

# **HP EnterpriseView**

For the Windows Operating System

Software Version: 2.0

## **Deployment Guide**

Document Release Date: June 2013

Software Release Date: June 2013





## Legal Notices

### Warranty

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

The information contained herein is subject to change without notice.

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

### Restricted Rights Legend

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

### Copyright Notice

© Copyright 2011 - 2013 Hewlett-Packard Development Company, L.P.

Follow this link to see a complete statement of copyrights and acknowledgments for all HP ArcSight products: <http://www.hpenterprisesecurity.com/copyright>.

### Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

**This document is confidential.**



## Documentation Updates

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

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

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

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

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

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

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

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



## Support

Visit the HP Software Support Online web site at:

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

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

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

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

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

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

To find more information about access levels, go to:

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**





# Contents

Welcome to This Guide .....	13
About EnterpriseView .....	15
Install EnterpriseView .....	17
System Requirements .....	17
Integration Matrix .....	19
EnterpriseView Architecture Diagram .....	21
Prerequisites .....	22
Install SAP BusinessObjects Enterprise CMC .....	23
Configure BusinessObjects Enterprise .....	25
Run EnterpriseView Setup Wizard .....	29
Log On To EnterpriseView .....	31
EnterpriseView Post Installation Tasks .....	33
Connect to Active Directory .....	35
User Management .....	37
Add Roles .....	38
Assign Roles to a User or Group .....	39
Search Users .....	39
Roles and Permissions .....	40
Define a Named User in BusinessObjects Enterprise .....	49
Synchronize Assets with External Asset Repository .....	51
Integrate with HP Universal CMDB .....	51
About UCMDB Asset Synchronization Job .....	52
How to Integrate with HP Universal CMDB .....	52
Define Connection Parameters with UCMDB .....	53
Map Asset Category with UCMDB .....	54
Edit Field Mapping .....	55
Define Imported Asset Type Properties .....	56
Schedule and Activate the UCMDB Asset Synchronization Job .....	56

Reverse Relationship Direction .....	57
Integrate with ArcSight Enterprise Security Manager .....	58
About ArcSight ESM Asset Synchronization Job .....	58
How to Integrate with ESM for Asset Synchronization .....	59
Change ESM Session Timeout .....	60
Define Connection Parameters with ESM .....	60
Map Asset Types with ESM .....	61
Schedule and Activate ArcSight ESM Job .....	63
Import Assets From CSV .....	63
About CSV Asset Synchronization Job .....	65
How to Import Assets from CSV .....	66
Configure CSV File Settings .....	67
Map Asset Categories with CSV .....	68
Schedule and Activate CSV Job .....	68
Import Security Threats from an SIEM System .....	71
About ESM Security Threats Job .....	71
How to Integrate with ESM to Import Threats .....	71
Apply a Weighting Scheme to Priority Factors .....	72
Import Vulnerabilities From Vulnerability Assessment Tools .....	73
About the Vulnerability Import Job .....	74
Install and Configure ArcSight SmartConnector .....	75
Schedule and Activate Vulnerabilities Import Job .....	78
Configure Automatic Policy Assessment .....	81
How to Integrate with HP Server Automation .....	81
Install Server Automation Connector .....	82
Define Server Automation Connection Parameters .....	82
Run SA Connector for the First Time (Manual) .....	83
Monitor and Troubleshoot the Server Automation Connector .....	84
Manage Configuration Sets .....	85
Select Configuration Set .....	85
Migrate Configuration Data .....	86

Save and Apply Configuration Changes .....	87
<b>Security .....</b>	<b>89</b>
Encrypt Password .....	89
Change Encryption Algorithm .....	90
Encryption Properties .....	90
Enable SSL on the Server .....	92
Enable SSL on the Server with a Self-Signed Certificate .....	93
<b>Appendix A: Asset and Threat Reporting .....</b>	<b>97</b>
About the Asset Report .....	97
About the Threat Report (URI) .....	98
Factors Used to Calculate an Asset Threat Score .....	98
Filter Event Processing .....	99
Importing the Asset and Threat Reports in ArcSight ESM .....	100
Threat Score Calculation on Asset - Example .....	100
<b>Appendix B: Learn About Cron Expressions .....</b>	<b>103</b>



