HP ArcSight EnterpriseView

For the Windows Operating System

Software Version: 1.0

Deployment Guide

Document Release Date: March 2012

Software Release Date: March 2012

Legal Notices

Warranty

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

Restricted Rights Legend

Copyright Notice

Trademark Notices

This document is confidential.

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 7

About ArcSight EnterpriseView 8

Install ArcSight EnterpriseView 9

- System Requirements 9
- Integration Matrix 10
- EnterpriseView Architecture Diagram 12
- Prerequisites 13
- Install SAP BusinessObjects Enterprise CMC 14
- Configure BusinessObjects Enterprise 15
- Run EnterpriseView Setup Wizard 18

EnterpriseView Post Installation Tasks 19

Module Administration 20

User Management 21

- Add Roles 22
- Assign Roles to a User or Group 23
- Search Users 23
- Roles and Permissions 24

Synchronize Assets with External Asset Repository 26

- Integrate with HP Universal CMDB 26
  - About UCMDB Asset Synchronization Job 26
  - How to Integrate with HP Universal CMDB 27
  - Define Connection Parameters with UCMDB 28
  - Map Asset Category with UCMDB 29
  - Edit Field Mapping 29
  - Define Imported Asset Type Properties 30

Schedule and Activate the UCMDB Asset Synchronization Job 30
Reverse Relation Direction 31
Integrate with ArcSight Enterprise Security Manager 31
About ArcSight ESM Asset Synchronization Job 32
How to Integrate with ESM for Asset Synchronization 32
Define Connection Parameters with ESM 33
Map Asset Types with ESM 33
Schedule and Activate ArcSight ESM Job 34
Import Assets From CSV 34
About CSV Asset Synchronization Job 36
How to Import Assets from CSV 37
Configure CSV File Settings 37
Map Asset Categories with CSV 37
Schedule and Activate CSV Job 38
Import Security Threats from an SIEM System 39
About ESM Security Threats Job 39
How to Integrate with ESM to Import Threats 39
Apply a Weighting Scheme to Priority Factors 40
Import Vulnerabilities From Vulnerability Assessment Tools 41
About the Vulnerability Import Job 41
Install and Configure ArcSight SmartConnector 42
Schedule and Activate Vulnerabilities Import Job 44
Configure Asset Vulnerability Score Aggregation Parameters 45
Configure Vulnerability Score Ranges 45
Configure Vulnerability Dashboard Settings 46
Configure Automatic Policy Assessment 47
How to Integrate with HP Server Automation 47
Install Server Automation Connector 48
Define Server Automation Connection Parameters 48
Run SA Connector for the First Time (Manual) 48
Monitor and Troubleshoot the Server Automation Connector 49
Configure Risk Score Aggregation Method 50

Manage SAP BusinessObjects Report Settings 51
EnterpriseView Workspace 52
Create a Customized Dashboard Page 52
Configure Page Layout 53
Save Page 54
Manage Pages 55
Edit Page Layout 55
Manage Components 56
Manage Component Categories 56
Create an External Component 57
Set Up Wiring Between Components 57
Dashboard Builder Toolbar 58
Manage Configuration Sets 60
Select Configuration Set 60
Save and Apply Configuration Changes 60
Appendix A: Asset and Threat Reporting 62
About the Asset Report 62
About the Threat Report (URI) 62
Factors Used to Calculate an Asset Threat Score 63
Filter Event Processing 64
Importing the Asset and Threat Reports in ArcSight ESM 64
Threat Score Calculation on Asset - Example 65
Appendix B: Learn About Cron Expressions 66

Welcome to This Guide

Welcome to the HP ArcSight EnterpriseView (EnterpriseView) Deployment Guide. This guide provides you information about the installation and initial configuration of EnterpriseView, including integration with external asset repositories and security information and event management systems.

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

This guide includes the following chapters:

"About ArcSight EnterpriseView" (on page 8)

"Install ArcSight EnterpriseView" (on page 9)

"EnterpriseView Post Installation Tasks" (on page 19)

"Module Administration" (on page 20)

"User Management" (on page 21)

"Synchronize Assets with External Asset Repository" (on page 26)

"Import Security Threats from an SIEM System" (on page 39)

"Import Vulnerabilities From Vulnerability Assessment Tools" (on page 41)

"Configure Risk Score Aggregation Method" (on page 50)

"Manage SAP BusinessObjects Report Settings" (on page 51)

"EnterpriseView Workspace" (on page 52)

"Manage Configuration Sets" (on page 60)

"Appendix A: Asset and Threat Reporting" (on page 62)

"Appendix B: Learn About Cron Expressions" (on page 66)

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.

Install ArcSight EnterpriseView

This chapter describes how to install and start EnterpriseView.

EnterpriseView integrates with SAP BusinessObjects Enterprise CMC primarily for creating reports and dashboards, but also for user management. As such, you must have a complete installation of SAP BusinessObjects version 3.1 SP 3.0 running in your network. If you do not already have SAP BusinessObjects installed on your network, you need to install it, as described in "Install SAP BusinessObjects Enterprise CMC" (on page 14).

To install EnterpriseView

1. Review the "System Requirements" (on page 9) and make sure that you comply with all the requirements.
2. Review the "Prerequisites" (on page 13) and make sure that all pre-installation tasks are done.
3. If SAP BusinessObjects is not installed, "Install SAP BusinessObjects Enterprise CMC" (on page 14).
4. "Configure BusinessObjects Enterprise" (on page 15).
5. "Run EnterpriseView Setup Wizard" (on page 18).

After you have completed the tasks above, proceed to the "EnterpriseView Post Installation Tasks" (on page 19).

System Requirements

This section includes server system requirements, database requirements, and client requirements for installing and running EnterpriseView.

> **Note:** It is recommended that you install SAP BusinessObjects and EnterpriseView on separate servers, although you can install them on the same server.

The following requirements assume that SAP BusinessObjects and EnterpriseView are installed on separate servers. If they are installed on the same server, then the minimum free disk space and the memory requirements for the server is the total of the minimum requirements for both applications.

> **Note:** Make sure the date and time zone that are configured on the server on which you are installing SAP BusinessObjects and on the server on which you are installing EnterpriseView are synchronized.

EnterpriseView Server System Requirements

Element	Requirement
Computer/Processor	Two processors, 3GHz each
Free Disk Space	Minimum of 10 GB
Memory (RAM)	Minimum of 4 GB

Element	Requirement
Operating System	Windows Server 2008 R2 (x64) Enterprise Edition
Database	Oracle 11.2.0.1 or later Tablespace for EnterpriseView 50 GB Tablespace for User Management module 0.5 GB

SAP BusinessObjects Server System Requirements

Element	Requirement
Computer/Processor	Two processors, 3GHz each
Free Disk Space	Minimum of 20 GB
Memory (RAM)	Minimum of 4 GB
Operating System	Windows Server 2008 R2 (x64) Enterprise Edition
Database	Oracle 11.2.0.1 or later Tablespace 2 GB **Note:** The EnterpriseView system is certified to work only with an Oracle database, however, SAP BusinessObjects can also be installed with other databases, such as MySQL and SQL Server. For more information, see the SAP BusinessObjects documentation. The installation described in this chapter assumes that SAP BusinessObjects is installed with an Oracle database.

Client Requirements

Element	Requirement
Browser	• Microsoft Internet Explorer 7.x, 8.x, 9.x (32-bit and 64-bit) • Mozilla Firefox 3.x or later (32-bit and 64-bit) • Google Chrome
Adobe Flash Player	Flash Player 10 or later
Screen Resolution	• Minimum 1024x768 • Recommended 1440x900

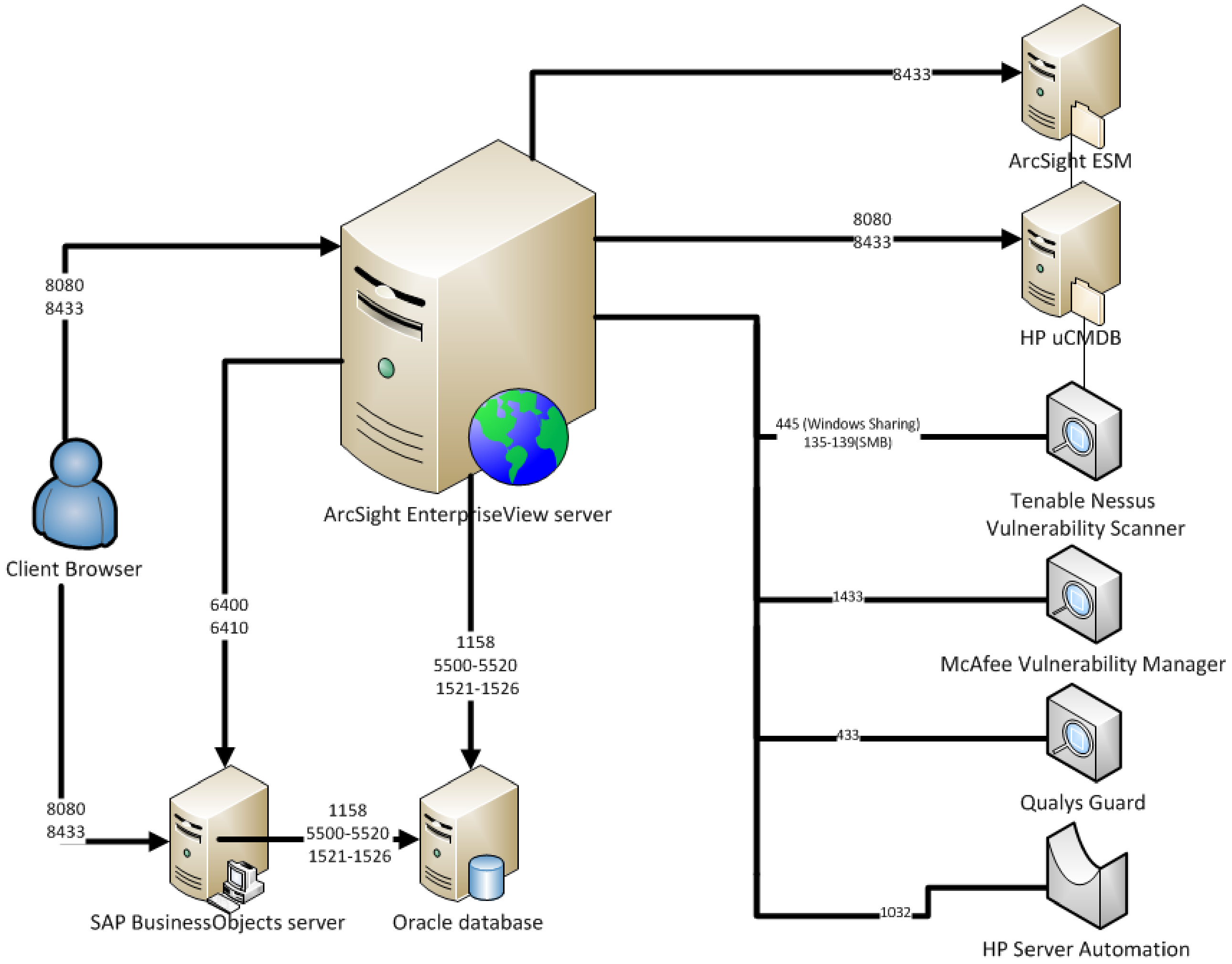
Integration Matrix

The following table includes the supported versions of products that EnterpriseView integrates with.

