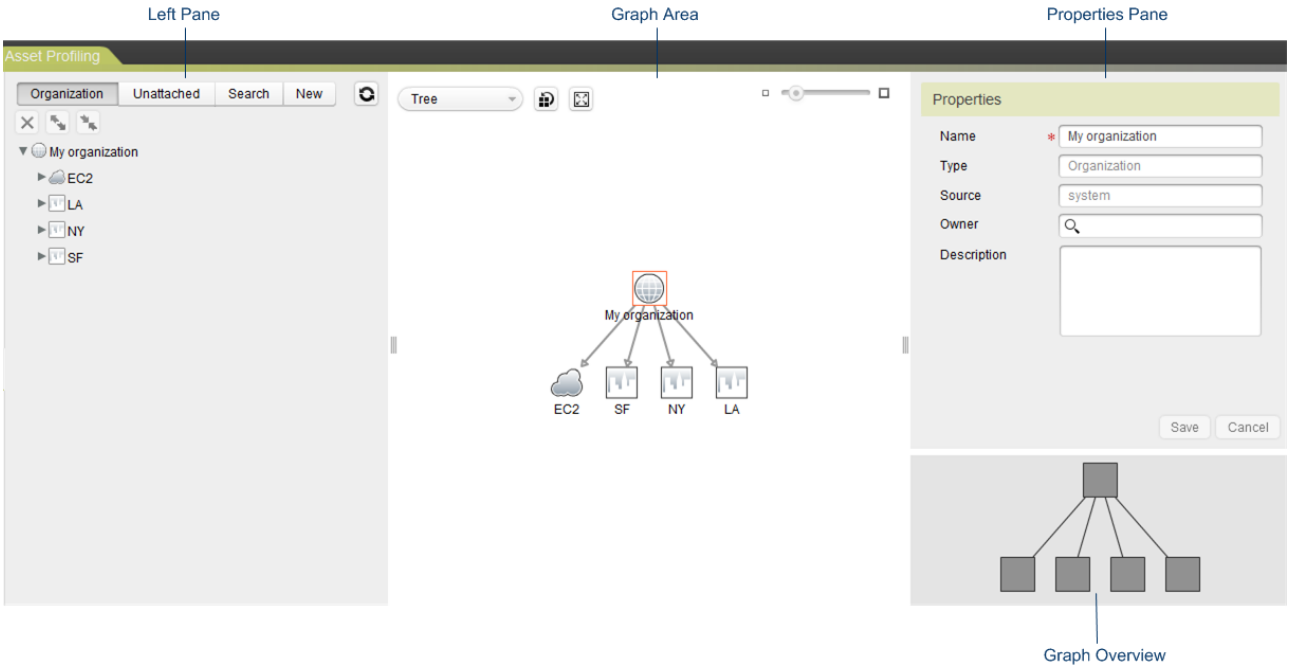
Asset Properties

Category	Property	Description
General	**Name** (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**. The source name for assets created in EnterpriseView is empty. 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**	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.
	Country	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. 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 and risk aggregation are done. For more information, see "Weights and Criticality Level" (on page 55) and "Risk Score Aggregation Mechanism" (on page 75).
Business	**Criticality Level**	See description above.
	Value	A numeric, monetary value.

Category	Property	Description
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.

Asset Profiling Window

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



Graph Area

UI Element	Description
<Graph Layout>	You can display the business model in one of the following layouts: • **Tree** tree-structured graph • **Circular** interconnected ring and star topology • **Incremental** highlights the direction or flow within the graph • **Organic** based on a force-directed layout paradigm • **Balloon** positions the sub-trees of a node in a radial fashion around that node • **Generic Tree**
	**Optimize Layout** Refreshes the layout of the business model in the graph.
	**Fit to Window** Resizes and displays the entire business model in the Graph Area.
	Zoom in/zoom out business model.

Left Pane

UI Element	Description
Organization tab	The Organization tab displays the EnterpriseView business model.
	**Disconnect** Clicking this button deletes the relation between the asset and its containing (parent) asset. If the contained asset has only one containing asset, then the asset is disconnected from the business model. The asset itself is not deleted; it is saved as **Unattached**. If you disconnect an asset that contains other assets, then the disconnected branch and its relations remain intact. You can delete only relations created in EnterpriseView.
	**Delete** Deletes the selected 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.
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.
	**Connect** Connects the asset that you have selected from the list of assets in the left pane to the asset selected in the business model. Available in the **Unattached** tab and in the **Organization** tab.
Search tab	You can search for a name or a partial name of any asset in EnterpriseView, connected to the business model or unattached.
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.
	**Create and Connect** Creates a new asset according to the type that you have selected in the left pane and connects it to the selected asset in the model.
	**Refresh** Refreshes the business model to display any changes that might have occurred due to synchronization with an external asset repository. Available in all tabs.

Properties Pane

UI Element	Description
<Asset properties>	See "Asset Properties" (on page 19)
Save	Click to save any changes that you have made to the asset properties.
Cancel	Click to cancel any changes that you have made to the asset properties.

Graph Overview

When the business model is expanded to a larger size than the graph area, you can navigate it by clicking and dragging in the Graph Overview area.

Chapter 4

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 and PCI PSS v2.0, as well as 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 CobiT, NIST ,and ISO/IEC 27001, allowing you to assess once and comply with many. For more information, see "About Unified Compliance Framework" (on page 26).

  EnterpriseView Policy Builder includes a highly configurable policy template for defining in-house policies, as described in "How to Create a Policy" (on page 28). 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 Policy Settings" (on page 27).

- **Policy Mapping**

  EnterpriseView policy mapping capability allows 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.

- **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 32). 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 allows 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 33).

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 49).

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

- **Assessment Aggregation**

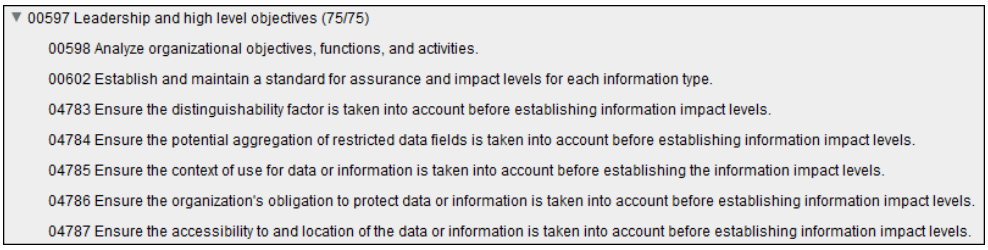
  Policy audits can be performed on lower-level assets and then trickled up and aggregated to top-level assets, providing a business centric analysis of security risk and policy compliance. For more information, see "Control Scores Aggregation Mechanism" (on page 50). Assessments can also be overridden for specific assets, as described in "Restore Aggregated Scores" (on page 34).

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 CobiT, NIST ,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 CobiT, NIST ,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 32) and for reporting purposes.
Main Security Category	**Impact Zone**	UCF includes impact zones, such as: • Leadership and High Level objectives • Audit and Risk Management • Product Design and Development • Acquisition of Technology • Operational Management • Human Resources Management • Records Management • Technical Security

EnterpriseView	UCF	Additional Information
		• Physical Security • Systems Continuity • Monitoring and Reporting • Privacy • 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**	

Configure Policy Settings

You can configure the control maturity and control compliance score range via the Policy Settings dialog box.

To define maturity and compliance score ranges

1. In EnterpriseView, click **Policy and Compliance > Policy Builder**, and then, on the upper right side of the left pane, click the **Policy Settings**  button.
2. On the **Policy Settings** dialog box, click one of the following:
   - **Maturity Score Ranges**
   - **Compliance Score Ranges**
3. Drag the slider to define the ranges for maturity or compliance score, and then click **Save**.

How to Create a Policy

EnterpriseView includes the Unified Compliance Framework, as described in "About Unified Compliance Framework" (on page 26). 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, as well as 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, the template can be modified 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 page 29).

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. In EnterpriseView, click **Policy and Compliance > Policy Builder**.
2. On the **Policy Builder** page, click **Create Policy**.
3. On the **Settings** 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 "Settings Tab" (on page 40).

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. Add a Main Security Category. For more information on policy attributes, see "Settings Tab" (on page 40)). In the left pane, click the **New Main Security Category**  button, 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 "Settings Tab" (on page 40). 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:

- Via the **Settings** tab of a specific policy. This option is recommended when you want to create a policy and immediately activate it.
- Via the **Policy Administration** dialog box. This option is recommended for managing the state of all the policies in EnterpriseView.

To activate a policy via the Settings tab

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 via the Policy Administration dialog box

1. In EnterpriseView, click **Policy and Compliance > Policy Builder**.
2. On the top right side, click **Administration**.
3. On the **Policy Administration** dialog box, 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 **OK**.

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. In EnterpriseView, 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.

If you delete a policy that includes controls that are already assigned to an asset, whether the control is applied to the asset or not, then the assignment and any related assessment, is deleted.

If you delete a policy that is mapped to another policy, then these mappings are deleted, as well.

To delete a policy

1. In EnterpriseView, 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 the **Delete Policy**  button.
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 (contained) 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. In EnterpriseView, 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 16).
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 (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.

   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 26). Enter the name of the authority document in the **Filter by authority document** box. The results are filtered accordingly.
4. 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 containing 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 contained assets.

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

To override control applicability

1. In EnterpriseView, 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 16).
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**: Compliance with a policy control.

Both scores are automatically aggregated to higher-level assets. For more information, see "Control Scores Aggregation Mechanism" (on page 50). Aggregated scores can be overridden. If you have manually overridden a score that was applied automatically, you can restore the aggregated score, as described in "Restore Aggregated Scores" (on page 34).

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 44).

To audit an asset

1. In EnterpriseView, 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. Or search for the asset by entering its name. Click **OK**.

   The policies that are relevant to this asset (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. You can review "P5 Control Maturity Model Guidelines" (on page 49) 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 41).

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

6. Click **Save**.

   The maturity score is calculated, as well as 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 44).

   The **Maturity Score**, **Compliance Score** and the **Maturity Progress** are trickled up and aggregated to higher-level assets per applied control. Their values are displayed in the left pane in the asset tree. For more information, see "Control Scores Aggregation Mechanism" (on page 50).

Restore Aggregated Scores

You can restore the aggregated score on a specific control on a specific asset, for any score that you have manually overridden. The score is restored according to the logic described in "Control Scores Aggregation Mechanism" (on page 50).

To restore aggregated scores

1. In EnterpriseView, 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 (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 **Restore 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. For more information on mapping policy controls, see "Map Controls" (on page 35).

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 while compliance reports are generated for a target policy and vice versa.

When assets are being assessed by auditors, if a control is mapped to another control and both controls 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.