# Chapter 1

## Welcome to This Guide

Welcome to the HP 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 EnterpriseView" on page 15](#)

["Install EnterpriseView" on page 17](#)

["Log On To EnterpriseView" on page 31](#)

["EnterpriseView Post Installation Tasks" on page 33](#)

["Connect to Active Directory" on page 35](#)

["User Management" on page 37](#)

["Synchronize Assets with External Asset Repository" on page 51](#)

["Import Security Threats from an SIEM System" on page 71](#)

["Import Vulnerabilities From Vulnerability Assessment Tools" on page 73](#)

["Configure Automatic Policy Assessment" on page 81](#)

["Manage Configuration Sets" on page 85](#)

["Security" on page 89](#)

["Appendix A: Asset and Threat Reporting" on page 97](#)

["Appendix B: Learn About Cron Expressions" on page 103](#)



## Chapter 2

### About EnterpriseView

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

The main modules in EnterpriseView are:

- **Policy and Compliance Management:** This module enables you to assess and audit the assets in your organization. Use the policy builder to create customized policies and the Statement of Applicability (SoA) feature to apply controls to assets. EnterpriseView includes out-of-the-box policies, such as Unified Compliance Framework (UCF) enabling "audit once - comply with many" functionality.
- **Risk Management:** This module enables you to manage all aspects of the risk life cycle. Use the flexible and expandable threat library to define the threats that may potentially harm your organization, create threat scenarios by assigning threats to assets, analyze the risk and specify its impact and likelihood, and mitigate the risk by using controls or other effective actions.
- **Vulnerability Management:** This module collects vulnerabilities from vulnerability assessment tools, removes duplicates, assigns them to assets, and prioritizes them accordingly, allowing you to manage the remediation process.
- **Asset Management:** Assets are the building blocks of the business model, which is the foundation for all core EnterpriseView functionality. The business model depicts the entire organization from high-level business assets to low-level IT assets, on which policy, risk, and vulnerability operations are performed. You can create the business model by synchronizing EnterpriseView with an external asset repository or by creating it by using the Assets module.
- **Dashboards and Reports:** This module includes sophisticated executive dashboards, such as Risk Register, and reports, as well as the ability to create your own customized dashboards and reports.
- **Task Management:** EnterpriseView enables you to create, manage, and monitor workflows. Use workflows to structure and streamline your organization's processes and assign tasks to the relevant people.





## Chapter 3

# Install 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. Before you install EnterpriseView, you must have a complete installation of SAP BusinessObjects version 3.1 SP 5.0 running in your network.

**Note:** EnterpriseView supports only a new installation of SAP BusinessObjects, which is delivered with the EnterpriseView installation package. It does not support the installation of EnterpriseView alongside an existing installation of SAP BusinessObjects.

To install EnterpriseView:

1. Review the system requirements and make sure that you comply with all the requirements. For more information, see ["System Requirements" below](#).
2. Review the prerequisites and make sure that all pre-installation tasks are done. For more information, see ["Prerequisites" on page 22](#)
3. Install SAP BusinessObjects. For more information, see ["Install SAP BusinessObjects Enterprise CMC" on page 23](#).
4. Configure SAP BusinessObjects Enterprise CMC. For more information, see ["Configure BusinessObjects Enterprise" on page 25](#).
5. Run the EnterpriseView setup wizard. For more information, see ["Run EnterpriseView Setup Wizard" on page 29](#).

After you have completed the tasks above, proceed to the ["EnterpriseView Post Installation Tasks" on page 33](#).

## System Requirements

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

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:**

- We recommend installing SAP BusinessObjects and EnterpriseView on separate servers, although you can install them on the same server.
- 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
<b>CPU</b>	4 CPU Cores (minimum)
<b>Free Disk Space</b>	25 GB (minimum)
<b>Memory (RAM)</b>	8 GB (minimum)
<b>Operating System</b>	Windows Server 2008 R2 (x64) Enterprise Edition
<b>Java Version</b>	1.6.0_31

### SAP BusinessObjects Server System Requirements

Element	Requirement
<b>CPU</b>	4 CPU Cores (minimum)
<b>Free Disk Space</b>	20 GB
<b>Memory (RAM)</b>	4 GB
<b>Operating System</b>	Windows Server 2008 R2 (x64) Enterprise Edition