Product	Version
HP Universal CMDB	8.x, 9.x
ArcSight Enterprise Security Manager	5.0.1.6572.0
HP Server Automation (SA)	9.10
Tenable Nessus Vulnerability Scanner	3.2.x, 4.x
McAfee Vulnerability Manager (Foundscan)	7.0
Qualys Guard	6.05

EnterpriseView Architecture Diagram

The following diagram outlines the IP ports used for communication between the different elements of EnterpriseView and systems with which it integrates. If you have a network security system that can block access, such as a firewall, its policy must be modified to allow communication between the systems.



Prerequisites

Before you begin installing, do the following:

- Allocate three new Oracle user schemas; for EnterpriseView, for SAP BusinessObjects Enterprise CMC, and for the User Management module. For each user schema, grant the following roles:
    - RESOURCE
    - CONNECT

  For the EnterpriseView user schema, grant the following additional roles:

    - CREATE ANY VIEW
    - DROP ANY VIEW
- The Oracle database must be configured to support UTF-8 character set. For more information, refer to Oracle documentation.
- Oracle Instant Client for Microsoft Windows (x64) version 11.2.0.2.0 must be installed on the machine on which SAP BusinessObjects is installed, and can be downloaded from the Oracle Web site.
- ojdbc5.jar (Oracle Database 11g Release 2 (11.2.0.3) JDBC Driver) must be installed on the machine on which SAP BusinessObjects is installed, and can be downloaded from the Oracle Web site.
- If the server on which SAP BusinessObjects is installed has a firewall installed, make sure that all SAP BusinessObjects ports are open.
- If a Shared Secret is already configured in SAP BusinessObjects, then make sure that you have it.
- Obtain a license for ArcSight EnterpriseView from your support or sales representative. After installation, save a copy of the license in your EnterpriseView environment, as described in "EnterpriseView Post Installation Tasks" (on page 19).
- Make sure that you have Adobe Flash Player version 11.0 or a higher version installed on your client machine. You can download Adobe Flash Player from the Adobe Web site.

Install SAP BusinessObjects Enterprise CMC

Before you install SAP BusinessObjects, make sure that you have a license key.

To install SAP BusinessObjects

1. Click the **setup.exe** file located in the **Installations\BusinessObjects** folder of your HP ArcSight EnterpriseView installation medium.
2. On the language selection dialog box, from the list of languages, select **English**, and then click **OK**.

   The **SAP BusinessObjects Setup Wizard** opens.
3. Follow the instructions in the **SAP BusinessObjects Setup Wizard**. When you reach the following pages, enter the required information:
   a. On the **User Information** page, in the **Product Keycode** box, enter the license key, and then click **Next**.
   b. On the **Install Type** page, select the **Use an existing database server** option, and then click **Next**.
   c. On the **Server Components Configuration** page, in the **Administrator account** group box, in the **Password** box, enter a password for the **Administrator** user. Enter the password again in the **Confirm password** box, and then click **Next**.

      > **Note:** These credentials will be used by the SAP BusinessObjects and the EnterpriseView administrator to access the applications.

   d. On the **CMS Database Information** page, in the **CMS Database** group box, enter the following information, and then click **Next**:
      - In the **Server** box, enter the server information in the following format: **<IP Address>:<Port>/<SID>**.
      - In the **Username** box, enter the Oracle schema user name.
      - In the **Password** box, enter the Oracle schema password.

   e. On the **Configure Tomcat** page, if ArcSight EnterpriseView and SAP BusinessObjects are installed on the same server, modify the following parameters:
      - **Connection port**
      - **Shutdown port**
      - **Redirect port**

After the installation is complete, you need to "Configure BusinessObjects Enterprise" (on page 15).

Configure BusinessObjects Enterprise

After SAP BusinessObjects is installed, do the following:

Enable SAP BusinessObjects Universe to operate with an Oracle database

1. In the SAP BusinessObjects server, open the following file:

   <SAP BusinessObjects Installation path>\BusinessObjects Enterprise 12.0\win32_x86\dataAccess\connectionServer\jdbc\jdbc.sbo

   > **Note:** it is recommended that you back up the jdbc.sbo file before editing it.

2. Search and replace.

   Search for the following:

   ```
   <DataBase Active="Yes" Name="Oracle 11">
   ```

   In the <JDBCDriver> tag below this line, replace the following lines:

   ```
   <!--  Uncomment and edit the following lines to define java classes
   required by JDBC driver

           &lt;ClassPath&gt;

           &lt;Path&gt;your jar or class files directory&lt;/Path&gt;

           &lt;/ClassPath&gt;

   -->
   ```

   with:

   ```
   <ClassPath>

           <Path><the ojdbc5.jar installation path></Path>

   </ClassPath>
   ```

   > **Note:** This is the ojdbc5.jar JDBC driver that you installed prior to installing SAP BusinessObjects, as described in "Prerequisites" (on page 13).

3. Save the changes in the file.

Configure the maximum number of document states kept in memory

1. In the SAP BusinessObjects server, open the following file:

   <SAP BusinessObjects Installation path>\Tomcat55\webapps\AnalyticalReporting\WEB-INF\classes\webi.properties

   > **Note:** It is recommended that you back up the webi.properties file before editing it.

2. Find the following lines:

```
#WID_FAILOVER_SIZE=11
```

```
#WID_STORAGE_TOKEN_STACK_SIZE=11
```

Remove the remarks by deleting the hash (#) from the parameters and change their value to **150**.

3. Save and close the file.

Configure the maximum number of simultaneous connections

1. Open SAP BusinessObjects Enterprise CMC.
2. Under **Organize**, click **Servers**.
3. In the left pane, expand **Service Categories**, and then click **Web Intelligence**.
4. In the right pane, double-click **WebIntelligenceProcessingServer**.
5. On the **Properties** window, in the **Web Intelligence Processing Service** group box, enter the following information:
   - In the **Maximum Connections** box, enter **150**.
   - In the **Maximum Documents Per User**, enter **20**.

Configure LDAP Authentication

> **Note:** Perform this procedure if:
>
> - You are using LDAP as an authentication system.
> - You are using a customized LDAP server configuration rather than an industry standard configuration (**LDAP Server Type**=**Custom**).

1. Follow the instructions in *Configuring LDAP Authentication* in the *Using LDAP Authentication* section in the *SAP BusinessObjects Enterprise Administrator's Guide*.
2. When you reach step 4, click **Show Attribute Mapping**.
3. Change the LDAP server attributes mapping as defined in your LDAP server for the following fields:
   - **User Name** (for example, **cn**)
   - **Full Name** (for example, **uid**)
   - **Email** (for example, **mail**)
   - **Default Group Search Attributes**
   - **Default User Search Attributes**

Restart the SAP BusinessObjects server

1. In the SAP BusinessObjects server, click **Start > BusinessObjects Enterprise > Central Configuration Manager**.
2. On the **Central Configuration Manager** window, stop and restart the following:

a. **Tomcat Application Server**

b. SAP BusinessObjects **Enterprise Server**

   For more information on stopping and starting SAP BusinessObjects servers, see the *SAP BusinessObjects Administrator Guide*.

After the configuration is complete, it is recommended that you run the SAP BusinessObjects**Diagnostics Tool** in order to check whether the installation and configuration were performed properly. For more information, see the *After Installing BusinessObjects Enterprise* chapter in the *SAP BusinessObjects Administration Guide*.

Run EnterpriseView Setup Wizard

This section describes how to run the EnterpriseView setup wizard.

> **Note:** If the installation fails, you can find the log file in the following location:
>
> **%TEMP%\enterpriseview-installation.log**

To run EnterpriseView setup

1. Click the **setup.exe** file located in the **\Installations\EnterpriseView** folder of your HP ArcSight EnterpriseView installation medium.
2. Follow the instructions in the **EnterpriseView Setup Wizard**.

   When you reach the **Database Settings** page, enter the database URL and credentials. For details about configuring the native Oracle JDBC URL format, see JDBC - Oracle FAQ.
3. On the completion page, click **Finish**.

   > **Note:** This setup deploys the EnterpriseView Universe and out-of-the-box reports in SAP BusinessObjects in the folders that you have defined during the installation.
   >
   > Reports: **Folders > All Folders > <*EnterpriseView_Folder*>**
   >
   > Universe: **Universes > Universes > <*EnterpriseView_Universe*>**
4. Restart the computer.

   The EnterpriseView application starts automatically. The service name is:

   ArcSight EnterpriseView

   You can access EnterpriseView via **http://<server IP>:8080/redcat**.

   > **Note:** The EnterpriseView login password is case-sensitive.

   After you access EnterpriseView, follow the instructions in "EnterpriseView Post Installation Tasks" (on page 19).

> **Note:** You can uninstall EnterpriseView by running **Uninstall.bat** from the EnterpriseView Installation folder.

EnterpriseView Post Installation Tasks

After you have installed EnterpriseView, do the following:

1. Save the ArcSight EnterpriseView license (arcsight.lic) that you have obtained from your support or sales representative in the EnterpriseView installation folder.
2. Select the modules that you are licensed to use, as described in "Module Administration" (on page 20).
3. Configure your "User Management" (on page 21) system. Users and groups may already be defined either in SAP BusinessObjects or in a security system integrated with SAP BusinessObjects, such as LDAP. EnterpriseView includes predefined roles that you need to assign to users and groups, as described in "Assign Roles to a User or Group" (on page 23). You can also create new roles, as described in "Add Roles" (on page 22).
4. If required, integrate with external systems, as described in "Synchronize Assets with External Asset Repository" (on page 26), "Import Security Threats from an SIEM System" (on page 39) and "Import Vulnerabilities From Vulnerability Assessment Tools" (on page 41).
5. "Configure Risk Score Aggregation Method" (on page 50).