Map Controls

You can map controls between policies. For an overview of this feature, see "Policy Mapping" (on page 35).

To map controls between policies

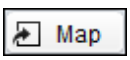
1. In EnterpriseView, click **Policy and Compliance > Policy Mapping**.
2. In the **Source Policy** pane, from the **Select a policy** drop-down list, select a source policy.

   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 

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.

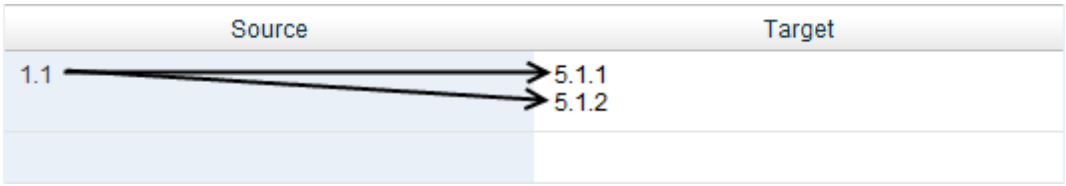
   Note: You cannot add controls to the **Mapped Controls** table until both **Source Policy** and **Target Policy** are selected.
5. From the **Target Policy** pane, from the list of controls, select the control that you want to map, and drag it to the **Target** column in the **Mapped Controls** table that reads "**Drag here**". Or click the 

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. In EnterpriseView, 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. In EnterpriseView, 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 a Mapping

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. In EnterpriseView, 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 page 36).
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 allows you to map controls between a source policy and a target policy. For more information, see "Policy Mapping" (on page 35)). The different areas and the functionality available in each is described in the following sections.

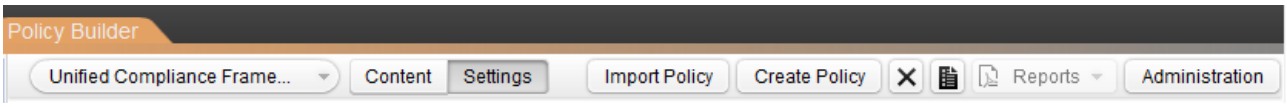
UI Element	Description
Map	Click this button to add the selected control to the **Associated Control** table. This button is only enabled when both a source policy and a target policy are selected and when an unmapped control in the source policy is selected. You can also drag and drop controls to the **Mapped Controls** table. For more information, see "Map Controls" (on page 35).
Details	Click a control and then click this button to display the control details.
<**Search Controls**>	This page provides three different search options: • **Search Source Controls**. Search within the list of controls that belong to the source policy, both mapped and not mapped. • **Search Target Controls**. Search within the list of controls that belong to the target policy, both mapped and not mapped. • **Search Associated Controls**. Search for controls that are already mapped, from the **Mapped Controls** pane. For more information, see "Search for Controls" (on page 36).
	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 a Mapping" (on page 36).

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. 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** 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** 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.

Policy Builder Window

The Policy Builder window allows 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 functionality available in each is described in the following sections.

Policy Toolbar

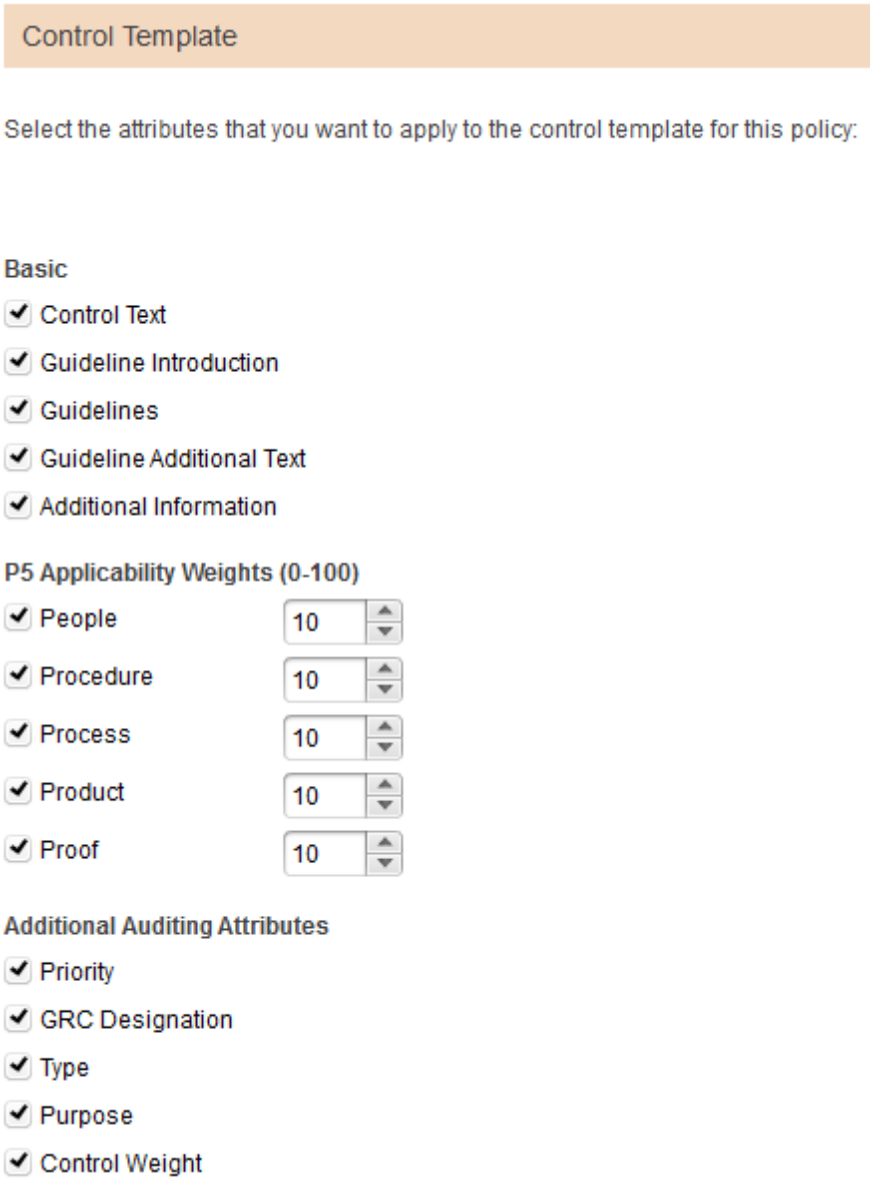


UI Element	Description
<Policy drop-down>	Select a policy from the drop-down.
Content tab	See "Content Tab" (on page 42) below.
Settings tab	See "Settings Tab" (on page 40) below.
Import Policy	Click this button to import a policy. For more information, see "Import a Policy" (on page 30).
Create Policy	Click this button to create a new policy. For more information, see "How to Create a Policy" (on page 28).
	**Delete Policy** Click this button to delete a policy. This button is disabled if the assessment process has begun (meaning that at least one control that is applied to an asset is assessed). **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.
	**Policy Settings** Click this button to configure the control maturity and control compliance score range. The control maturity score range and compliance score range affect the risk acceptance level.
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.
Administration	**Administration**

UI Element	Description
	Click this button to activate or deactivate policies.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. For more information, see "Activate a Policy" (on page 29).

Settings Tab

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

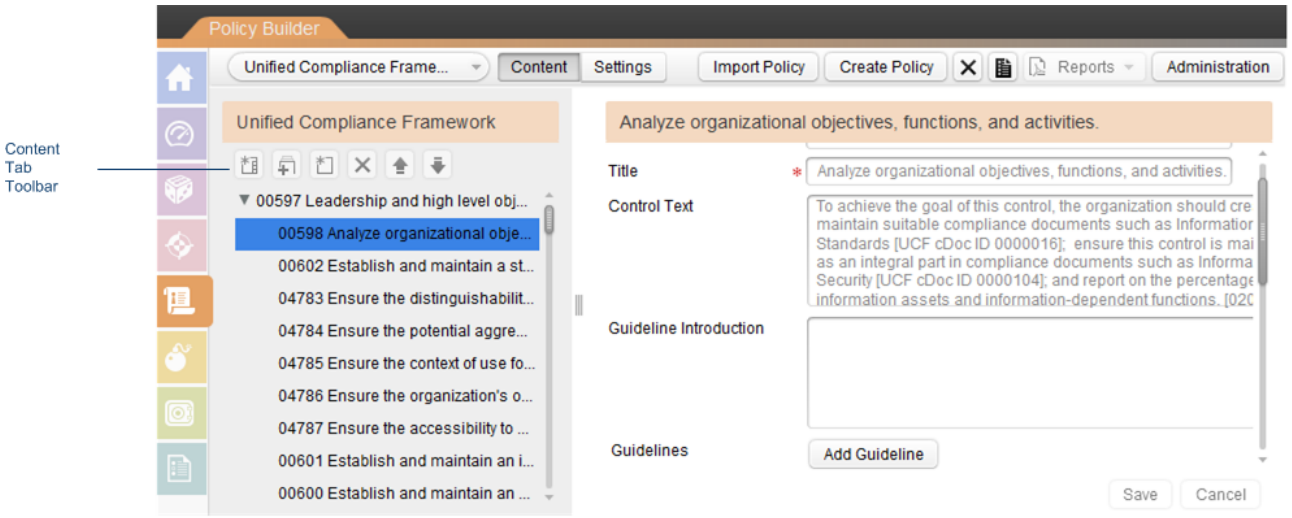


UI Element	Description
Control Text **Guideline Introduction** **Guidelines** **Guideline Additional Text** **Additional Information**	The **Basic** attributes include content elements. Selecting an attribute adds a text box to the control in which you can add content. For example, if the control has numerous guidelines, you can select the **Guidelines** attribute. 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. 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. 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. 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 28).
Priority	You can prioritize controls by selecting this check box. The following priorities can be applied: • **Low** • **Medium** • **High**
GRC Designation	You can categorize the controls according to the following criteria: • **Regulation** • **Legal Status** • **Standards** • **Threats**
Type	You can further categorize the controls according to the following criteria: • **Management** • **Technical** • **Operations**
Purpose	Additional segmentation according to purpose:

UI Element	Description
	• **Confidentiality** • **Integrity** • **Availability** • **Audit** • **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 55). 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.