### EnterpriseView Database Requirements

Element	Requirement
<b>Type</b>	Oracle 11.2.0.1 or later
<b>CPU</b>	8 CPU Cores (minimum)
<b>Memory (RAM)</b>	8 GB (minimum)
<b>Tablespace for EnterpriseView</b>	50 GB
<b>Tablespace for User Management Module</b>	0.5 GB
<b>Temporary Tablespace for EnterpriseView</b>	50 GB

### SAP BusinessObjects Database Requirements

Element	Requirement
Type	<p>Oracle 11.2.0.1 or later</p> <p><b>Note:</b> 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.</p>
Tablespace for SAP BusinessObjects	2 GB

### Client Requirements

Element	Requirement
Browser	<ul style="list-style-type: none"> <li>• Microsoft Internet Explorer 8.x, 9.x (32-bit)</li> <li>• Mozilla Firefox 16.0 or later (32-bit)</li> <li>• Google Chrome</li> </ul>
Adobe Flash Player	Flash Player 11.0
Screen Resolution	Recommended 1440x900

## Integration Matrix

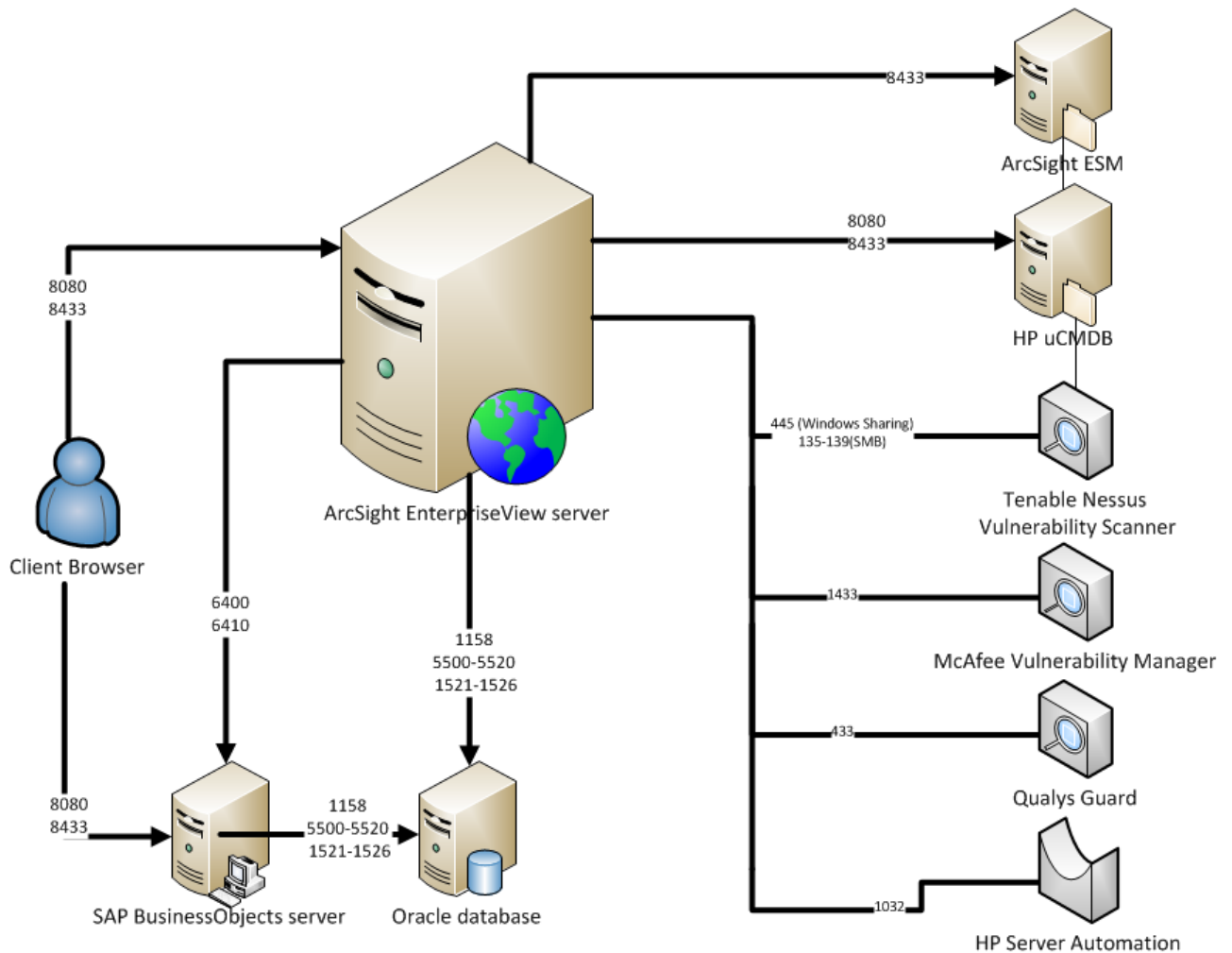
The following table includes the supported versions of products that EnterpriseView integrates with.