Module Administration

The first task to perform after you open EnterpriseView is to select the modules with which you are licensed to work.

To configure the EnterpriseView module set

1. In EnterpriseView, click **Administration** > **Configuration**.
2. In the **Configuration** window, in the left pane, click **Module Administration**, and then click **Enabled Modules**.
3. To comply with your licensing agreement, clear the check boxes for the modules for which you do not have a license. (By default, all of the modules in EnterpriseView are enabled.)
4. "Save and Apply Configuration Changes" (on page 60).

   Any components and pages that belong to the modules that you removed from the configuration are not displayed.

User Management

EnterpriseView integrates with SAP BusinessObjects Enterprise CMC primarily for delivering robust reporting functionality, but also for user management. Users and groups are managed in SAP BusinessObjects, but are displayed in EnterpriseView as well. Any changes that are made to users and groups in SAP BusinessObjects are automatically reflected in EnterpriseView. If SAP BusinessObjects is integrated with a security system, such as LDAP, then any change made in the security system is propagated to both SAP BusinessObjects and EnterpriseView.

HP ArcSight EnterpriseView enables you to define roles, as described in "Add Roles" (on page 22), and assign them to users and groups, as described in "Assign Roles to a User or Group" (on page 23). A role defines which actions a user can perform in EnterpriseView. For example, if none of the user’s roles have permission for Risk Assessment, the Risk Modeling Assessment window is not available.

> **Note:** EnterpriseView manages roles and permissions for all inherent EnterpriseView components and pages; it does not manage permissions for printable reports and dashboards based on the BusinessObjects Reports component. These permissions are managed directly via SAP BusinessObjects. By default, all users have access to the reports. To set security limitations on reports, refer to the *Managing Users and Groups* chapter in the *SAP BusinessObjects Enterprise Administrator's Guide*.

Roles and Permissions

In EnterpriseView, a role is a set of permissions that is assigned to a user. EnterpriseView includes out-of-the-box roles, which correspond to common EnterpriseView users. You can add or edit roles in order to comply with your organization's business requirements. Permissions define which EnterpriseView actions the role can perform according to their responsibilities in the organization. Permissions can determine which modules you can access and which actions you can perform; they can also determine the actions you can perform on specific data.

Some permissions are bundled into permission sets, which are predefined groups of permissions that you can apply to a role, without having to select each permission individually. Permissions and permission sets are predefined in EnterpriseView and they cannot be changed or added.

Users and Groups

Every user has one or more roles that define their permissions for working with EnterpriseView. When you assign a role, that user has access only to specific portions of the program that are relevant to their role. Groups are a collection of users. A specific role can be assigned to a group, and all of the users in that group automatically inherit that role.

Add Roles

In EnterpriseView a role is a set of permissions that is assigned to a user and defines the user's capacity. EnterpriseView includes out-of-the-box roles, which correspond to common EnterpriseView users. You can add or remove permissions from a role at any time in order to comply with your organization's business requirements.

To add a role

1. In EnterpriseView, click **Administration > User Management**, and then click the **Role Management** tab.
2. On the **Roles** pane on the left, click the **Create Role** button.
3. On the **Edit Role Details** dialog box, enter a **Name** and **Description** for the new role. Click **OK**.
4. In the **Role Details** pane, under **Permissions**, click the **Attach Permissions** ✚ button and follow the instructions on the **Assign Permissions to Roles Wizard**.
   - When you reach the **Assign environments to permissions** page, in **Available Environments**, click **All** and then click ➡. Click **Next** to continue.

Assign Roles to a User or Group

You can assign roles to a user or a group. Roles that are assigned to a group are applied to all of the users in the group.

To assign roles

1. In EnterpriseView, click **Administration > User Management**
2. In the **Users and Groups** tab, click the user or group to which you want to assign a role. You can also "Search Users" (on page 23).
3. On the right pane, under **Roles and Permissions**, click the **Assign Role** ➕ button.
4. On the **Assign Roles** dialog box, from the list of **Available Roles**, click the arrow ➡ button to select the roles that you want to assign to the user or group, and then click **OK.**

   The **Roles and Permissions** area, in the **Details** pane, displays the roles.

Search Users

You can use wildcards to search for a user. For example, if you enter the '*' character in the search field, then all of the EnterpriseView users are retrieved.

To search for a user

1. In EnterpriseView, click **Administration > User Management**
2. On the left pane, click the **User Management** tab.
3. On the left pane, click the **Search Users** tab.
4. On the **Search Users** tab, enter the search criteria, and then click **Search**. No search criteria will return empty results.

Roles and Permissions

EnterpriseView manages permissions for all EnterpriseView components and pages. It does not manage permissions for printable reports and dashboards based on the BusinessObjects Reports component. These permissions are managed directly via SAP BusinessObjects. By default, all users have access to the reports.

The BSF Administrator role has permissions to all components. It is the only role that can access the following modules and pages:

- Configuration
- User Management
- Job Management
- Dashboard Builder

The following table includes all the default roles that are defined in EnterpriseView, their permissions, and which components are accessible for these roles. For more information on permissions, see "User Management" (on page 21).

Note: All roles have a **Login** permission.

Role	Permissions	Accessible components
Asset Profiler	• Read Assets • Edit Assets • Read Policy Statement of Applicability	• Asset Profiling
Policy Auditor	• Read Policies • Read Policy Statement of Applicability • Read Assets • Read Policy Assessments • Edit Policy Assessments	• Policy Assessment • Policy Compliance Map
Policy Compliance Manager	• Read Policies • Read Policy Statement of Applicability • Edit Policy Statement of Applicability • Read Assets	• Statement of Applicability
Policy Builder	• Read Policies • Edit Policies	• Policy Builder • Policy Mapping

Role	Permissions	Accessible components
Policy Viewer	• Read Policies • Read Assets • Read Policy Statement of Applicability • Read Policy Assessments	• Policy Compliance Map
Risk Auditor	• Read Risk Assessments • Read Assets • Read Threat Library • Edit Risk Assessments	• Risk Modeling Assessment • Risk Heat Map • Risk Scorecard
Risk Viewer	• Read Risk Assessments • Read Assets • Read Threat Library	• Risk Modeling Assessment • Risk Heat Map • Risk Scorecard
Security Officer	• Read Security Threats • Read Risk Assessments • Read Assets • Read Threat Library • Read Policies • Read Policy Statement of Applicability • Read Policy Assessments	• Policy Compliance Map • Risk Modeling Assessment • Risk Heat Map • Risk Scorecard
Threat Library Administrator	• Read Risk Assessments • Read Assets • Read Threat Library • Edit Threat Library • Edit Risk Assessment	• Threat Library Builder • Risk Modeling Assessment • Risk Heat Map • Risk Scorecard
Security Threat Viewer	• Read Security Threats • Read Assets	• ESM Threat View
Vulnerability Manager	• Read asset • Edit asset • Read vulnerability • Edit vulnerability	• Vulnerability Management • Vulnerability Assignment • Asset Profiling

Synchronize Assets with External Asset Repository

You can synchronize the EnterpriseView business model with an external asset repository that is used by your organization, such as a Configuration Management System. Synchronization involves integration with the external asset repository and a periodic import of the assets that it holds, into the EnterpriseView database. Assets can be added, deleted or modified in the asset repository and the changes are automatically reflected in EnterpriseView, providing a single point of reference for your organization's assets. Assets that have been imported from an asset repository cannot be deleted in EnterpriseView; their properties, however, might be editable, depending on your configuration preferences, as described in "Define Imported Asset Type Properties" (on page 30).

> **Note:** While you can rely on an external asset repository to provide you with a complete business model, you can, at any time, create new assets in EnterpriseView and add them to your business model. Assets that are added manually can be removed from the business model and their properties can be modified.

EnterpriseView supports integration with the following systems:

- HP Universal CMDB version 8.x and version 9.x. For more information see "Integrate with HP Universal CMDB" (on page 26).
- ArcSight Enterprise Security Manager version 5.0.1.6572.0. For more information see "Integrate with ArcSight Enterprise Security Manager" (on page 31).

In addition, you can synchronize your business model with an asset repository that does not integrate with EnterpriseView by importing a CSV file, as described in "Import Assets From CSV" (on page 34).

You can synchronize assets with only one external asset repository.

Integrate with HP Universal CMDB

Integrating with UCMDB involves preparation in EnterpriseView as well as in UCMDB. Before you begin the integration process, the UCMDB administrator must first create a TQL (Topology Query Language) query. The TQL query will be activated by EnterpriseView and will retrieve the assets (or CIs in UCMDB) and relationships that comprise the business model from the UCMDB database. The UCMDB administrator should provide you with the TQL query name, as any connection parameters. After you have gathered all the information from the UCMDB administrator, you can begin the integration process, as described in "How to Integrate with HP Universal CMDB " (on page 27).

After EnterpriseView is fully integrated with UCMDB, the Synchronization job is run periodically, according to the schedule that you define in "Schedule and Activate the UCMDB Asset Synchronization Job" (on page 30). To learn more about the Synchronization job, see "About UCMDB Asset Synchronization Job" (on page 26).

About UCMDB Asset Synchronization Job

The Asset Synchronization Job periodically imports UCMDB elements (CIs and relationships), as defined in the TQL query, from UCMDB into EnterpriseView, as follows:

1. The UCMDB TQL query for retrieving UCMDB elements is triggered.
   - For **UCMDB version 8.0**, all of the elements are retrieved at once.
   - For **UCMDB version 9.0**, elements are retrieved in batches. The maximum batch size is determined in EnterpriseView when you define connection parameters. For more information, see "Define Connection Parameters with UCMDB" (on page 28).
2. The fields in UCMDB elements are compared against fields in assets/relations and are loaded to a temporary table.
3. UCMDB elements are converted into EnterpriseView assets and relations.
4. The process checks the EnterpriseView database for each of the assets/relations.

   > **Note:** If the category of an asset was changed in UCMDB, then a new asset is created and the old asset is deleted. Any controls applied to that asset, as well as risk and policy assessments, are deleted.