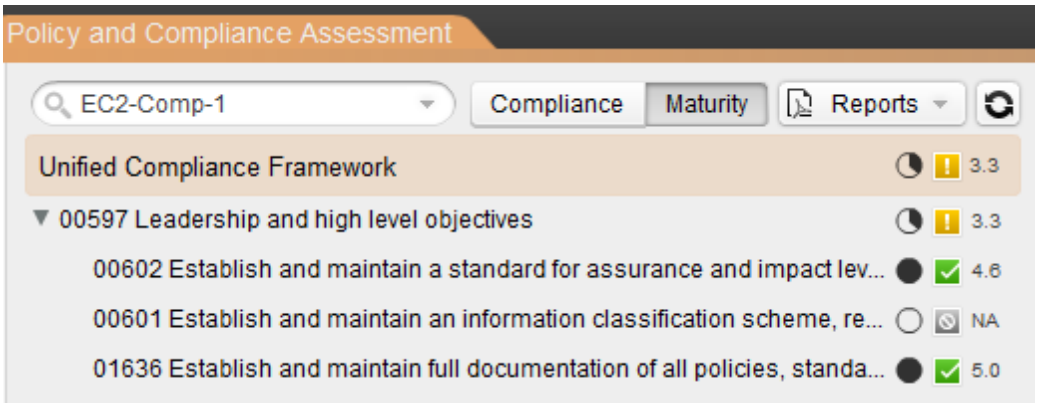
UI Element	Description
	**New Main Security Category** A Security Category lets you group controls with common characteristics. Examples of security categories in ISO can be: Asset Management, Risk Assessment and Treatment, and Security Policy. Examples of security categories in COBIT can be: Plan and Organize, Acquire and Implement. A Main Security Category is the first level in a policy; you cannot add controls to a policy without first defining their security category. Click this button to create a new Main Security Category. In the right pane, enter the security category information.

UI Element	Description
	**New Security Category** 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. 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.
	**New Control** 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. Click the security category to which the control belongs, and then click this button. In the right pane, enter the control information.
	**Delete** Deletes a Main Security Category, Security Category, or Control.
	**Move Up** Changes the order of any one of the following items in the policy tree: • **Main Security Category** within a policy • **Security Category** within a policy or within another security category • **Control** within a security category. In order to move a control between security categories, you need to drag and drop the control.
	**Move Down** See Move Up.

Policy Assessment Window

The Policy Assessment window allows you to audit assets by assessing the control maturity and asset compliance with a control, per asset. The different areas and the functionality available in each is described in the following sections.

Left Pane

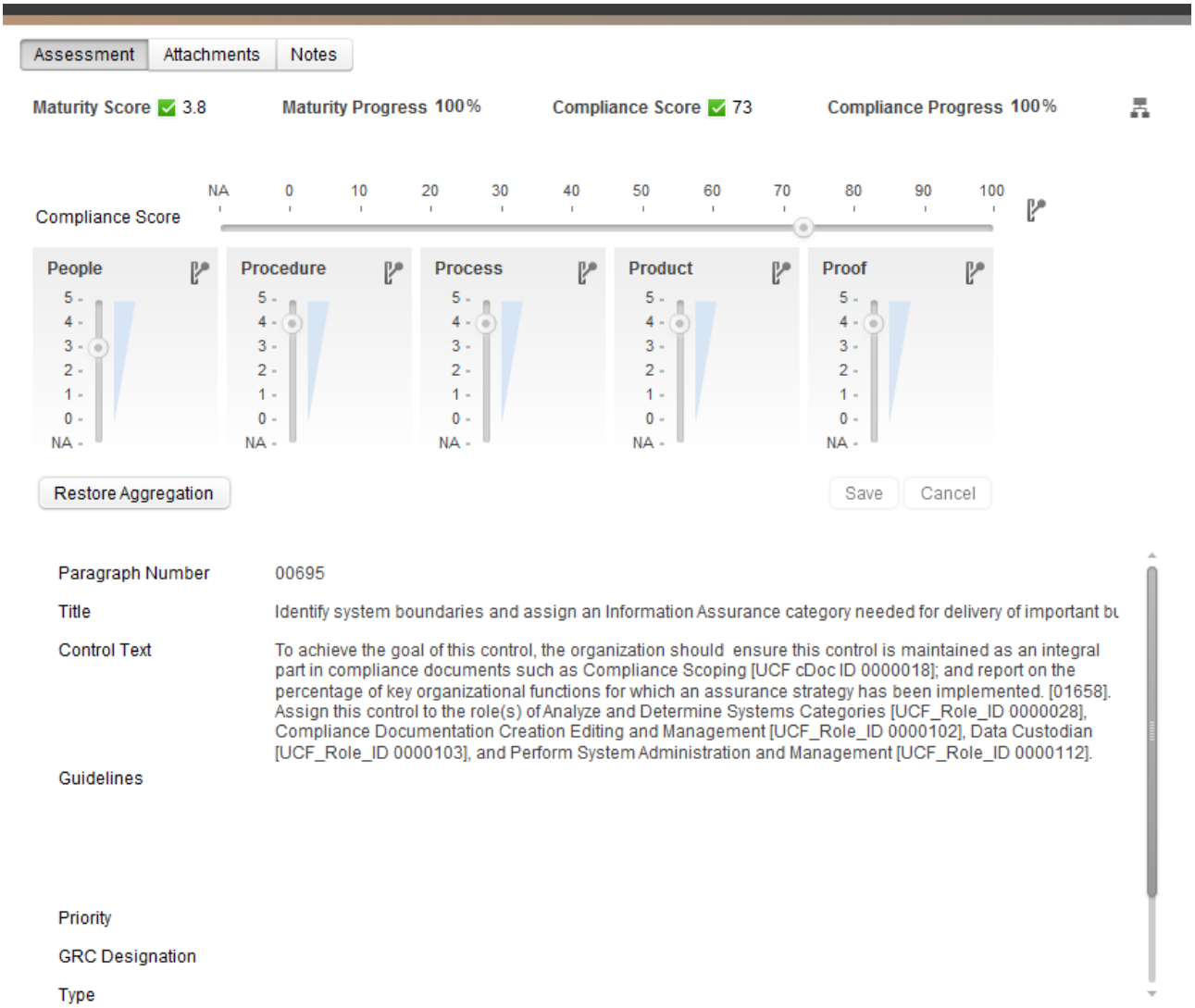


UI Element	Description
Select an asset	Select the asset that you want to assess from this drop-down list or search for an asset by entering its name.
Compliance Tab/ **Maturity Tab**	Displays information about the asset, per policy element (controls and security categories). The **Compliance** tab displays compliance information and the **Maturity** tab displays control maturity information.
	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 50).
<Score Range>	The score range for a specific policy element is indicated by one of the following icons: High score Medium score Low score The ranges are determined in "Configure Policy Settings" (on page 27). The actual score is displayed next to this icon.

UI Element	Description
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.
	Refresh Refreshes the policy and its elements to display assessment changes.

Right Pane

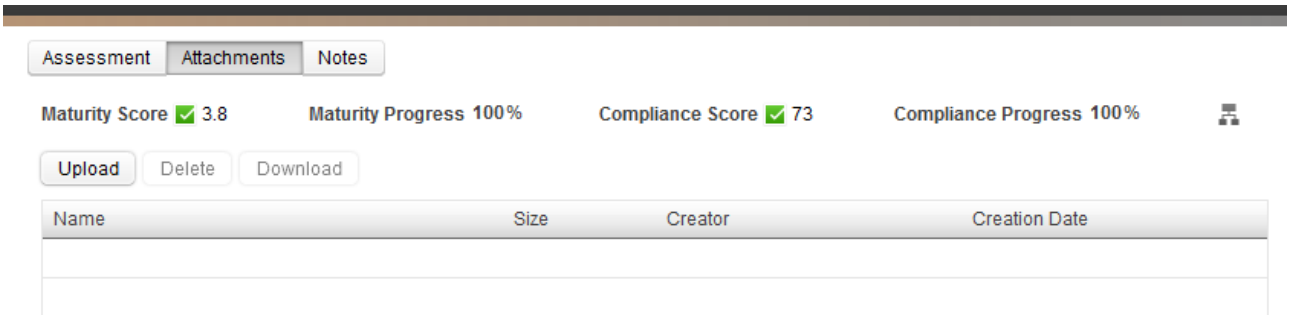
Assessment Tab



UI Element	Description
<Control Data>	Control data includes the following: • **Maturity Score** and score range icon (high, medium, low) 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 below. • **Inherited from: <asset>**  Indicates from which higher level asset the applicability of this control was inherited.
<P5 Maturity Score Slider>	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 49).
Compliance Score	This number defines how compliant the asset is with the control. Use the slider to select a score between 0 and 100. For more information, see "Audit Assets" (on page 33). 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.
	**Score Applied Manually** This icon indicates that a score was applied manually. It is applied

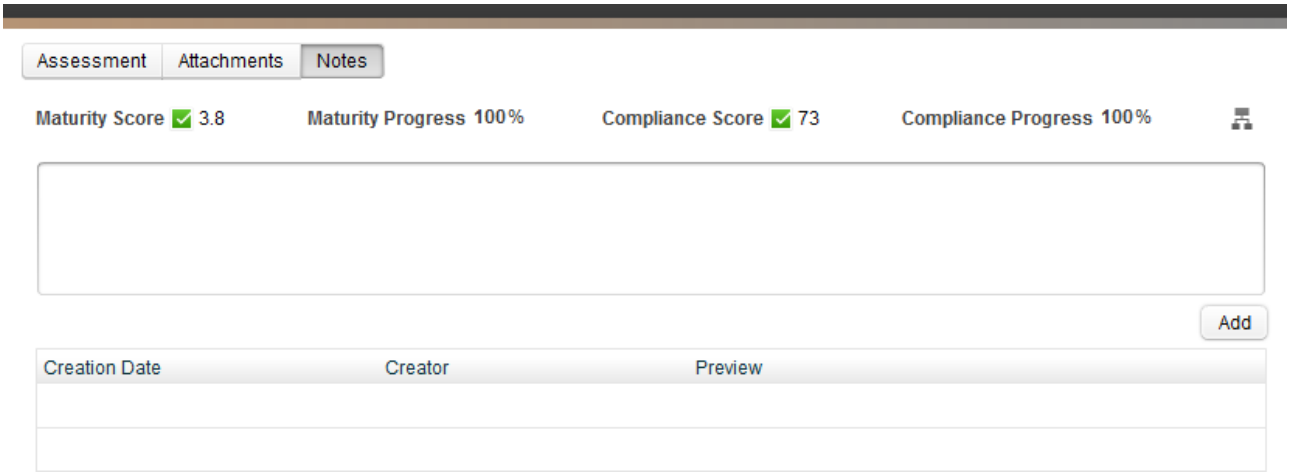
UI Element	Description
	only to the scores that have been changed.
Restore Aggregation	This button is enabled only when scores on the specific control are manually assessed. If you have made manual changes to aggregated scores, you can click this button to restore scores that have been aggregated from lower-level assets.

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, containing assets get the aggregated compliance score, control maturity score, compliance assessment progress and maturity assessment progress from their contained assets, per 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. The compliance of an asset with a specific control.
Control Maturity Score	Measured as a score between 0-5. 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, 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 containing 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.