Product	Version
HP Universal CMDB	8.x, 9.x
ArcSight Enterprise Security Manager	6.0c
ArcSight Express	4.0
HP Server Automation (SA)	9.10
Tenable Nessus Vulnerability Scanner	3.2.x, 4.x, 5.x
McAfee Vulnerability Manager (Foundscan)	7.0
Qualys Guard	6.05, 7.1

Product	Version
HP WebInspect	9.1 or later
Rapid7 Nexpose	4.0 or later

## 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, perform the following tasks:

- Allocate new Oracle user schemas; for EnterpriseView, for SAP BusinessObjects Enterprise CMC, and for the User Management module.

**Note:** We recommend disabling the Oracle password expiration date for all user schemas.

For each user schema, grant the following roles:

- RESOURCE
- CONNECT

For each user schema, grant the following privileges:

- CREATE ANY VIEW
- DROP ANY VIEW
- Configure the EnterpriseView login to be the owner of the EnterpriseView database, and configure the EnterpriseView database to be the default database for the EnterpriseView login. Do the same for the User Management module login and database.
- The Oracle database must be configured to support AL32UTF-8 character set. For more information, refer to Oracle documentation.
- Oracle Instant Client for Microsoft Windows (32-bit) version 11.2.0.2.0 must be installed on the machine on which SAP BusinessObjects is installed. You can download it from the following folder from your HP EnterpriseView installation medium:

**Installations\BO Installation.zip\Oracle\_client\_32**

- 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. You can download it from the following folder from your HP EnterpriseView installation medium:

**Installations\BO Installation.zip\Oracle\_client\_32**

- 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 EnterpriseView from your support or sales representative and save a copy of the license on the EnterpriseView server.

# 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 EnterpriseView installation medium.
2. In 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. In the **User Information** page, in the **Product Keycode** box, enter the following license key, and then click **Next**.

**CSZ0F-13KG93M-Y40A00Y-1TCF**

This license key provides a license to ten concurrent users.

- b. In the **Install Type** page, select the **Use an existing database server** option, and then click **Next**.
- c. In 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:** Use these credentials to access EnterpriseView for the first time. This is the only user that can begin defining authorized users in the business model. For more information, see the *Authorize a User to Work with an Asset* section in the *HP EnterpriseView User Guide*.

- d. In 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. In the **Configure Tomcat** page, if EnterpriseView and SAP BusinessObjects are installed

on the same server, modify the following parameters:

- **Connection port**
- **Shutdown port**
- **Redirect port**

4. To log on to SAP BusinessObjects:

- a. In the **Username** box enter **Administrator**.
- b. In the **Password** box, enter the password that you configured during the installation of SAP BusinessObjects, and then click **Login**.

After the installation is complete, you need to ["Configure BusinessObjects Enterprise" on the facing page](#).



# Configure BusinessObjects Enterprise

After SAP BusinessObjects is installed, perform the following procedures:

## Configure SAP BusinessObjects license key

1. Open SAP BusinessObjects Enterprise CMC.
2. Under **Manage**, click **License Keys**.
3. In the **Add Key** box, enter the following license key, and then click **Add**:

**CRZ0K-U4KG938-Y40200S-W2K9**

This license key provides license to two named users. (In SAP BusinessObjects, a named user can access the application regardless of the number of users who are currently connected.)