   - If the **element does not exist** in the database, then the process writes that element to the EnterpriseView database.
   - If the **element changed**, then the process makes these changes in the EnterpriseView database.
5. Outdated assets and their relations (meaning that they no longer exist in the UCMDB database) are deleted from the EnterpriseView database.

How to Integrate with HP Universal CMDB

Before you begin integrating EnterpriseView and UCMDB, you must be acquainted with the Synchronization process, as described in "About UCMDB Asset Synchronization Job" (on page 26), as well as with the UCMDB BTO Data Model and structure logic. Make sure that you have the TQL query name and connection parameters provided to you by the UCMDB administrator.

The following procedure outlines the steps for integrating with UCMDB:

1. If any part of the UCMDB BTO Data Model is reversed in structure to the business model that you are planning to deploy in EnterpriseView, then follow the instructions in "Reverse Relation Direction" (on page 31).
2. **Define connection parameters**. Define the parameters necessary for connecting with UCMDB. These parameters must be provided to you by the UCMDB administrator. Follow the instructions in "Define Connection Parameters with UCMDB" (on page 28).
3. **Review Default Asset Category Mapping**. Review the default asset category mappings that are included in EnterpriseView to see whether they reflect your business model. Compare the default mapping in EnterpriseView to the mapping defined in the UCMDB TQL query. Make sure that all CIs defined in the TQL query or the composite CI (any upper-level CI containing the CI in the TQL query) are mapped. If any CI type is not mapped, then the Asset Synchronization job will fail. If required, follow the instructions in "Map Asset Category with UCMDB" (on page 29) to tailor the mapping to your needs.
4. **Review Default Asset Field Mapping**. Review the mapping between the asset fields and CI fields. If the CIs in UCMDB have been customized, follow the instructions in "Edit Field Mapping" (on page 29) to include these customizations.

5. **Define Imported Asset Type properties**. For each asset property, decide which will be imported from UCMDB, as described in "Define Imported Asset Type Properties" (on page 30).
6. **Schedule and activate the Synchronization job** to complete the process, as described in "Schedule and Activate the UCMDB Asset Synchronization Job" (on page 30).

Define Connection Parameters with UCMDB

The first step in integrating with UCMDB is defining connection parameters. Excluding **Max Bulk Size**, all of these parameters should be provided by the UCMDB administrator prior to integration.

To define connection parameters with UCMDB

1. In EnterpriseView, click **Administration > Configuration**.
2. In the left pane, click **Integrations > UCMDB > Asset Synchronization**. Click on the configuration management system that you are integrating with:
   - **HP Universal CMDB 8**
   - **HP Universal CMDB 9**
3. Click **Connector**, and then enter the parameters for connecting with UCMDB, as described in the following table:

Parameters	Description
Communication Protocol	Select either **HTTP** or **HTTPS**, according to the specifications received from the UCMDB administrator.
Communication Host	The address of the UCMDB server, provided by the UCMDB administrator.
Communication Port	The UCMDB server port, provided by the UCMDB administrator.
UCMDB User Name	Credentials for accessing UCMDB, provided by the UCMDB administrator.
UCMDB Password	Credentials for accessing UCMDB, provided by the UCMDB administrator.
Application Context	Credentials for accessing UCMDB, provided by the UCMDB administrator.
TQL Query Name	The name of the TQL query that EnterpriseView activates for retrieving assets, provided by the UCMDB administrator.
Max Bulk Size	This parameter is relevant only when integrating with UCMDB version 9. Defines the maximum number of UCMDB entities (assets and relations) that the query returns to EnterpriseView at a time. When integrating with UCMDB version 8, the UCMDB entities are sent to EnterpriseView in one batch.

4. "Save and Apply Configuration Changes" (on page 60).

Map Asset Category with UCMDB

EnterpriseView includes mapping between all of the default asset categories and their UCMDB counterparts.

You can create additional mappings based on the model's business logic. Several unrelated CI types can be mapped to the same asset category, when more than one CI type is reflected in that asset category.

> **Note:** This step deals with mapping assets on the highest level—the category level. The asset **Type** field in EnterpriseView is identical to the CI type in UCMDB. As such, the asset **Type** field is populated automatically during the import process.

To map asset categories

1. In EnterpriseView, click **Administration > Configuration**.
2. In the left pane, click **Integrations > UCMDB > Asset Synchronization**. Click the configuration management system that you are integrating with:
    - **HP Universal CMDB 8**
    - **HP Universal CMDB 9**
3. Click **Asset Category Mapping**, and then do the following:
    - On the right pane, click the **Add configuration to configuration set** button.
    - In the **Asset Type** box, enter the asset category.
    - In the **CI Type** box, enter the CI type.
4. "Save and Apply Configuration Changes" (on page 60).

Edit Field Mapping

The Asset Field Mapping page displays the mapping between asset properties and CI properties for all asset categories. These mappings reflect the default asset and CI properties that are included in EnterpriseView and UCMDB, respectively. Some asset properties are common to all assets while others are asset-specific.

If you want the mapping to reflect customized UCMDB CI fields, you can edit the CI field settings.

> **Note:** If you map fields with different value types (for example, if you map a field defined as a string to a field defined as an integer) make sure that the field value from UCMDB can be converted to the expected value in the EnterpriseView field. If the value cannot be converted, then the Asset Synchronization job will fail.

To edit field mapping

1. In EnterpriseView, click **Administration > Configuration**.
2. In the left pane, click **Integrations > UCMDB > Asset Synchronization**. Click the

configuration management system that you are integrating with:

- **HP Universal CMDB 8**
- **HP Universal CMDB 9**

3. In the left pane, click **Asset Field Mapping**, and then, in the right pane, make the necessary changes in the **CI Field**.
4. "Save and Apply Configuration Changes" (on page 60).

Define Imported Asset Type Properties

This task is relevant only if you are importing assets from an asset repository, such as a Configuration Management System (CSM), in order to create the organization's business model.

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

- Name
- Description
- Owner

To define imported asset type properties

1. In EnterpriseView, click **Administration > Configuration**.
2. In the **Configuration** module, in the left pane, click **Asset Management > Imported Asset Properties Policy**.
3. For each asset category displayed under **Imported Asset Properties Policy**, do the following:
   a. In the left pane, click the asset category.
   b. For each property, select or clear the **Synchronize** check box. If a check box is not selected, then the asset property will be editable in EnterpriseView.
4. "Save and Apply Configuration Changes" (on page 60).

Schedule and Activate the UCMDB Asset Synchronization Job

After you define all of the required parameters for connecting with UCMDB, you can schedule and activate the UCMDB Asset Synchronization job.

For more information on the flow of the Synchronization job, see "About UCMDB Asset Synchronization Job" (on page 26).

To schedule and activate a synchronization job

1. In EnterpriseView, click **Administration > Configuration**.
2. In the left pane, click **Integrations > UCMDB > Asset Synchronization**.Click the configuration management system that you are integrating with:

- **HP Universal CMDB 8**
- **HP Universal CMDB 9**

3. In the left pane, click **Schedule Job**, and then, in the right pane, do the following:
   - **Connector Name:** Enter a name for the UCMDB system to which you want to connect. This is the name that is displayed in the **Source** property of the asset.
   - **Job Schedule**: Enter a Cron expression.

     For example, to run the job once every hour, every day, enter **0 0 0/1 * * ?**

     For more information , see "Appendix B: Learn About Cron Expressions" (on page 66).
   - Select the **Activate Job** check box.
4. "Save and Apply Configuration Changes" (on page 60).

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

Reverse Relation Direction

This task is relevant only if any part of the UCMDB Data Model is reversed to the business model in EnterpriseView. You can decide whether to reverse the relation direction, for any UCMDB relation type defined in EnterpriseView.

To reverse relation direction

1. In EnterpriseView, click **Administration > Configuration**.
2. In the left pane, click **Integrations > UCMDB > Asset Synchronization**. Click the configuration management system that you are integrating with:
   - **HP Universal CMDB 8**
   - **HP Universal CMDB 9**
3. Click **Relation**, and then select the **Reverse** check box for the type of relation that you want to reverse.
4. "Save and Apply Configuration Changes" (on page 60).

Integrate with ArcSight Enterprise Security Manager

You can integrate with ArcSight ESM in order to synchronize the EnterpriseView business model with ArcSight ESM assets, to import security threats for monitoring purposes, or for both purposes.

Integrating with ESM involves preparation in EnterpriseView as well as in ArcSight ESM. Before you begin the integration process, the ArcSight ESM administrator must install an ArcSight Resource Bundle (*.arb) file. This file defines the parameters of data from the ESM data source that will be delivered in the EnterpriseView Report (in the form of a .csv file). For more information, see "Importing the Asset and Threat Reports in ArcSight ESM" (on page 64). The name of the file is **EnterpriseView_v1.arb** and it is located in **<installation folder>/resources/**. The EnterpriseView Report will be triggered by EnterpriseView and will be used to create a file (.csv) that includes asset/security threat information.

The ArcSight ESM administrator should provide you with connection parameters. After you have gathered all the information from the ArcSight ESM administrator, you can begin the integration process, as described in "How to Integrate with ESM for Asset Synchronization" (on page 32) and in "How to Integrate with ESM to Import Threats" (on page 39).

After EnterpriseView is fully integrated with ArcSight ESM, the Synchronization job runs periodically, according to the schedule that you defined. To learn more about the Asset Synchronization job, see "About ArcSight ESM Asset Synchronization Job" (on page 32). To learn more about the security threats import job, see "About ESM Security Threats Job" (on page 39).

About ArcSight ESM Asset Synchronization Job

The Asset Synchronization Job periodically imports all of the ArcSight ESM elements from ArcSight ESM into EnterpriseView, as follows:

1. The ArcSight Resource Bundle (*.arb) file triggers the creation of the EnterpriseView Asset Report.
2. The ArcSight ESM Report contains all of the asset information, according to the asset mapping between these two applications. Each record in the report represents an asset.
3. ArcSight ESM assets and their properties are converted into EnterpriseView assets and relations. For more information on mapping logic, see "Map Asset Types with ESM" (on page 33).
4. The process checks the EnterpriseView database for each of the assets/relations.
   - If the **element does not exist** in the database, then the process writes that element to the database.
   - If the **element changed**, then the process updates these changes in the database.
5. Outdated assets and relations are deleted from the EnterpriseView database (meaning that they no longer exist in the database).