Compliance Score

A containing asset gets the average compliance score of all its contained assets, on a specific control.

$$\frac{\sum(Compliance\ Scores)}{\sum(Contained\ Assets)}$$

For example:

For control X

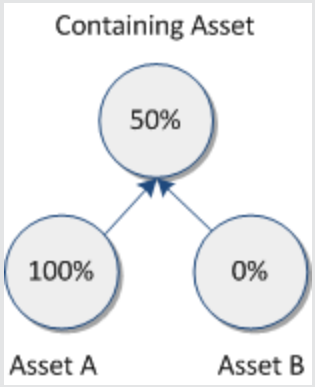
If

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

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

Then

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



Control Maturity Score

Aggregation is done in two steps:

1. A containing asset gets the average score for each P5 maturity factor of all its contained assets.
2. The final control maturity score is the weighted average of the P5 maturity factor scores.

For example:

For control X

If

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

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

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

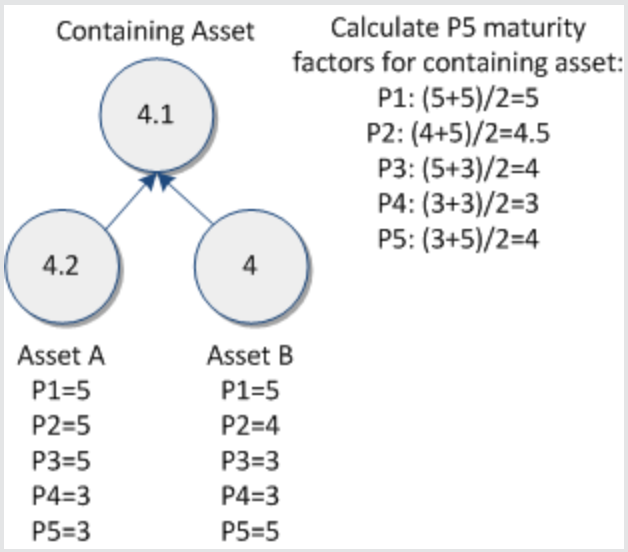
People=5, Policy/Procedure=4, Process=3, Product=3, Proof=5

Then

The containing 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**



Aggregation on Policy Level

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

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 19).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 contained asset A: Compliance Score= **100**, Criticality Level=**1**

  For contained asset B: Compliance Score =**10**, Criticality Level=**2**

  Then

  Compliance Score for containing asset=**40**

  Calculation: $\frac{(100 * 1) + (10 * 2)}{(1 + 2)}$

- **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 42).

  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: $\frac{(10 * 100) + (100 * 50)}{(100 + 50)}$

Chapter 5

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 is 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 60).

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, as well as 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 Threat Library Settings" (on page 57). 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 63).

Threats can be applied to top level assets and trickled down to all lower level assets that belong to that hierarchy. Analyzed data is displayed in numerous forms,such as the "Risk Register" (on page 117).

Configure Threat Library Settings

You can configure basic risk assessment parameters in the Threat Library Settings dialog box.

To apply weights to categories and actors

1. In EnterpriseView, click **Risk Modeling > Threat Library Builder**.
2. On the **Threat Library Builder** window, in the left pane, click the **Threat Library Settings** button.
3. On the **Threat Library Settings** dialog box, click **Actor Weights**.
4. In the right pane, 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.
5. Enter a weight between 0 and 100.
6. Click **Save**.

> **Note:** You can override these settings for a specific asset, as described in "Configure Asset Risk Settings" (on page 59).

To manage impact area settings

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

1. In EnterpriseView, click **Risk Modeling > Threat Library Builder**.
2. On the **Threat Library Builder** window, in the left pane, click the **Threat Library Settings** button.
3. On the **Threat Library Settings** dialog box, click **Impact Area**.
4. Do one of the following, and then click **Save**.
   - To add an impact area, in the right pane, click the **Create new impact area** 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, in the right pane, click the **Delete impact area** button.

     A confirmation message is displayed. Click **Yes** to confirm.
   - To apply a weight to an impact area, click the weight to make it editable, and enter a weight between 0 and 100.

To define probability ranges

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

1. In EnterpriseView, click **Risk Modeling > Threat Library Builder**.
2. On the **Threat Library Builder** window, in the left pane, click the **Threat Library Settings**  button.
3. On the **Threat Library Settings** dialog box, click **Probability Ranges**.
4. In the right pane, drag the slider to define the ranges for probability, and then click **Save**.

To define risk score ranges

1. In EnterpriseView, click **Risk Modeling > Threat Library Builder**.
2. On the **Threat Library Builder** window, in the left pane, click the **Threat Library Settings**  button.
3. On the **Threat Library Settings** dialog box, click **Risk Score Ranges**.
4. Drag the slider to define the ranges for inherent and residual score risks, and then 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. In EnterpriseView, 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**.

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 66).

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" (on page 60).
2. If the operation required for this threat does not exist in the threat library, follow the instructions in "Create an Operation" (on page 61).
3. "Connect Actor to Operation" (on page 62).

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. 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. 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. 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. In EnterpriseView, click **Risk Modeling > Threat Library Builder**.
2. On the **Actor** 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 **Actor** 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. In EnterpriseView, 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. In EnterpriseView, click **Risk Modeling > Threat Library Builder**.
2. On the **Operation** tab, click the **New Operation** button.

3. On the **Operation** 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

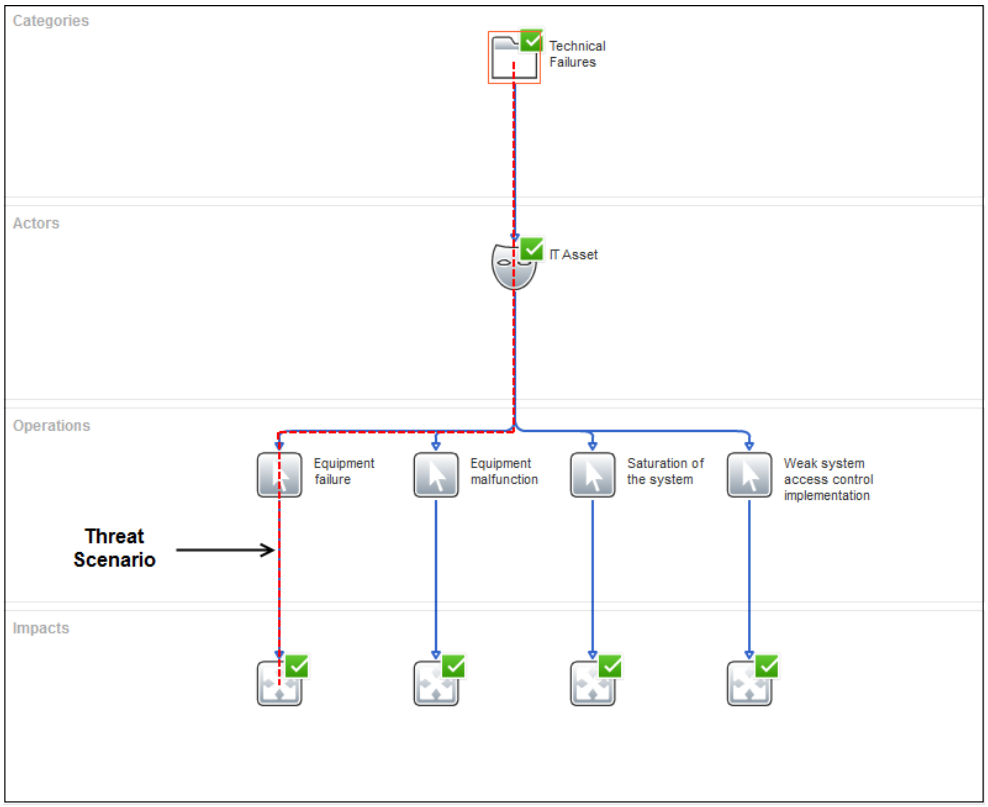
1. In EnterpriseView, click **Risk Modeling > Threat Library Builder**.
2. On the **Actors** tab, from the actors tree, locate the required actor. To expand the actors tree, click  next to the category. Drag the actor to which you want to connect an operation to the graph area. If the actor already has operations that are connected to it, they are displayed in the graph 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 graph area.

   The operation is connected to the actor and is displayed in the **Operations** section in the graph 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" (on page 63) and then "Apply Risk to Asset" (on page 64).

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. In EnterpriseView, 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 graph area.

   The threat is displayed in the **Associated Threats** area and in the graph 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 graph 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. In EnterpriseView, 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 "Risk Score Calculation" (on page 73).

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 117). For more information on the risk score aggregation mechanism, see "Risk Score Aggregation Mechanism" (on page 75).

To apply risk to an asset

1. In EnterpriseView, 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 graph area, in the **Impacts** section at the bottom, click the impact icon.

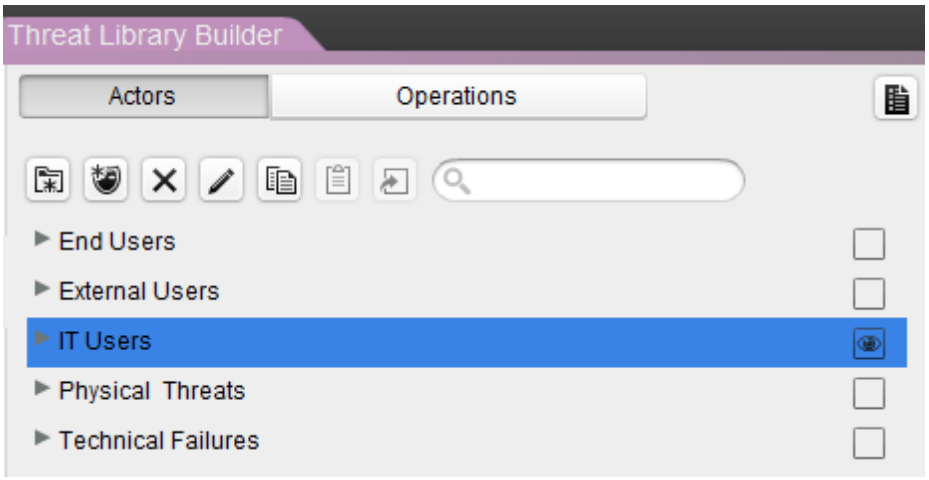
   The risk **Properties** pane is displayed.
5. On the **Properties** pane, do the following, and then click **Save**.
   a. In the **Probability** box, enter a number between 0 and 1, up to two places after the decimal point. For example, 0.5.
   b. In the **Impact Areas** table, click inside the **Value** cell of each impact area and select **Low**, **Medium** or **High** to represent the impact of each area.

   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 "Risk Score Calculation" (on page 73).

Threat Library Builder Window

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

Left Pane



UI Element	Description
	**Threat Library Settings** You can configure basic risk assessment parameters via the Threat Library Settings dialog box, such as: • Apply weights to categories and actors • Manage impact areas • Define probability ranges • Define risk score ranges For more information, see "Configure Threat Library Settings" (on page 57).
	**Search** 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** Click this button to create a new actor category. For more information, see "Create an Actor" (on page 60).
	**New Actor**

UI Element	Description
	Click this button to create a new actor. For more information, see "Create an Actor" (on page 60).
	**Delete** (category or actor) Select the category or actor from the actor tree, and then click this button. Deleting a category automatically deletes all of its actors. **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) 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.
 	**Copy** and **Paste** (actor) You can duplicate actors using the copy/paste functionality. Select an actor from the actor tree, and then click this 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: **Copy of <original actor name>** You can rename the actor by clicking the **Edit**  button. If the actor is connected to operations, then associations are also copied.
	**Connect Actor to Operation** Select an actor from the actors tree, click an operation on the graph, and then click this button. 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** Click this button to create a new operation. For more information, see "Create an Operation" (on page 61).
	**Edit Operation** Select the operation from the operation list, and then click this button to edit the name and description of the operation.

UI Element	Description
	**Delete Operation** Select the operation from the operation list, and then click this button. **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** 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. The operation/operations that you selected are connected to the actor and displayed in the graph area.

Graph Area

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

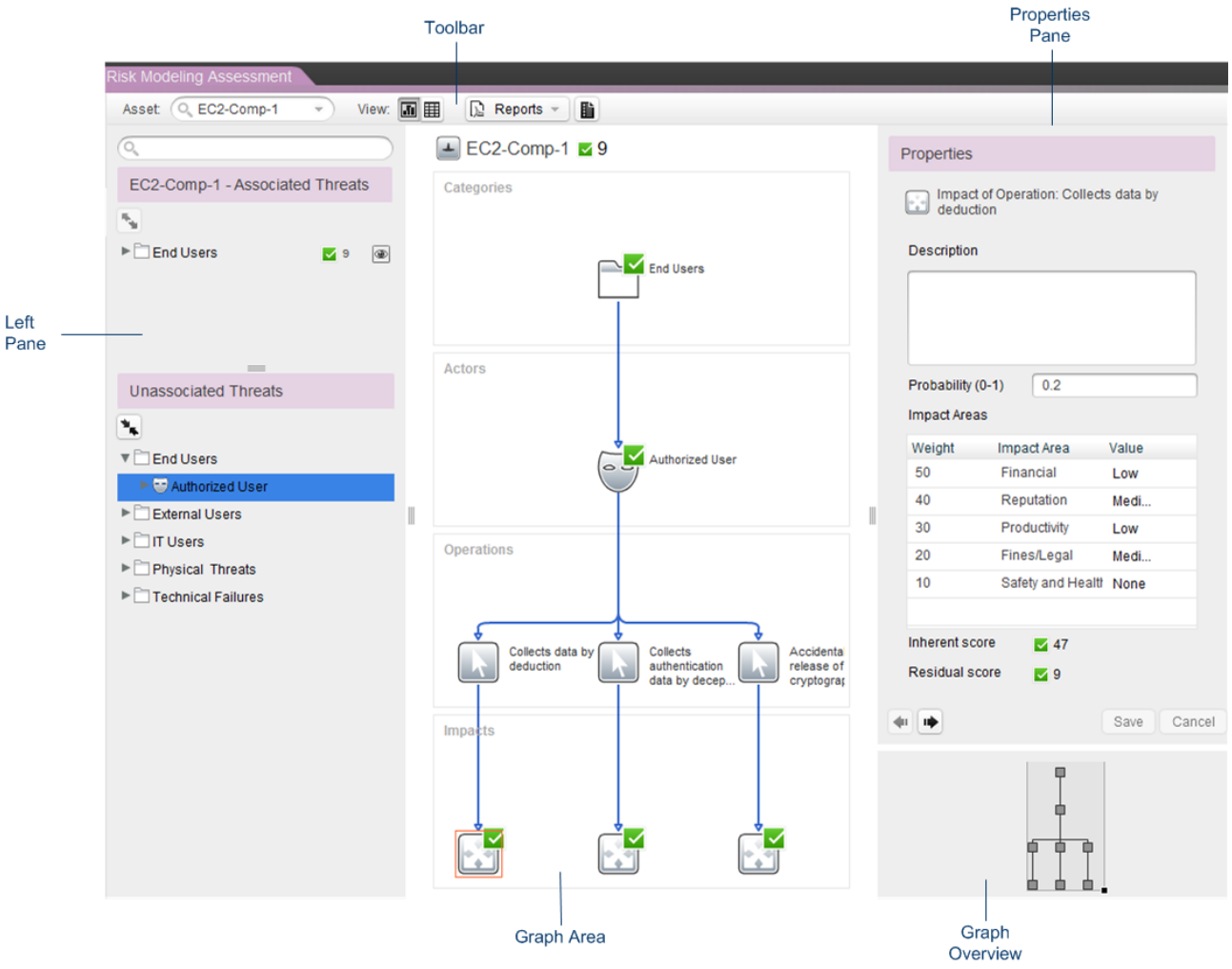
- To display threats on the graph, on the **Actors** tab, from the actors tree, drag the actors that you want to display to the graph area. You can also drag a category in order to display all of its actors and the operations connected to the actors.
- To disconnect an operation from an actor, in the graph area, click the operation that you want to disconnect, and then press **DELETE**.

Graph Overview

When a threat includes multiple operations and is larger than the graph area, you can navigate it by clicking and dragging in the Graph Overview area.

Risk Modeling Assessment Window

The Risk Modeling Assessment window allows you to create threat scenarios and assess them. The different areas and the functionality available in each is 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) In this view, the Risk Modeling Assessment window is divided into the following sections: • Left pane

UI Element	Description
	• Graph area • Properties pan • Graph overview This is the default view.
	**Table** (view) In this view, all threats are displayed in a table. You can do the following: • **Disconnect threats from an asset**. Clear the **Associated** check box. • **Edit the threat description**. • **Apply risk to an asset**. Edit the **Probability** and impact area fields.
	**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.
	**Risk Asset Settings** 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 graph area. For more information, see "Assign Threat to Asset" (on page 63).

UI Element	Description
	**Remove the selected threat from the asset** From the **Associated 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 graph area. For more information, see "Assign Threat to Asset" (on page 63).

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, as well as 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. • **Probability**: The probability that this threat will occur. Enter a number between zero and one. • **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. • **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). •  **Next Threat**  **Previous Threat**: Enabled when more that one threat is displayed in the graph area. Allows you to navigate between threat scenarios and efficiently assess risk.

Graph Overview

When a threat includes multiple operations and is larger than the graph area, you can navigate it by clicking and dragging in the Graph Overview area.

Risk Score Calculation

The "Residual Risk " (on page 65) that is applied to a threat scenario is also calculated and applied separately on the actor, actor category, and asset.

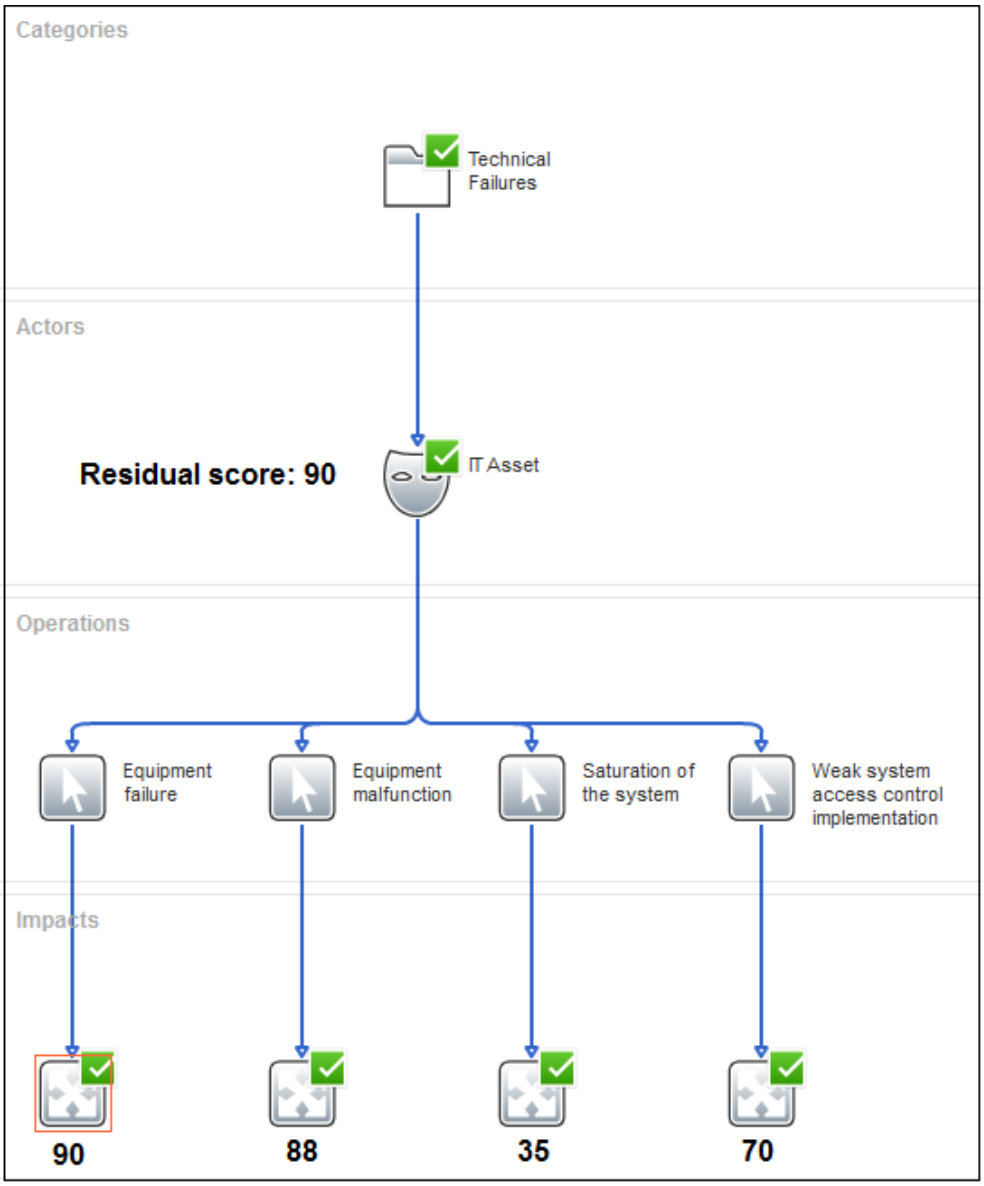
The parameters used to calculate risk score and their values are:

- **Impact Area Weight**: Between 0 and 100. Defined in the Threat Library Settings, as described in "Configure Threat Library Settings" (on page 57).
- **Impact Area Value**: **Low**=1, **Medium**=2, **High**=3.
- **Weight**: of actor or category, between 0 and 100. Defined in the Threat Library Settings, as described in "Configure Threat Library Settings" (on page 57).
- **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. The residual score is the inherent score multiplied by probability*100. $\frac{\sum(Impact\ Area\ Value * Impact\ Area\ Weight)}{\sum(Impact\ Area\ Weights * 3)} * \left(Probability * 100\right)$
Actor	The actor receives the score of the threat scenario (impact) with the highest risk.