How to Integrate with ESM for Asset Synchronization

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

The following procedure outlines the steps for integrating with ArcSight ESM. This procedure includes steps for configuring asset synchronization. For information on configuring security threat import, see "How to Integrate with ESM to Import Threats" (on page 39).

1. **Define connection parameters**. Define the parameters necessary for connecting with ArcSight ESM. These parameters must be provided to you by the ArcSight ESM administrator. Follow the instructions in "Define Connection Parameters with ESM" (on page 33).
2. **Review Default Asset Type Mapping**. Review the default asset type mappings that are included in EnterpriseView to see whether they reflect your business model. If required, follow the instructions in "Map Asset Types with ESM" (on page 33) to tailor the mapping to your needs.
3. **Define Imported Asset Type properties**. Decide which asset properties will be imported from ArcSight ESM, as described in "Define Imported Asset Type Properties" (on page 30).
4. **Schedule and activate the Synchronization job** in order to complete the process, as described in "Schedule and Activate ArcSight ESM Job" (on page 34).

Define Connection Parameters with ESM

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

To define connection parameters with ArcSight ESM

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

ArcSight ESM Integration Parameters

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

4. "Save and Apply Configuration Changes" (on page 60).

Map Asset Types with ESM

ArcSight ESM holds assets that represent IP addresses in a flat file format. When these assets are imported to EnterpriseView they are converted into the EnterpriseView business model format, where the IP asset is the primary asset. Some of the IP Address properties that are imported from ESM are kept as properties in the EnterpriseView IP asset (Name, Description, DNS Name, MAC Address, IP Address), while the following properties are converted into actual EnterpriseView assets:

- **Operating System Name** is converted into an asset type from the Infrastructure Element category.
- **Zone** is converted to an asset type from the Business category.
- **Location** is converted to an asset type from the Location category.

Note: In ESM, the only mandatory property for an IP Address asset is the IP Address; the rest of the properties are optional. If the optional properties of the ArcSight ESM assets are populated, then the corresponding EnterpriseView asset type is created for each one. Therefore, the imported business model will be more comprehensive if more properties have values.

You can change the default mapping for the following properties:

- **Zone**
- **Location**

To edit mapping with ArcSight ESM asset properties

1. In EnterpriseView, click **Administration > Configuration**.
2. In the left pane, click **Integrations > ArcSight ESM > Asset Synchronization > Asset Type Mapping**.
3. On the **Asset Type Mapping** page, do the following:
   - From the **Select Business asset type for ESM Zone** drop-down, select the business asset type that you want to create for all assets in ArcSight ESM that have defined zones. The default is **Zone**.
   - From the **Select Location asset type** drop-down, select the Location asset type that you would like to create for all assets in ArcSight ESM that have a populated Location field. The default is **City**.
4. "Save and Apply Configuration Changes" (on page 60).

Schedule and Activate ArcSight ESM Job

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

For more information on the jobs, see "About ArcSight ESM Asset Synchronization Job" (on page 32) and "About ESM Security Threats Job" (on page 39).

To schedule and activate a synchronization job

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

     For example, to run the job once every hour, every day, enter **0 0 0/1 * * ?**

     For more information , see "Appendix B: Learn About Cron Expressions" (on page 66).
   - Select the **Activate Job** check box.
4. "Save and Apply Configuration Changes" (on page 60).

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

Import Assets From CSV

You can synchronize your business model with an asset repository that does not integrate with EnterpriseView by exporting the business model information to CSV files and configuring the CVS Asset Synchronization job. For more information, see "How to Import Assets from CSV" (on page 37).

The business model information from your asset repository needs to be extracted into two files: one that includes asset information and one that includes relation information. The asset file is mandatory and the relations file is optional. If the asset file is missing, then the job fails; if the relations file is missing, the assets are imported without relations. For more information on the synchronization job, see "About CSV Asset Synchronization Job" (on page 36).

CSV file format

- EnterpriseView supports only comma-separated (.csv) file formats.
- The files must be stored in a UTF-8 format if a non-Latin alphabet is used.
- The data in the asset file must be filled according to the relevant properties for each asset category.
- All fields are alphanumeric except for **criticalityLevel** and **businessValue**, which are integers.
- The asset **Type** name must be accurate in order to display the appropriate icon for that type in EnterpriseView. If the type does not exist in EnterpriseView, then the icon displayed for that type is a question mark.

Asset file header

The header record of the asset file must contain the following columns:

- Category (mandatory)
- Name (mandatory)
- Description
- Owner login name
- Type (mandatory)
- ExternalId (mandatory)
- AddressLine1
- AddressLine2
- City
- State
- Country
- ZipCode
- coordinate-latitude
- coordinate-longitude
- criticalityLevel
- businessValue
- Operating system name
- Operating system version
- Application name
- Application version

- dnsName
- ipAddress
- macAddress

Relation file header

- SourceExternalId
- DestinationExternalId

About CSV Asset Synchronization Job

The CSV Asset Synchronization Job periodically imports assets and relations from a CSV file into EnterpriseView, as follows:

1. Assets are read from the asset file. This file is mandatory. If the job cannot locate the asset file, then the job will fail.
2. Relations are read from the relation file. This file is optional.

   The following table includes errors that can occur during this process and their impact on the process:

Error	Action
External ID duplication.	Job fails.
The relations file includes a circular connection between assets.	Job fails.
One of the following mandatory fields is missing: External ID, Name, Category, and Type.	Record is skipped.
The CSV asset category is not mapped to a EnterpriseView asset category.	Record is skipped.
The criticality level or the business value of an asset is not an integer.	Record is skipped.

3. The elements in the CSV file are converted into EnterpriseView assets and relations.
4. The process checks the EnterpriseView database for each asset and relation.

   > **Note:** If the category of an asset was changed in the CSV file, then a new asset is created and the old asset is deleted. Any controls applied to that asset, along with risk and policy assessments, are deleted.

   - If the **element does not exist** in the database, then the process writes that element to the EnterpriseView database.
   - If the **element changed**, then the process updates these changes in the EnterpriseView database.
5. Outdated assets and their relations (meaning that they no longer exist in the CSV file) are deleted from the EnterpriseView database.

How to Import Assets from CSV

Before you begin, make sure you are acquainted with the synchronization job, as described in "About CSV Asset Synchronization Job" (on page 36).

The following procedure outlines the steps for importing assets from a CSV file:

1. **Configure CSV File Settings**. Follow the instructions in "Configure CSV File Settings" (on page 37).
2. **Map Asset Categories**. Follow the instructions in "Map Asset Categories with CSV" (on page 37).
3. **Define Imported Asset Type properties**. Decide which asset properties will be imported from CSV, as described in "Define Imported Asset Type Properties" (on page 30).
4. **Schedule and activate the Synchronization job**. In order to complete the process, as described in "Schedule and Activate CSV Job" (on page 38).

Configure CSV File Settings

To configure CVE file settings

1. In EnterpriseView, click **Administration > Configuration**.
2. In the left pane, click **Integrations > CSV File > Configuration**.
3. On the **Configuration** page, enter the following information:

Parameter	Description
Connector Name	Enter a logical name for the asset repository from which you are importing. This is the name that is displayed in the **Source** property of the asset.
Asset File path	The location of the asset file that is imported into EnterpriseView. The file can be placed anywhere in the network, as long as EnterpriseView can access the path.
Relation File Path	The location of the relation file that is imported into EnterpriseView. The file can be placed anywhere in the network, as long as EnterpriseView can access the path.
Max Business Criticality Level in Source	Enter the upper limit of the business criticality in the asset repository from which you are importing your business model. The criticality level range in the asset repository from which you are importing your business model might be different than the one employed by EnterpriseView. EnterpriseView uses a range of 0 to 10. During the import process, the criticality level is normalized according to this parameter.

4. "Save and Apply Configuration Changes" (on page 60).

Map Asset Categories with CSV

You need to map the asset categories that are defined in EnterpriseView to the asset categories defined in the asset CSV file, in order for EnterpriseView to convert the categories.

To map asset categories

1. In EnterpriseView, click **Administration > Configuration**.
2. In the left pane, click **Integrations > CSV File > Asset Category Mapping**.
3. On the **Asset Category Mapping** page, edit the **CSV Asset Category** column.
4. If more than one CSV asset category is mapped to an EnterpriseView asset category, you can add another mapping by clicking the **Add configuration to configuration set** button, and entering the required information.

   > **Note:** Make sure to enter the exact asset category name. Records with an inaccurate name are skipped during the import process.

5. "Save and Apply Configuration Changes" (on page 60).

Schedule and Activate CSV Job

After you define all of the required CSV job settings, you can schedule and activate the CSV Asset Synchronization job.

For more information on the flow of the synchronization job, see "About CSV Asset Synchronization Job" (on page 36).

To schedule and activate a synchronization job

1. In EnterpriseView, click **Administration > Configuration** .
2. In the left pane, click **Integrations > CSV File > Configuration**.
3. In the right pane, enter the following information:
   - **Job Schedule**: enter a cron expression.

     For example, to run the job once every hour, every day, enter **0 0 0/1 * * ?**

     For more information , see "Appendix B: Learn About Cron Expressions" (on page 66).
   - Select the **Activate Job** check box.
4. "Save and Apply Configuration Changes" (on page 60).

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

Import Security Threats from an SIEM System

EnterpriseView allows you to import security threats regularly from a Security Information and Event Management (SIEM) system, providing near real-time monitoring capabilities on the threats imposed on your organization's assets—on all levels (physical assets and business assets). This information is displayed graphically, either per asset or for multiple assets and allows you to identify security threat trends over selected time periods.

EnterpriseView supports importing security threats from ArcSight ESM. ArcSight ESM analyzes and correlates every security event that occurs across the organization–every login, log ff, file access, database query, and so on. These security events are scored according to priority factors in order to determine the threat level on a particular asset. The process results in a priority score, using a scale of 0 to 10 (10 being the most significant value), to depict threat level.

To configure importation of security events from ArcSight ESM, see "Integrate with ArcSight Enterprise Security Manager" (on page 31). For information on the event import job, see "About ESM Security Threats Job" (on page 39).

About ESM Security Threats Job

The Security Threats Job periodically imports all of the newly added ArcSight ESM security threats from ArcSight ESM into EnterpriseView, as follows:

1. The ArcSight Resource Bundle (*.arb) file triggers the creation of the EnterpriseView security threats Report.

   The ArcSight ESM Report contains all of the security threat information, per asset. This information includes scores for all the factors comprising the asset priority level.

2. The security threat rating is processed into a score between 0 and 10, according to the weighting scheme defined in "Apply a Weighting Scheme to Priority Factors" (on page 40). The information is displayed graphically via the ESM Threat View component.

How to Integrate with ESM to Import Threats

The following procedure outlines the steps for integrating with ArcSight ESM. This procedure includes steps for configuring security threat import. For information on configuring asset synchronization, see "How to Integrate with ESM for Asset Synchronization" (on page 32).

1. Skip this step if you have already configured integration for asset synchronization with ESM.

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

   Define connection parameters. Define the parameters necessary for connecting with ArcSight ESM. These parameters must be provided to you by the ArcSight ESM administrator. Follow the instructions in "Define Connection Parameters with ESM" (on page 33).

2. **Review the default weighting scheme of priority factors**. If required, you can modify the weight of each of the priority factors, as described in "Apply a Weighting Scheme to Priority Factors" (on page 40).

3. **Schedule and activate the Synchronization job** in order to complete the process, as described in "Schedule and Activate ArcSight ESM Job" (on page 34).

Apply a Weighting Scheme to Priority Factors

In ArcSight ESM, a priority is defined as a value used to prioritize the investigation of security event. The calculation of a priority is comprised of the following factors:

- Asset criticality
- Model confidence
- Relevance
- Severity

Imported security threats include a score for each factor, per asset. For more information on score calculation in ArcSight ESM, see "Threat Score Calculation on Asset - Example" (on page 65).

These scores are processed into one weighted average score between 0 and 10 representing the priority rating.

You can apply different weights to these factors to reflect the business logic of your organization.

To apply a weighting scheme to priority factors

1. In EnterpriseView, click **Administration > Configuration**.
2. In the left pane, click **Integrations > ArcSight ESM > Asset Threat Synchronization > ESM Priority Factors**.
3. On the **ESM Priority Factors** page, in the **Weight text box**, enter a weight (numerical value) for all **Priority Factors**. For details on each priority factor, see "Factors Used to Calculate an Asset Threat Score" (on page 63).
4. "Save and Apply Configuration Changes" (on page 60).

Import Vulnerabilities From Vulnerability Assessment Tools

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

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

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

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

Vulnerability Assessment Tool	ArcSight SmartConnector
Tenable Nessus Vulnerability Scanner	Tenable Nessus .nessus File
McAfee Vulnerability Manager (Foundscan)	McAffee Vulnerability Manager DB
Qualys Guard	Qualys Vulnerability Scanner File

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

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

To import vulnerabilities, first "Install and Configure ArcSight SmartConnector" (on page 42) and then "Schedule and Activate Vulnerabilities Import Job" (on page 44).

About the Vulnerability Import Job

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

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

   <EnterpriseView Installation folder>/vm/import/pending/<connector ID>

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

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

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

   c. The vulnerability instance records are saved in the EnterpriseView database.

3. The process aggregates vulnerability instances that represent the same vulnerability into a single vulnerability occurrence, according to the vulnerability name and location. For more information on these properties, see "Vulnerability Properties" (on page 1).

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

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

6. Outdated vulnerability occurrences (no vulnerability instances have been reported for over an N number of day) are closed, with remediation status Automatically Closed. The **Automatically close vulnerability after (days)** parameter is configured in "Schedule and Activate Vulnerabilities Import Job" (on page 44).

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

   - Successfully processed files are moved to the <EnterpriseView **Installation folder>/vm/import/done/<connector ID>** folder.

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

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

Install and Configure ArcSight SmartConnector

Before you begin:

For all installation instructions, including system requirements for the connector that you want to install, see the *SmartConnector Configuration Guide* for:

- Tenable Nessus .nessus File
- McAffee Vulnerability Manager DB
- Qualys Vulnerability Scanner File

In order for EnterpriseView to work with ArcSight SmartConnectors, you need to run a configuration tool after each installation. The configuration tool configures the connector to write the CSV files containing the vulnerability information to the following folder on the EnterpriseView server:

<EnterpriseView installation folder>\vm\import\pending\<connector ID>

> **Note:** Do not add or modify the CSV file destination folder. There can be only one destination folder per connector.

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

Perform the following procedures sequentially for each connector that you want to install. The same executable is used for all ArcSight SmartConnectors.

To install ArcSight SmartConnector

1. On the server that you want to install, from the **\Connectors** folder of your HP ArcSight EnterpriseView installation medium, start the ArcSight SmartConnector Installer by running one of the following:

   ArcSight-<version>-Connector-Win.exe

   ArcSight-<version>-Connector-Linux.bin

2. Run the wizard with the default settings until the installation is completed. Enter the required information:
   a. When prompted to select the destination type for the connector, select **CSV File**.
   b. When prompted to select a **Mode**, select **Automatic**.
   c. When prompted, select **Yes, I want to configure the SmartConnector to run as a service**.

   A main folder for all connectors is created. For each connector that you install, a dedicated folder is created under the main folder.

To configure ArcSight SmartConnector

1. From your HP ArcSight EnterpriseView installation medium, copy the following lines:

   \Tools\vm-connector-configuration.zip

   To this directory:

   <ArcSight SmartConnector main folder>\<folder of connector you want to configure>

   > For example: ArcSightSmartConnectors\current

2. Extract the zip file to a separate folder.
3. Open the following folder from the command line:

   <ArcSight SmartConnector root folder>\<folder of connector you want to configure>\<extracted zip folder>\bin

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

   - For a 64-bit Windows operating system
   - For a 32-bit Windows operating system
   - For a 64-bit Linux operating system
   - For a 32-bit Linux operating system

4. Run the configuration tool with a parameter :

   run_vm_connector_config_*.* <path to pending folder>

> **Note:** Make sure that the connector has **write** permissions for the following folder in EnterpriseView:
>
> **<EnterpriseView installation folder>\vm\import\pending**

> **Note:** If you are working on a Linux operating system, make sure that the shell script has execute permissions.

5. If you installed a **Tenable Nessus .nessus File** SmartConnector and if your Nessus scanner is version 4.2 or higher, do the following:

   Copy file **nessus_dotnessus_v2.vulns.xqueryparser.properties**

   From:

   <EnterpriseView installation folder>\Connectors\ArcSight SmartConnectors\Add-ons:

   To:

   <ArcSight SmartConnector root folder>\<Nessus folder>\user\agent\fcp\nessus_file

6. If you installed a **Qualys Vulnerability Scanner File** SmartConnector, do the following:

   Copy file **qualys_xml_file.vulns.xqueryparser.properties**

   From:

   <EnterpriseView installation folder>\Connectors\ArcSight SmartConnectors\Add-ons:

   To:

   <ArcSight SmartConnector root folder>\<Nessus folder>\user\agent\fcp\qualys

7. Start the ArcSight SmartConnector service.

Schedule and Activate Vulnerabilities Import Job

After the connector/connectors are running, you need to schedule and activate the Vulnerabilities Import Job. For more information on the job, see "About the Vulnerability Import Job" (on page 41).

To schedule and activate the Vulnerabilities Import Job

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

      For example, to run the job at 02:00, every day, enter **0 0 2 * * ?**

      For more information , see "Appendix B: Learn About Cron Expressions" (on page 66).

   c. Select the **Automatically Close Vulnerabilities** check box in order to enable automatic closing of vulnerabilities.

   d. If you selected the **Automatically Close Vulnerabilities** check box, then in the **Automatically Close Vulnerability After (days)**, enter the number of days after which the remediation status for outdated vulnerability occurrences, meaning that no vulnerability instances have been reported for over an X number of day, is changed to Automatically Closed.

4. "Save and Apply Configuration Changes" (on page 60).

Configure Asset Vulnerability Score Aggregation Parameters

You can configure the asset vulnerability score aggregation parameters to better suit your business needs and your organization structure. For more information on these parameters, see the *Asset Vulnerability Score Aggregation Mechanism* section in the *HP ArcSight EnterpriseView User Guide*.

To configure asset vulnerability score aggregation parameters

1. In EnterpriseView, click **Administration > Configuration**.
2. In the left pane, click **Vulnerability Management > Vulnerability Score Settings > Vulnerability Aggregation**.
3. On **the Vulnerability Aggregation** page, enter the following information:
   - **Maximum Contained Assets in Calculation**
   - **Contained Assets Multiplier**

   > **Note:** This change recalculates scores for the entire business model, therefore it might take some time until the updated scores are apparent.

4. "Save and Apply Configuration Changes" (on page 60).

Configure Vulnerability Score Ranges

You can configure the vulnerability score ranges via the Configuration module. Vulnerability scores are displayed with one of the following icons:

☑ Low score

⚠ Medium score

☒ High score

The score range is between 0 and 10.

To configure vulnerability aggregation score ranges

1. In EnterpriseView click **Administration > Configuration**.
2. In the **Configuration** module, in the left pane, click **Vulnerability Management > Vulnerability Score Settings > Vulnerability Score Ranges**.

3. In the right pane, enter the following information:
    - **Lower Limit for Medium Range**. Determines the low range.
    - **Upper Limit for Medium Range**. Determines the medium and high ranges.

    > **Note:** The **Lower Limit for Medium Range** must be smaller than the **Upper Limit for Medium Range**.

4. "Save and Apply Configuration Changes" (on page 60).

Configure Vulnerability Dashboard Settings

The Vulnerability Dashboard provides comprehensive information about the vulnerabilities in your organization. You can configure the severity of the statistics that are displayed in the Vulnerability Dashboard according to your organization's business preferences. This data includes:

- The number of assets with open vulnerabilities attached. This data is displayed in the Most Vulnerable Contained Assets component. You can define high, medium, and low ranges for this data.
- The number of unhandled vulnerabilities (vulnerabilities that have a remediation status of New or Reopened). This data is displayed in the Vulnerabilities with the Highest Scores component. You can define high, medium, and low ranges for this data.