Threat Element	Risk score calculation
	
Actor Category	The weighted average of all actor scores. $\frac{\sum(Actor\ Score\ *\ Actor\ Weight)}{\sum(Actor\ Weights)}$
Asset	The weighted average of all actor category scores. $\frac{\sum(Category\ Score\ *\ Category\ Weight)}{\sum(Category\ Weights)}$

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 "Risk Score Calculation" (on page 73).
- **Aggregated risk score**. Generally defined as the weighted average of aggregated risk scores of the contained assets of an asset, 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 "Risk Register" (on page 117).

Three methods are available for calculating the aggregated risk score:

Note: If an asset does not have contained assets, then the risk score is used instead of the aggregated risk score.

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

$$\frac{\sum(\textit{Aggregated Risk Score Contained Asset} * \textit{CriticalityLevel}) + \textit{Asset Risk Score} * \textit{CriticalityLevel}}{\sum(\textit{CriticalityLevel})}$$

- **Override**: 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 $\frac{\sum(\textit{Aggregated Risk Score Contained Asset} * \textit{CriticalityLevel})}{\sum(\textit{CriticalityLevel})}$

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

$$\frac{\sum(\textit{Aggregated Risk Score Contained Asset} * \textit{CriticalityLevel})}{\sum(\textit{CriticalityLevel})}$$

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

Chapter 6

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. 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 allows you to view vulnerabilities that affect an asset and all of its contained assets 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 and the asset "Criticality Level" (on page 19) 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

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 *ArcSight 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 one single vulnerability, in order to eliminate duplication of data, allowing you to manage the vulnerability once.

About the EnterpriseView 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, this disparity would make it difficult to identify duplicate reports, provide additional information about the vulnerabilities, and associate them with remediation actions efficiently.

To solve this problem, EnterpriseView labs creates and maintains a comprehensive vulnerability dictionary that includes all vulnerabilities, regardless of whether they have been recognized by an industry standard source. These vulnerabilities are compiled, correlated, processed and enriched, creating 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

About the Vulnerability Life Cycle

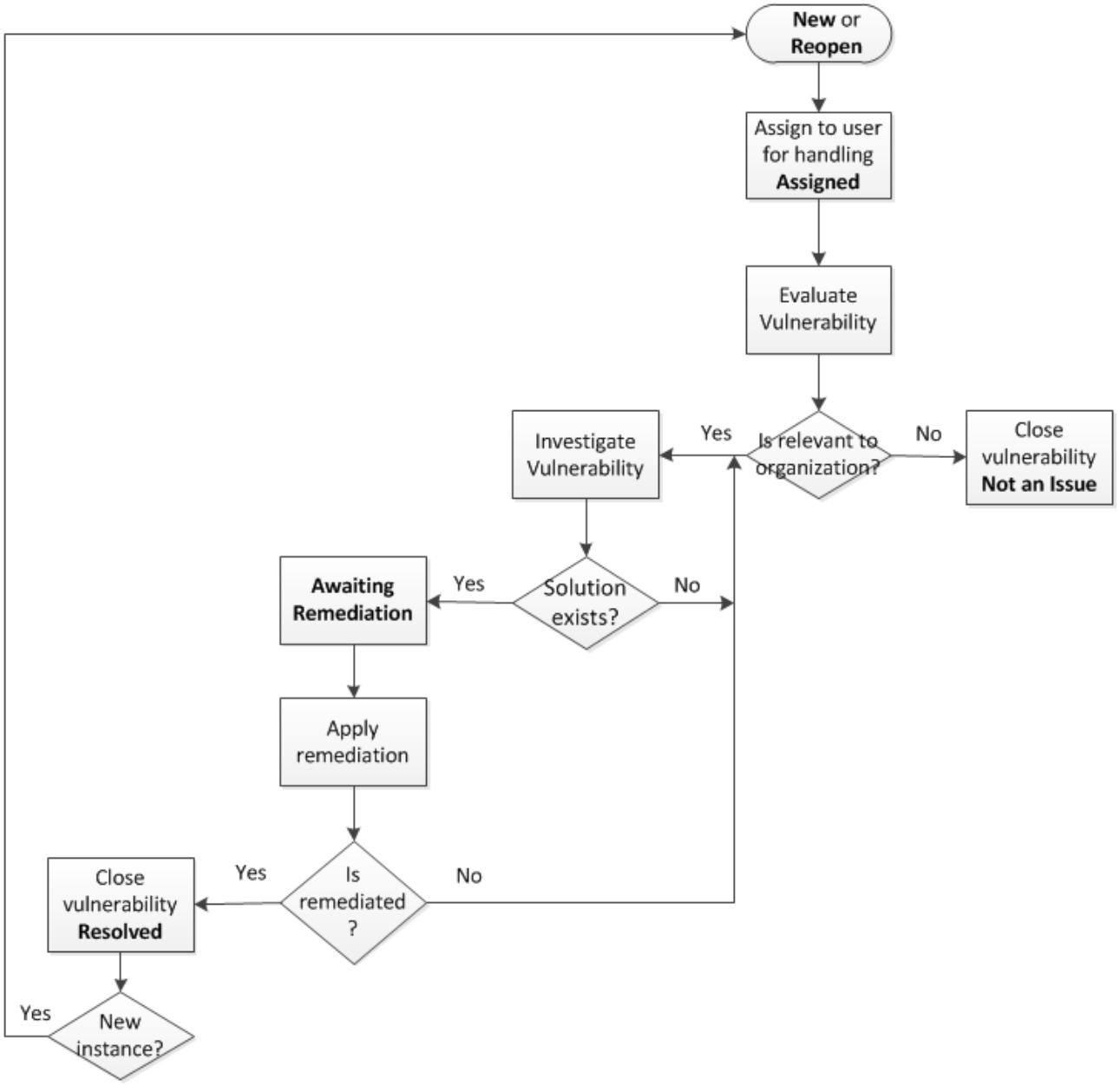
In EnterpriseView, the vulnerability life cycle is managed by using the vulnerability's "Status" (on page 82) and the vulnerability's "Remediation Status" (on page 82). Vulnerability remediation has both manual and automatic aspects. For more information on the automatic aspects, see the *About the Vulnerability Import Job* section in the *ArcSight EnterpriseView Deployment Guide*. The following example outlines how this process can be managed.

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. The user might identify the vulnerability as a non-issue, 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.
4. If the vulnerability is found to be significant, then the user investigates methods for solving the problem. The user can use the "Solution" (on page 84) parameter to help solve the problem. When the solution is found, the user changes the remediation status to **Awaiting Remediation**.
5. After the vulnerability is remediated, the user changes the vulnerability's status to **Closed** and the remediation status to **Resolved**.
6. 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.


New or Reopen
Assign to user for handling Assigned
Evaluate Vulnerability
Is relevant to organization?
Yes
No
Investigate Vulnerability
Close vulnerability Not an Issue
Solution exists?
Yes
No
Awaiting Remediation
Apply remediation
Is remediated ?
Yes
No
Close vulnerability Resolved
New instance?
Yes

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 78).

To manage the vulnerability life cycle

1. In EnterpriseView, 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 *ArcSight 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

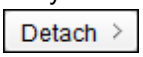
1. In EnterpriseView, click **Vulnerabilities > Assignment**.
2. On the **Vulnerability Assignment** window, in the **Assets** pane, select the asset to which you want to attach a vulnerability/vulnerabilities using either of the following methods:
   - In the **Organization** tab, expand the organization 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 were not attached to an asset during the vulnerability import process.
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 81).
4. From the **Unattached Vulnerabilities**, select the vulnerability that you want to attach to the asset, and then click the 

Attach Vulnerabilities to Asset button. 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. In EnterpriseView, 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 Vulnerabilities from Asset** 

button.

   The vulnerability/vulnerabilities are displayed in the **Unattached Vulnerabilities** pane.

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. Scores are imported from the different vulnerability scanners and are normalized to the EnterpriseView scoring system.
Status	The following options are available: • **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. • **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 *ArcSight EnterpriseView Deployment Guide*. Closed vulnerabilities do not affect the vulnerability scores of assets in the business model.
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

Property	Description
	by the organization. A vulnerability with this status will not be reopened. • **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 *ArcSight 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 81).
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.
Location	**<Hostname>:<Network Port>**
First Reported On	The date that the vulnerability occurrence was first reported, as recorded by the external source from which the vulnerability was imported. Format: Mon Day, Year 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.

Property	Description
ID	See "ID" (on page 82)

Property	Description
Related CVEs	The CVE identifiers of related vulnerabilities. Defined by EnterpriseView labs.
Host	The host where the vulnerability was found. Along with the port, comprises the "Location" (on page 83) of network vulnerabilities.
Port	The port where the vulnerability was found. Along with the host, comprises the "Location" (on page 83) of network vulnerabilities.
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.
Vulnerable Parameter	The parameter that is used to find the vulnerability. For example, User ID can be the vulnerable parameter in case of an SQL injection vulnerability.
Solution	A recommended solution for remediating the vulnerability, as provided from the vulnerability assessment tool.

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.
Scanner Type	Network.
Scanner Version	The version of the vulnerability assessment tool.
IP	IP address where the vulnerability was found.
MAC	MAC address where the vulnerability was found.

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.
- $$\mathbf{m} * \frac{\sum(\textit{Aggregated Asset Vulnerability Score} * \textit{Criticality Level}) \textit{ of top } \mathbf{n} \textit{ Contained Assets}}{\sum(\textit{Criticality Level})}$$
  - **m=Contained Assets Multiplier**: This variable is a number between 0 and 1 (inclusive) that is typically used to decrease the impact of the contained assets 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 contained assets will have a bigger impact then if you have a structure with many levels of hierarchy.
  - **n=Maximum Contained Assets in Calculation**: Sorted primarily by aggregated asset vulnerability score and secondarily by criticality level. This variable is used to decrease the impact of contained asset 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 contained assets 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 *ArcSight EnterpriseView Deployment Guide*.