To configure vulnerability dashboard settings

1. In EnterpriseView click **Administration > Configuration**.
2. In the **Configuration** module, in the left pane, click **Vulnerability Management > Vulnerability Status Ranges**.
3. Click **Ranges for Impacted Assets with Open Vulnerabilities**, and then enter the following information:
    - **Upper Limit for Low Range (as percent)**. Enter a number between 0 and 100, not inclusive. Determines the low and medium ranges.
    - **Upper Limit for Medium Range (as percent)**. Enter a number between 0 and 100, not inclusive. Determines the high range.
4. Click **Ranges for Vulnerability Remediation Status New and Reopened**, and then enter the following information:
    - **Upper Limit for Low Range (as percent)**. Enter a number between 0 and 100, not inclusive. Determines the low and medium ranges.
    - **Upper Limit for Medium Range (as percent)**. Enter a number between 0 and 100, not inclusive. Determines the high range.

    > **Note:** The **Upper Limit for Low Range** must be smaller than the **Upper Limit for Medium Range**.

Configure Automatic Policy Assessment

As part of the EnterpriseView security policy compliance management framework, EnterpriseView provides both manual and automatic assessment capabilities. Manual assessment performed by auditors is described in the *Audit Assets* section in the *HP ArcSight EnterpriseView User Guide*. Policy assessments can be imported regularly from external systems, both commercial and home-grown, using EnterpriseView REST API, as described in the *HP ArcSight EnterpriseView REST API Developer Guide*.

EnterpriseView integrates with HP Server Automation (SA), using its audit and compliance management capabilities in order to automate the policy assessment (auditing) process, as described in "How to Integrate with HP Server Automation" (on page 47). For more information on SA, see *SA User Guide: Audit and Compliance*.

> **Note:** After Installing SA, you must install the SA Compliance Content Streams from the HP Live Network in order to integrate with EnterpriseView.

SA includes security compliance checks for various operating systems. In EnterpriseView, Unified Compliance Framework (UCF) controls are mapped to SA security compliance checks. A single control can be represented by one or more checks.

> **Example:**
>
> The following UCF control:
>
> "PCI 2.0, Establish and maintain an identification, authentication, and access rights management plan."
>
> Is mapped to numerous security check, following are examples:
>
> - "Verify that there are no accounts with empty password fields."
> - "Max password age of active accounts is 90."
> - "Password MIN length is at least 7."

Each SA check can either be compliant or not compliant. These values are normalized by EnterpriseView to a compliance score between 0 and 100. The final compliance score of the control is the average of all the compliance score of all the checks mapped to this control.

For each assessment, a note is created with the details of the assessment.

How to Integrate with HP Server Automation

The following procedure outlines the steps for integrating with SA. This procedure includes steps for configuring policy assessment importation.

1. "Install Server Automation Connector" (on page 48)
2. "Define Server Automation Connection Parameters " (on page 48)
3. "Run SA Connector for the First Time (Manual)" (on page 48)
4. Schedule and activate the SA connector:

- In Windows, use the Task Scheduler
- In Linux, use a Cron job

> **Note:** it is recommended that you synchronize scheduling of the SA connector with the automatic checks in SA.

5. "Monitor and Troubleshoot the Server Automation Connector" (on page 49)

Install Server Automation Connector

The SA connector can be installed on the EnterpriseView machine, on the SA machine, or on any other machine in your network. Before you install the SA connector, make sure that the ports to the EnterpriseView machine and the SA machine are open on the machine on which you intend to install the SA connector. The default port for EnterpriseView is 8080 and the default port for SA is 1032.

To install the server automation connector

From your HP ArcSight EnterpriseView installation medium, unzip the following file:

sa-connector.zip

Define Server Automation Connection Parameters

After you have installed the SA connector, you need to define the connection parameters between SA and EnterpriseView. This is done using the property files in the SA connector directory.

To define SA connection parameters

1. On the machine on which the SA connector is installed, open the following directory:

   <SA connector installation directory>\conf

2. Enter the following information in both the **EnterpriseView-server.properties** and **sa-server.properties**, and then save the files.
   - **Host**: Enter the IP address of the EnterpriseView/SA server.
   - **Port**: Enter the port of the EnterpriseView/SA server. The default port for EnterpriseView is 8080 and the default port for SA is 7878.
   - **Username** and **Password**: Enter the credentials of the EnterpriseView/SA server.

   > **Note:** The credentials that you enter must have System Administrator permissions.

Run SA Connector for the First Time (Manual)

It is recommended that you schedule SA to run automatically. However, the first time that you run the SA connector is manual in order to verify the connection between the connector and SA and the connector and EnterpriseView and to verify the entire importation process.

> **Note:** The length of the first import process depends on the amount of assessment data that is imported from SA. However, subsequent runs, which import only the incremental data, are shorter.

To run the SA connector manually from a Windows operating system

1. Open the following directory:

   `<SA connector installation directory>\bin`

2. Double click the following file:

   run_job.bat

To run SA connector manually from a Linux operation system

1. Make sure that the shell script has executable permissions.
   - Open the `<SA connector installation directory>/jre/linux` directory and run the following command:

     chmod +x –R .

   - Open the `<SA connector installation directory>/bin` directory and run the following command:

     chmod +x run_job.sh

2. In the `<SA connector installation directory>/bin` directory, run the following file:

   run_job.sh

Monitor and Troubleshoot the Server Automation Connector

The SA connector imports assessments within a range of dates. The start date is dynamic and the end date is the current date. The process has a three-time retry mechanism. In case of failure, the consequent run will begin on the same start date as the failed run.

You can validate the automatic assessment process at any time after the connector has been run once. The SA connector is not monitored via EnterpriseView; it is monitored via logs in the SA connector environment located in the following directory:

<SA connector installation directory>\logs

The **logs** directory is created after the connector has been run once. It includes the following logs:

- **sa-connector.log**: Includes the status of the process that was run.
- **all-errors.log**: Includes all the assessments that have been discarded, such as assessments on assets with an unknown IP address and assessments on controls that are not applied to any asset.
- **batch.log**: Includes information on batch metadata.
- **hibernate.log**: Includes information on the database connection.

Configure Risk Score Aggregation Method

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

To configure risk score aggregation method

1. In EnterpriseView, click **Administration > Configuration**.
2. In the **Configuration** module, in the left pane, click the **Risk Aggregation Method** folder, and then click the **Risk Aggregation Method** page.
3. In the right pane, from the **Risk Aggregation Method** drop-down list, select an option:
   - **Average** (default)
   - **Override Contained Assets**
   - **Average of Contained Assets**

   For more information on the different methods, see the *Risk Score Aggregation Mechanism* section in the *HP ArcSight EnterpriseView User Guide*.
4. "Save and Apply Configuration Changes" (on page 60).

Manage SAP BusinessObjects Report Settings

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

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

To update SAP BusinessObjects reports settings

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

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

4. "Save and Apply Configuration Changes" (on page 60).

EnterpriseView Workspace

EnterpriseView comes with a variety of out-of-the-box dashboard pages, based on common needs of IT and GRE personas, such as system administrators, auditors, and senior management. EnterpriseView administrators can create role-based dashboards for different types of users by mixing and matching components from the component gallery to form a rich UI experience. For each page, the administrator can define the layout of components on the page, and their interaction with one another, as described in "Set Up Wiring Between Components" (on page 57).

Create a Customized Dashboard Page

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

To create a customized dashboard page

1. In EnterpriseView , click **Administration > Dashboard Builder**.

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

2. On the **Dashboard Builder** window, click **New Page** button.
3. "Configure Page Layout" (on page 53).

   It is recommended that you plan in advance which components you want to place on your page and how they should be arranged.

4. In an empty layout area, click the **Add Component** button.
5. On the **Component Gallery** dialog box, in the left pane, select the **Executive View** category.
6. From the right pane, drag the **BusinessObjects Reports** component to the empty layout space.
7. Close the **Component Gallery** dialog box.
8. In the BusinessObjects Reports component, from the **Reports** list, select the report you want to use in the dashboard that you are creating.
9. If the report requires parameters, select one of the following:

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

   - To create a report/dashboard for a specific asset/policy, select either **Select a Specific Asset** or **Select a Specific Policy**.
   - To create a dynamic report/dashboard, that receives the asset/policy as a parameter using

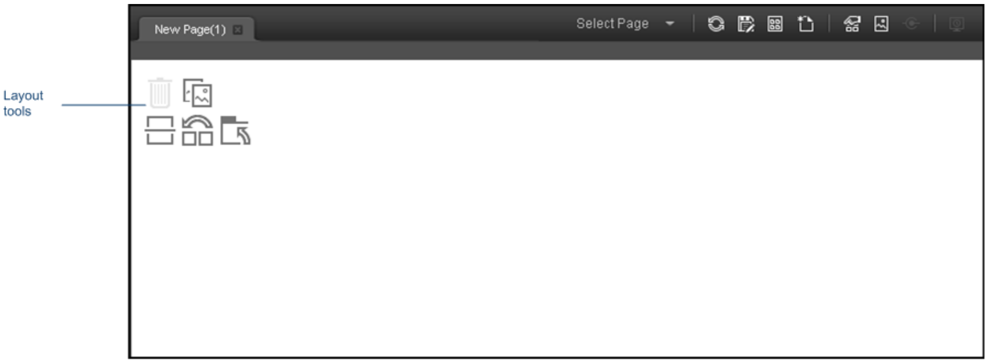
the wiring capability, select either **Set up wiring between this component and an Asset Selector component** or **Set up wiring between this component and a Policy and Asset Selector component**.

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

10. To remove a component from a page, select a component, and then click the **Remove Component** ☒ button.
11. Click **Create Report**.
12. "Save Page" (on page 54).

Configure Page Layout

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



To configure page layout

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

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

Layout tool	Description
⊟	**Split** Click to divide a vertical layout into two layouts, one above the other.
◫	**Split**

Layout tool	Description
	Click to divide a horizontal layout into two layouts, side by side.
	Switch to Horizontal Click to change the layout from vertical or tabbed to horizontal. Components placed in this area will be added side by side.
	Switch to Vertical Click to change the layout from horizontal or tabbed to vertical. Components placed in this area will be added one above the other.
	Switch to Tabs Click to change the layout from vertical or horizontal, to a tab layout. Components placed in this area will be added as tabs.
	Add Component Click to open the Component Gallery. You can then double-click a component to place it in the layout area.
	Remove Layout Click to remove a layout from the page.

Save Page

Save the page to the Page Gallery.

To save a page

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

> **Note:** Pages that are saved to a specific category are displayed under that category in

> the EnterpriseView Homepage and in the navigation bar. Pages in the **Not Categorized** group are not displayed.

3. Refresh your browser.

Manage Pages

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

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

To assign a page to a category

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

To clone a page

1. On the EnterpriseView toolbar, click the **Page Gallery** button.
2. On the **Page Gallery** dialog box, select the category check box from the categories on the left side, and then select the page.
3. Click the **Clone Page** button.

To delete a page

1. On the EnterpriseView toolbar, click the **Page Gallery** button.
2. On the **Page Gallery** dialog box, select the category check box from the categories on the left side, and then select the page.
3. Click the **Delete Page** button. A confirmation message is displayed. Click **Yes**.

Edit Page Layout

To edit page layout

1. Select the page that you want to lay out again from the **Select Page** drop-down on the EnterpriseView toolbar.
2. Click the **Edit Page Layout** button.

   The components are hidden and the layout of the page is displayed.

3. Lay out the page again using the layout tools, as described in "Configure Page Layout" (on page 53), and then click the **Edit Page Layout** button to exit editing.
4. "Save Page" (on page 54).

Manage Components

Components are areas on a page that display information relevant to EnterpriseView users' business tasks. The Component Gallery contains components that can be used within EnterpriseView, grouped by categories. You can add, edit and delete user-created component categories via the Component Gallery, as described in "Manage Component Categories" (on page 56). You can also create external components, as described in "Create an External Component" (on page 57).

Each component has permissions that are relevant to the function that it provides. When you create a new page, the components that you choose define which roles will be able to access the page. Only users with roles that include permissions for all of the components on the page are granted access to that page. For more information on the permissions of each component, see "Roles and Permissions" (on page 24).

Manage Component Categories

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

To create a new component category

1. On the EnterpriseView toolbar, click the **Components** button.
2. On the **Components Gallery** dialog box, click the **New Category** button on the top left side.
3. In the **New Category** dialog box, in the **Name** field, enter a name for the category that you are creating, and then click **OK**.

To rename a component category

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

To delete a component category

1. On the EnterpriseView toolbar, click the **Components** button.
2. On the **Components Gallery** dialog box, from the list of categories on the left side, select the

check box of the category you want to delete, and then click the **Delete Category** button. A confirmation message is displayed. Click **Yes**.

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

Create an External Component

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

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

To create an external component

1. On the EnterpriseView toolbar, click the **Components** button.
2. On the **Components Gallery** dialog box, in the left pane, click the **Add External Component** button.
3. On the **New Component** dialog box, do the following, and then click **OK**:
   a. In the **Name** field, enter a name for the component.
   b. In the **URL** field, enter the URL.
   c. Click **Categorize Component** to expand the section. Select the check box of the category to which you want to add the component or click the **New Category** button to create a new one.

Set Up Wiring Between Components

The interaction between components on a page in EnterpriseView is called wiring. After you place components on a page, you can define how components interact with one another. In addition, a component can send a wiring context to another component indicating what has changed in the first component, and the second component can respond to this change. For example, you can set up a page so that if you select an asset in one component (source), the other components on the page display information relating to that asset (target).

Default pages have predefined wiring. You can define wiring for user-created pages as well as modify default wiring definitions.

To set up wiring between components

1. Do one of the following:

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

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

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

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

Dashboard Builder Toolbar

The Dashboard Builder toolbar enables you to create customized dashboards.

The following table describes the toolbar's functionality.

UI Element	Description
Select Page ▾	Select a page from this drop-down list to open the page in your workspace. The list contains the dashboards that are defined in the Page Gallery. The list is narrowed when you start typing a page name in this box.
⟳	**Refresh** Click to refresh the page.
🖫	**Save or Save As** Click to save the current page to the Page Gallery. A dialog box enables you to name the page, give the page a description, and select a category for the page. The description appears as a tooltip for the page in the Page Gallery. For more information, see "Save Page" (on page 54).
▦	**Page Gallery** Click to open the Page Gallery. The Page Gallery contains default pages, as well as pages you have saved. You can then edit page definitions, or open pages. For more information, see "Manage Pages" (on page 55).
🗋	**New Page** Click to create a new page. After opening a new page, you can configure its layout and add components. For more information, see "Create a Customized Dashboard Page" (on page 52).
▦	**Edit Page Layout**

UI Element	Description
	Click to modify the layout of an existing page. Use the Layout tools in the top left corner of each layout to modify the layout areas. For more information, see "Edit Page Layout" (on page 55). **Exit Editing** When you are done, click this button to stop editing.
🖼	**Components** Click to open the Component Gallery, which contains default components, as well as components you have added. You can edit component definitions, or add components to a page. For more information, see "Manage Component Categories" (on page 56).
⊸	**Page Wiring** Click to define the wiring between components; this determines how components interact with one another. For more information, see "Set Up Wiring Between Components" (on page 57).

Manage Configuration Sets

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

A configuration set contains the properties defined for the system. You can create any number of configuration sets and then select one with which to run your system. EnterpriseView maintains a history of all the configuration sets created. For more information, see "Select Configuration Set" (on page 60).

A new configuration set is initially saved as a draft. A draft is a configuration set that has not yet been activated. A draft can be edited only until it is first activated. The new configuration properties are only applied to EnterpriseView after a draft is activated. For details on how to activate a draft, see "Save and Apply Configuration Changes" (on page 60).

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

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

Select Configuration Set

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

Changing the configuration set will require you to log onto EnterpriseView again.

To select a configuration set

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

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

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

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

   In the **Activate Configuration Set** dialog box, click **Yes**.
5. Close the EnterpriseView application, and then access the application again.

Save and Apply Configuration Changes

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

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

To create a new configuration set

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

   A draft is a configuration set that has not yet been activated. After a draft is activated, the new configuration settings are applied to EnterpriseView.

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

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

Appendix A: Asset and Threat Reporting

ArcSight Enterprise Security Manager (ESM) provides content regarding assets and threats that can be viewed in two reports from the EnterpriseView interface. Both of these reports are generated in .csv format.

The following sections describe these reports and provide additional information about accessing them and interpreting their content. For more information about integration with EnterpriseView, see "Integrate with ArcSight Enterprise Security Manager" (on page 31).

About the Asset Report

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

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

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

.. /All Reports/JumpStart/ArcSight/EnterpriseView/Asset Report

About the Threat Report (URI)

The Threat report shows an average threat score for assets that have been targeted. By default, the report queries the event schema for the last hour. The system computes the average of the priority rating factors (Asset Criticality, Model Confidence, Relevance, and Severity) for each asset currently modeled in your ESM environment. The report is then generated in .csv format. It includes the following fields:

- Asset ID
- Asset Name
- IP Address
- Zone URI
- Hostname
- MAC address
- Asset Criticality – Average
- Model Confidence – Average
- Relevance – Average
- Severity – Average

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

../All Reports/JumpStart/ArcSight/EnterpriseView/Threat Report

Factors Used to Calculate an Asset Threat Score

Four factors are used to calculate a threat score. Each factor contributes a numeric value between 0 (lowest) and 10 (highest).

The following table describes the four factors used to calculate the threat score. These values are configurable with ArcSight assistance.

Priority Factor	Description
Model confidence	Whether the target asset has been modeled in ESM and to what degree.
Relevance	Whether an event is relevant to an asset based on whether it contains ports, known vulnerabilities, or both – and, if so, whether those vulnerabilities and ports are exposed on the asset.
Severity	An indicator of the event's history as far as exposure or vulnerability – for example, whether the system has been attacked or compromised before, or if the attacker scanned or attacked the network before. Scores are assigned based on the attacker and target's presence in one of ArcSight ESM's threat tracking active lists, whose contents are updated automatically by ArcSight ESM rules.
Asset criticality	Measures how important the target asset is in the context of your enterprise as set in the network modeling process by using the standard asset categories.

Priority Factor	Description
	`/System Asset Categories/Criticality/Very High` (+10) `/System Asset Categories/Criticality/High` (+8) `/System Asset Categories/Criticality/Medium` (+6) `/System Asset Categories/Criticality/Low` (+4) `/System Asset Categories/Criticality/Very Low` (+2) For example, customer-facing systems or devices with access to confidential information would be classified as criticality level of High, whereas a staging or test system may have a criticality level of Low.

Filter Event Processing

Depending on the number and type of assets currently stored in your ArcSight ESM environment, the Asset and Threat Reports could be extensive if you have a large number of assets. ArcSight ESM provides a filtering capability to specify conditions that focus on particular event attributes. Filters enable narrowing the number of events processed, allowing greater focus on the types of assets and vulnerabilities most relevant in your organization. For more information, see the *Filtering Events* section in the *ArcSight ESM User Guide*.

Filters are created as condition statements using ArcSight ESM's Common Conditions Editor (CCE), a Boolean logic editor. Conditions created in the CCE are expressions consisting of a value or variable, an operator (such as NOT, OR, AND), and a second value or variable by which the first value or variable is evaluated. For more information, see the *Common Conditions Editor* section in the *ArcSight ESM User Guide*.

The CCE can be used to create conditions that apply to specific categories, ranges, or zones of assets, as well as to specific types of threats.

The following queries in your ArcSight ESM environment can be modified as part of the CCE:

- `../All Queries/JumpStart/ArcSight/EnterpriseView/Asset Report`
- `../All Queries/JumpStart/ArcSight/EnterpriseView/Threat Report`

Importing the Asset and Threat Reports in ArcSight ESM

The Asset and Threat reports are available from a bundled file (EnterpriseView_v1.arb) in the ArcSight ESM Manager.

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

1. In the **ESM Manager Console**, in the **Navigator** panel, click the **Packages** tab.
2. Click the green down-arrow icon.
3. Select the **EnterpriseView_v1.arb** file, and click **Open**.

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

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

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

   /All Packages/JumpStart/ArcSight/EnterpriseView

Threat Score Calculation on Asset - Example

The following example shows how a threat score is calculated for an asset for which three events have been reported in the last hour ($Now-1h to $Now).

For each event, the report calculates a value between 0 and 10 for each of the priority factors.

	Model Confidence	Severity	Relevance	Asset Criticality
Event 1	10	8	10	10
Event 2	0	8	0	0
Event 3	8	4	8	6

It then computes an average value for each factor, which provides four values for the asset. In this example, those values are:

- Model Confidence 6
- Severity: 6.7
- Relevance 6
- Asset Criticality 5.3

Appendix B: Learn About Cron Expressions

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

Cron Expression Format

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

You can use the following special characters:

Cron Expression Special Characters

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

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

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