The aggregated asset vulnerability score is calculated when:

- Any change is made to the Contained Asset Multiplier or to the Maximum Contained Assets 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 *ArcSight 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 "Troubleshoot Batch Jobs" (on page 129).

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

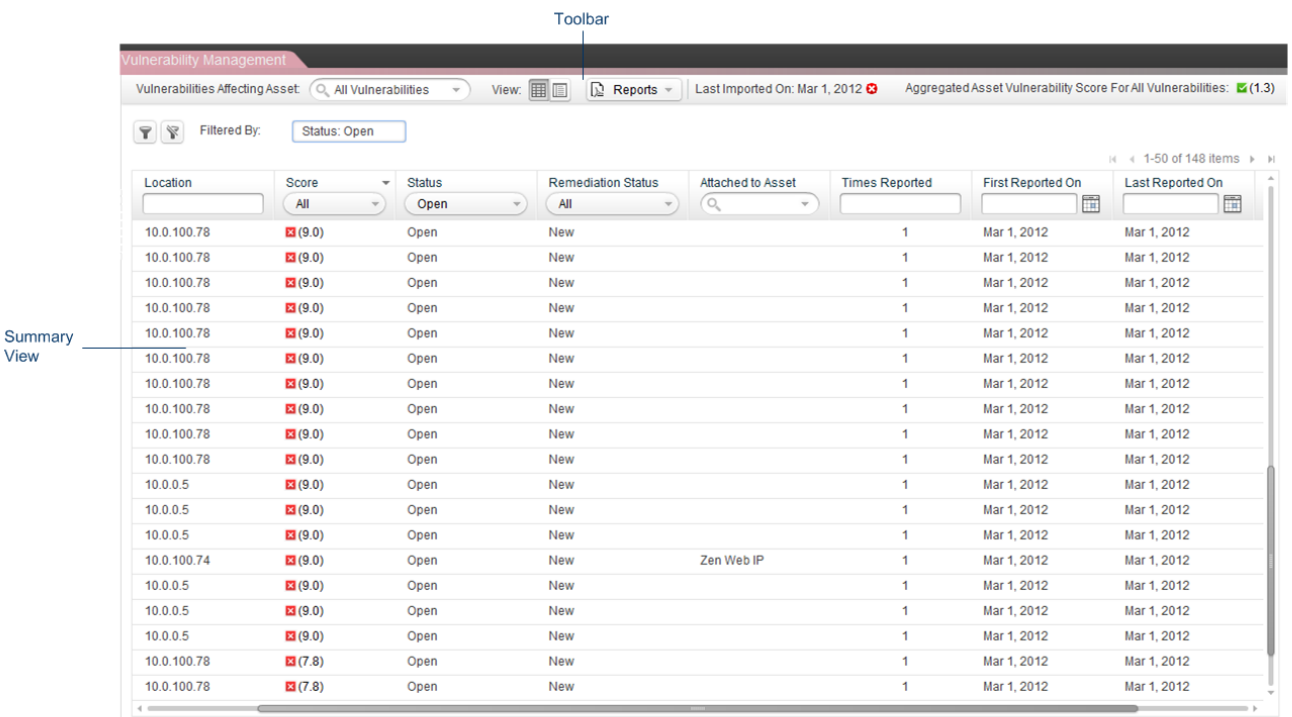
The Vulnerability Management window allows you to filter the vulnerabilities found in your organization's network using various criteria, creating views that help you manage the vulnerability life cycle. The different areas and the functionality available in each is described in the following sections.

Toolbar

UI Element	Description
Vulnerabilities Affecting Asset	Filter the vulnerabilities in the grid using one of the following options: • **All Vulnerabilities**: View all vulnerabilities, both attached to assets and unattached assets. • **Unattached Vulnerabilities**: Select this option to view vulnerabilities that are not attached to an asset. • **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 contained assets.
	**Summary View** This is the default view. For more information, see "Summary View" (on page 89). Filters are retained when passing from one view to another.
	**Details View** To open this view, select a vulnerability from the grid, and then select this view. For more information, see "Details View" (on page 90). Filters are retained when passing from one view to another.
	**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. You can generate a report for an asset, an asset and its contained assets, or for all vulnerabilities.
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: Errors. Hovering over this icon displays the following message: "The last update was completed with errors. For more information, see the redcat-vulnerability-admin.log file or contact your Administrator." Notifications (INFO). Hovering over this icon displays the following message:

UI Element	Description
	"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." For more information or error handling, see "Vulnerability Error Handling" (on page 86).
Aggregated Asset Vulnerability Score For <asset>	For more information on how this score is calculated, see "Asset Vulnerability Score Aggregation Mechanism" (on page 85).
	**Filter Vulnerabilities** 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 81). 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** Click this button to clear all the filters that you set through the **Filter Vulnerabilities** dialog box.

Summary View

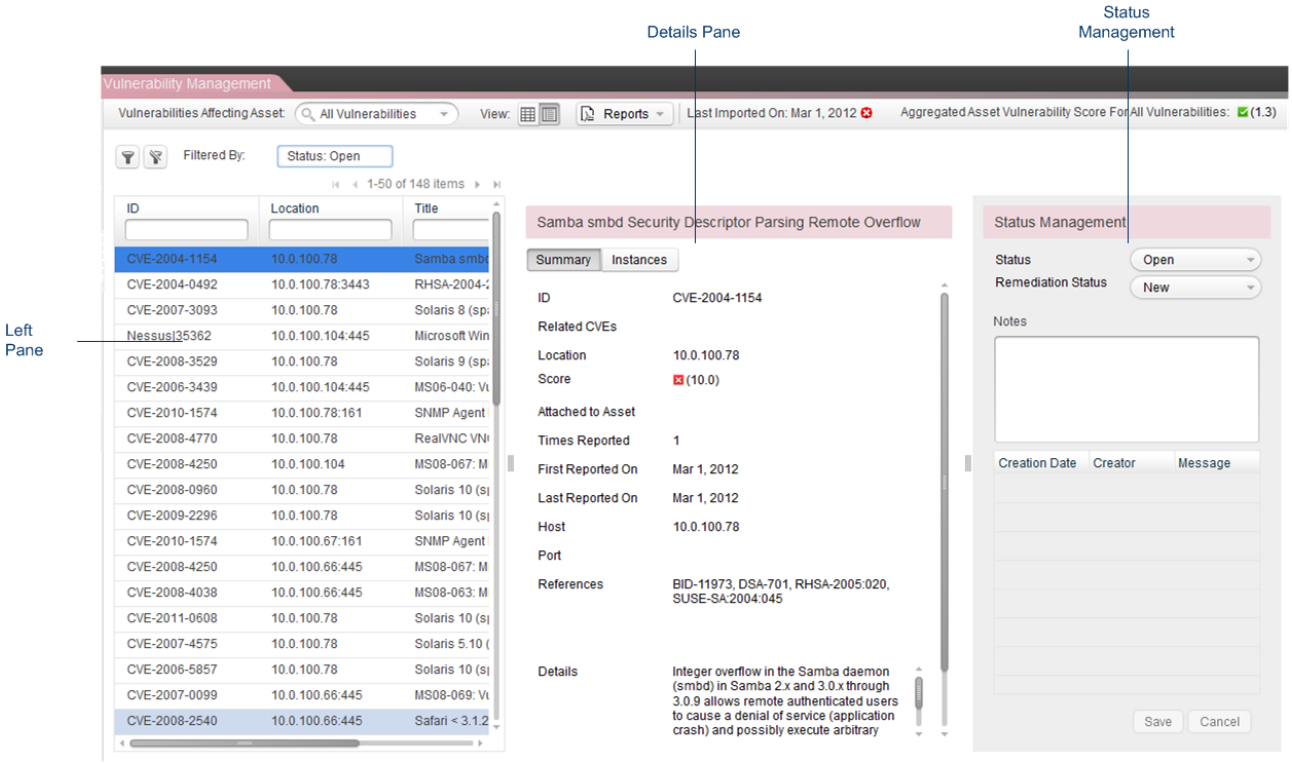


Each record in the summary view grid is an occurrence of a vulnerability in a specific location.

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 81).

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 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 83).

Instances (tab)

This tab displays the vulnerability properties described in "Instances " (on page 84).

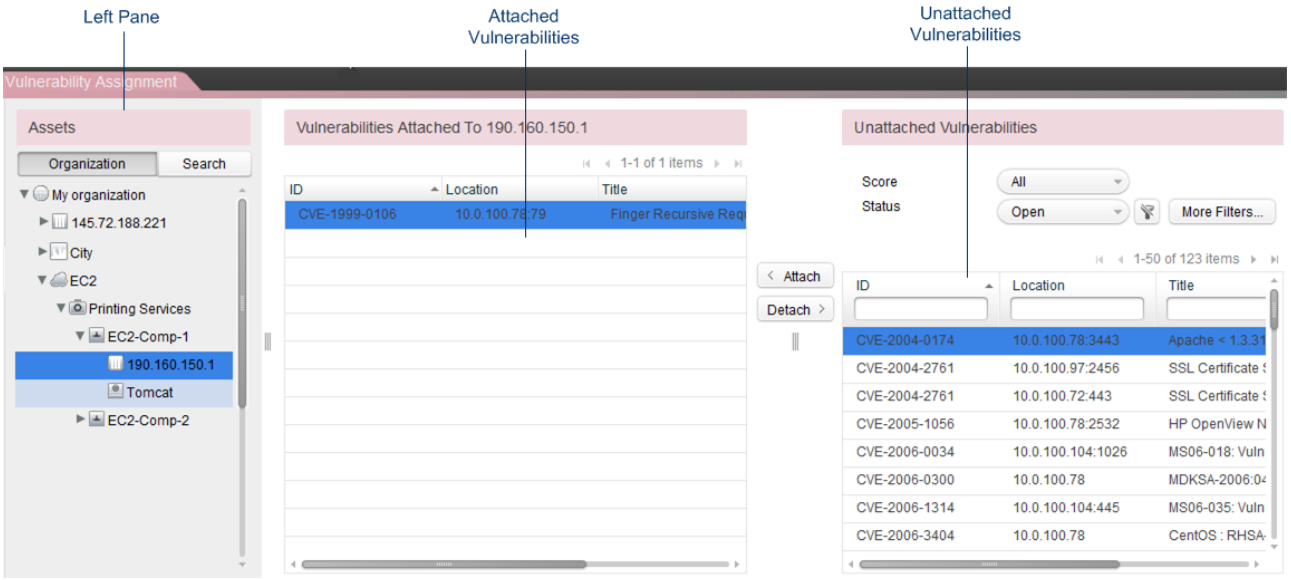
Status Management

UI Element	Description
Status	Filter according to the vulnerability's status (**Open** or **Closed**).

UI Element	Description
Remediation Status	Filter according to the vulnerability's remediation status. For more information on the different statuses, see "Remediation Status" (on page 82).
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 allows you to attach vulnerabilities to assets or detach vulnerabilities from assets. The different areas and the functionality available in each is 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	Allows 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
Detach >	**Attach Vulnerabilities to Asset** Select a vulnerability from the grid, and then click this button. For more information, see "To detach a vulnerability from an asset" (on page 81).

UI Element	Description
Attach	**Detach Vulnerabilities from Asset** 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 81).
<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: Low Medium High The ranges are determined in the *Configure Vulnerability Score Ranges* section in the *ArcSight EnterpriseView Deployment Guide*.
Status	Filter according to **Open** or **Closed**.
More Filters...	**Filter Vulnerabilities** 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 81). 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 are displayed on the toolbar.
	**Clear Filter** 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 and Title. You can filter vulnerabilities using the grid column headers.

Chapter 7

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 *ArcSight 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** 

button. For more information on the reports included in EnterpriseView, see "Printable Reports" (on page 127).

- **Dashboard**

  These reports are used as data analysis components and can be grouped together with other components in order to create comprehensive dashboards for the various roles, such as the "Risk Register" (on page 117).

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 115).

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 an EnterpriseView Report Using SAP BusinessObjects Web Intelligence" (on page 115).

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 11).
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 55).
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.
Country	Country of the asset.
OS Name	The operating system that is installed on the infrastructure

Object	Description
	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.
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. • 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. • For the Organization asset the source name is **System**.

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. The following formula is used for calculating the overall asset score: $\frac{Risk * weight + (100 - Maturity * 20) * weight + (100 - Compliance) * weight + ESM * 10 * weight + Vulnerabilty * 10 * weight}{\sum weights}$

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

Object	Description
	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 contained assets of an asset, but depends on the calculation method configured. For more information, see "Risk Score Aggregation Mechanism" (on page 75).

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. $\frac{\sum(Actor\ Score\ *\ Actor\ Weight)}{\sum(Actor\ Weights)}$ For more information, see "Risk Score Calculation" (on page 73).

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. For more information, see "Risk Score Calculation" (on page 73).

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.

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: • **Inherited**: From a containing asset. • **Inheritance Exception**: Control applicability has been overridden. • **Applied Manually**: A regular control assignment.

Inherited From Asset (subclass of Control - SoA)

Controls that are inherited from a containing asset.

Object	Description
Asset ID	The unique ID of the containing asset.
Asset Category	The category of the containing asset.
Asset Name	The name of the containing asset.
Asset Type	The type of the containing 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.
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.
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. 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

Object	Description
	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	Control unique ID.

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.

Object	Description
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.
Compliance Applied Manually	Indicates that a score was applied manually. It is applied only to the specific scores that have been changed.

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 35).

Object	Description
Assessed Policy ID	The unique ID of the assessed policy.

Object	Description
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.
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. A numeric value between 0 and 10.
Aggregated Asset ESM Threat Score	The highest threat score out of all the asset's contained assets (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: • Asset vulnerability score • $m * \frac{\sum(\text{Aggregated Asset Vulnerability Score} * \text{Criticality Level}) \text{ of top } n \text{ Contained Assets}}{\sum(\text{Criticality Level})}$ ***m***=*Contained Assets Multiplier* ***n***=*Maximum Contained Assets 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 contained assets.

Object	Description
Parent Asset ID	Containing 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 contained assets.

Object	Description
Child Asset ID	Contained asset unique ID.
Hierarchy Level	The position of the asset in the hierarchical tree, in reference to the containing asset (Parent Asset ID object).

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 55).
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.
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.

Object	Description
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.
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.

Object	Description
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 29).

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.
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**, **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, as well as 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.
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

Object	Description
	below the medium range are displayed in green.
High	Scores within the high range are 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	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.
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	The word "People" is displayed in the report.
Procedure	The word "Procedure" is displayed in the report.
Process	The word "Process" is displayed in the report.
Product	The word "Product" is displayed in the report.
Proof	The word "Proof" is displayed in the report.

Create an EnterpriseView Report Using SAP BusinessObjects Web Intelligence

In addition to the various reports provided by EnterpriseView, you can create customized reports 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 a 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 95).
2. Prompts can be added to the report in order to get the application context. Add an **assetId** prompt to initialize the report with a selected asset or a **policyId** prompt to initialize the report with a selected policy.
3. 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.

To create a EnterpriseView report that displays the contained assets 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 contained assets 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** 

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 *ArcSight 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 allows 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.

  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 75).
  - **Compliance**: The aggregated compliance score of the asset. For more information on how this score is calculated, see "Control Scores Aggregation Mechanism" (on page 50).
  - **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 50).
  - **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 85).
  - **ESM Threat**: The aggregated ESM threat score of the asset. This score is calculated as the highest score out of all the asset's contained assets and the asset itself.

    For more information on how the ESM threat score is calculated, see "Apply Weighting Scheme to Priority Factors" (on page 1).

  The following formula is used for calculating the overall asset 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 any of the scores by modifying the following objects in the EnterpriseView universe belonging to the Overall Score Weights class: **Risk Weight**,

Compliance Weight, **Maturity Weight**, **Vulnerability Weight**, or **ESM Weight**. For more information, see the *Universe Designer Help*.

- **Contained Assets Summary**

  Displays the information provided in the **Asset Summary** for the highest risk, first level contained assets of the asset that you selected (up to five are displayed).

- **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.

- **Risk Modeling**

  Includes:

  - **Assessed Risk Breakdown**: A pie chart displaying the distribution of assets according to risk scores divided into low, medium, and high for all first and second level contained assets.
  - **Highest Assessed Risk Scores**: A list of the highest risk contained assets (up to five are displayed).

- **Vulnerability Overview**

  Includes:

  - **Open Vulnerability Remediation Status**: Displays the number of contained, open vulnerabilities according to their remediation status.
  - **Most Vulnerable Assets**: A list of the most vulnerable contained assets (up to five are displayed).

Overall Score Heat Map

The Overall Score Heat Map allows 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 overall asset score is comprised of the aggregated scores of the following: risk, compliance, control maturity ,vulnerability, and ESM threat.

The assets displayed in the graph are first and second level contained assets 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 allows 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.

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. Clicking the icon of the asset in the graph selects 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 (...). Hovering over this icon displays information on all the assets that have the same overall asset score and criticality level.

Policy Compliance Dashboard

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

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

The Policy Compliance Dashboard includes the following components:

Policy and Asset Selector

This component enables you to select an asset and one of the policies to which it is applied to it and display compliance information on that asset and its contained assets.

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 allows 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 **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, as well as the maturity assessment score and progress for the asset that you have selected, in relation to the policy that you have selected. For more information on the aggregation mechanism, see "Control Scores Aggregation Mechanism" (on page 50).

Contained Asset Summary

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

Control Score Distribution

Displays the following pie charts:

- **Compliance Score Distribution**. The distribution of first and second level contained assets according to low, medium and high compliance scores.
- **Maturity Score Distribution**. The distribution of first and second level contained assets according to low, medium and high maturity scores.

P5 Score Breakdown

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

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 50).

Risk Modeling Dashboard

The Risk Modeling Dashboard includes information on risk assessment that is performed on a specific asset.

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

The 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 allows 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 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 (...). Hovering over this icon displays 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.

Vulnerability Dashboard

The Vulnerability Dashboard includes comprehensive vulnerability information providing you with an overview of your organization's vulnerability state, for a specific asset and its contained assets.

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 allows 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 85).

Most Vulnerable Contained Assets

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

- Aggregated asset vulnerability score.
- The percentage of open vulnerabilities that have not been handled yet, meaning, with a remediation status of New or Reopened.

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 contained assets, 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 contained asset. 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 contained asset.

The **Impacted Assets with Open Vulnerabilities** column displays the percentage of assets with vulnerabilities that have an open status out of all vulnerabilities.

Policy Compliance Map

The Policy Compliance Map allows 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 functionality available in each is described in the following sections.

Left Pane (Asset Selector)

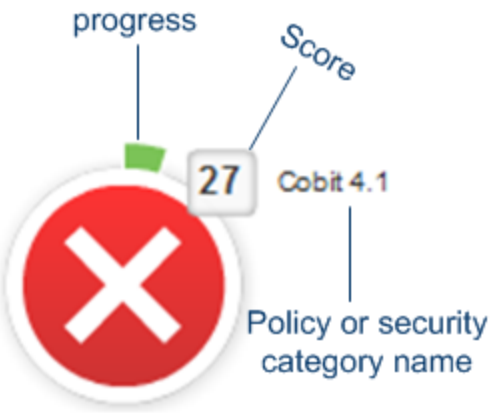
UI Element	Description
Organization tab	The Organization tab displays the EnterpriseView business model. Expand the business model and select the asset that you want to view.
Search tab	You can search for a name or a partial name of any asset in EnterpriseView, connected to the business model.

Graph Area

Compliance assessment information and control maturity assessment information is displayed in two separate tabs: **Compliance** and **Maturity** in the graph area. This allows you to focus specifically on the information that 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** Refreshes the layout of the business model in the graph.

UI Element	Description
	**Fit to Window** 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:  High score  Medium score  Low score The ranges are determined in "Configure Policy Settings" (on page 27)

Graph Overview

When an asset has multiple policies/security categories applied to it and is larger than the graph area, you can navigate it by clicking and dragging in the Graph Overview area.

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 *ArcSight EnterpriseView Deployment Guide*.

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

For each security threat, a score (1-10) is used to depict threat level. This information is displayed graphically either per asset or for multiple assets and allows identifying 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 contained assets (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.

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** 

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 115).

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.
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 contained assets.
	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 contained assets.

Chapter 8

Job Management

The EnterpriseView Job Management module is based on the Spring Batch framework. Using the Job Management module you can:

- **Launch batch jobs manually**

  Generally, batch jobs are scheduled to run automatically via the EnterpriseView Configuration module. However, you can also launch jobs manually when required, for example, in order to re-run a job that failed or in order to test a job in a test environment. For more information, see "Launch Batch Jobs Manually" (on page 129).

- **Troubleshoot batch jobs**

  You can inspect the details of each step that comprises the job in order to identify where it failed. For more information, see "Troubleshoot Batch Jobs" (on page 129).

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

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

Launch Batch Jobs Manually

To launch batch jobs manually

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

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

Troubleshoot Batch Jobs

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

To troubleshoot batch jobs

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

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

   - Details on the job level.
   - A table that includes all the job steps and their statuses.
3. From the job steps table, identify the step with the **Failed** status, and in the **Status** column click the **Failed** link.

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

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