## 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:** We recommend backing up the jdbc.sbo file before editing it.

2. 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
```

```
    <ClassPath>
```

```
    <Path>your jar or class files directory</Path>
```

```
    </ClassPath>
```

```
-->
```

with:

```
<ClassPath>
```

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

```
</ClassPath>
```

**Note:** This is the ojdbc5.jar JDBC driver that you installed prior to installing SAP BusinessObjects, as described in ["Prerequisites" on page 22](#).

3. Search for the following:

```
<Defaults>  
  
    <Parameter Name="Array Fetch Size">0</Parameter>  
  
</Defaults>
```

change the Array Fetch size to 500, as follows:

```
<Parameter Name="Array Fetch Size">500</Parameter>
```

4. 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:** We recommend 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. In the **Properties** window, in the **Web Intelligence Processing Service** group box, enter the

following information, and then click **Save**:

- In the **Maximum Connections** box, enter **1000**.
  - In the **Maximum Document Cache Size (KB)** box, enter **10000000**.
  - In the **Maximum Documents Per User** box, enter **20**.
6. In the right pane, double-click **AdaptiveJobServer**.
  7. In the **Properties** window, in the **Maximum Concurrent Jobs** box, enter **10**, and then click **Save**.

## Configure Active Directory authentication

**Note:** Perform this procedure if you are using Active Directory for authenticating users.

Follow the instructions in the *Using AD Authentication* section in the *SAP BusinessObjects Enterprise Administrator's Guide*.

## Configure LDAP Authentication

**Note:** Perform this procedure in either of the following cases:

- You are using an LDAP server 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**

## Configure group display name in SAP BusinessObjects

Perform this procedure if you are using an LDAP server as an authentication system.

1. Open SAP BusinessObjects Enterprise CMC.
2. Under **Organize**, click **Users and Groups**.
3. Under **Group Hierarchy**, locate the group that you want to edit.
4. Right-click the group, and then click **Properties**.
5. In the **Properties** page, in the **Title** box, enter a new display name.

**Note:** The display name cannot include commas.

6. Click **Save**.

### Restart the SAP BusinessObjects server

1. In the SAP BusinessObjects server, click **Start > BusinessObjects Enterprise > Central Configuration Manager**.
2. In the **Central Configuration Manager** window, stop and restart the following:
  - a. **Apache Tomcat**
  - b. **Server Intelligence Agent**

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**

When you finish installing EnterpriseView, follow the instructions in ["EnterpriseView Post Installation Tasks" on page 33](#).

### To run EnterpriseView setup

1. Click the **setup.exe** file located in the **\Installations\EnterpriseView** folder of your HP 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. In 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:

#### **HP EnterpriseView**

5. Log on to EnterpriseView, as described in ["Log On To EnterpriseView" on page 31](#).

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



# Chapter 4

## Log On To EnterpriseView

You access EnterpriseView by using a supported Web browser, from any computer with a network connection to the EnterpriseView server. Adobe Flash Player version 11.0 must be installed on your client machine.

The level of access granted a user depends on the user's permissions. For details on granting user permissions, see ["Assign Roles to a User or Group" on page 39](#).

For details on Web browser requirements, see ["System Requirements" on page 17](#).

### To log on to EnterpriseView

1. From the server on which EnterpriseView is installed:
  - a. From the desktop, click **Start > All Programs**.
  - b. Click **HP EnterpriseView > EnterpriseView**.
2. From the server or any other computer in the network: Access EnterpriseView via **http://<server IP>:8080**.
3. Use your credentials to log on to EnterpriseView. If you are logging on to EnterpriseView for the first time, use the following credentials:

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

- a. In the **Username** box enter **Administrator**.
- b. In the **Password** box, enter the password that you configured during the installation of SAP BusinessObjects, and then click **Login**.





# Chapter 5

## EnterpriseView Post Installation Tasks

After you have installed EnterpriseView, perform the following tasks:

1. If you are using Active Directory (AD) for user authentication, follow the instructions in ["Connect to Active Directory" on page 35](#).
2. Configure your User Management system, as described in ["User Management" on page 37](#). Users and groups must already be defined either in SAP BusinessObjects or in a security system integrated with SAP BusinessObjects, such as an LDAP server. 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 39](#). You can also create new roles, as described in ["Add Roles" on page 38](#).
3. Define named users in SAP BusinessObjects. For more information, see ["Define a Named User in BusinessObjects Enterprise" on page 49](#).
4. If required, integrate with external systems, as described in ["Synchronize Assets with External Asset Repository" on page 51](#), ["Import Security Threats from an SIEM System" on page 71](#), and ["Import Vulnerabilities From Vulnerability Assessment Tools" on page 73](#).



# Chapter 6

## Connect to Active Directory

If you are using Active Directory (AD) for authenticating users, then you have already configured it in SAP BusinessObjects. To configure AD connection with EnterpriseView, perform the following procedure.

### To connect to AD

1. Stop the EnterpriseView service.
2. On the EnterpriseView server, open the following file for editing:

**<EnterpriseView installation Folder>\conflad\krb5.ini**

3. In the **krb5.ini** file, do the following:
  - Change all the instances of **MYDOMAIN.COM** to the domain where AD resides.
  - Change **MYDHOSTNAME.MYDOMAIN.COM** to the full computer name of the server where AD is installed.

**Note:** To find the domain and the full computer name of AD, open a command line and run the command **set**. To find the domain name, look for **USERDNSNAME**. To find the full computer name, look for **LOGONSERVER**.

See the following sample:

```
[libdefaults]

default_realm = MYDOMAIN.COM

dns_lookup_kdc = true

dns_lookup_realm = true

default_tgs_enctypes = rc4-hmac

default_tkt_enctypes = rc4-hmac

udp_preference_limit = 1

[realms]

MYDOMAIN.COM = {
```

```
kdc = MYDHOSTNAME.MYDOMAIN.COM  
  
default_domain = MYDOMAIN.COM  
  
}
```

4. Start the EnterpriseView service.

# Chapter 7

## 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 an LDAP server, then any change made in the security system is propagated to both SAP BusinessObjects and EnterpriseView.

**Note:** If you are using an LDAP server as a security system, then when you configure authentication with LDAP, make sure to map each group separately. For more information, see *SAP BusinessObjects Administration Guide*.

HP EnterpriseView enables you to define roles, as described in ["Add Roles" on the next page](#), and assign them to users and groups, as described in ["Assign Roles to a User or Group" on page 39](#). 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 Assessment and Treatment 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.



**Note:** When you create a user in SAP BusinessObjects, you cannot use an **Account Name** that you have used previously, even if that user was deleted and no longer exists in the system. This issue can arise when an employee leaves the organization and later returns to work for the organization. To overcome this issue, Do not delete users in SAP BusinessObjects; instead, disable the user by selecting the **Account is disabled** check box, as described in the *To modify a user account* section, in the *Managing Users and Groups* chapter, in the *SAP BusinessObjects Enterprise Administrator's Guide*.

## Add Roles

In addition to the out-of-the-box roles defined in EnterpriseView, you can create new roles.

If you want to create a role with edit permissions to a page in EnterpriseView, then you must also add the corresponding view permission to that page.



### To add a role

1. In EnterpriseView, click **Administration > User Management**, and then click the **Role Management** tab.
2. In the **Roles** pane on the left, click the **Create Role**  button.
3. In 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**.

## 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. 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 for users, as described in ["Search Users" below](#).
3. On the right pane, under **Roles and Permissions**, click the **Assign Role**  button.
4. In 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. Click **Administration > User Management**.
2. In the left pane, click the **User Management** tab.
3. In 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 dashboard components based on the BusinessObjects Reports component. These permissions are managed directly via SAP BusinessObjects. By default, all users have access to the dashboards and reports.

The System Administrator role has permissions for 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 37](#).

Role	Permissions	Accessible components
All roles	<ul style="list-style-type: none"><li>• Login</li><li>• View Executive View Settings</li><li>• View Task Management</li><li>• View Executive View Dashboards</li></ul>	<ul style="list-style-type: none"><li>• Task Management Dashboard</li><li>• Workflow Management</li><li>• My Tasks</li><li>• External Risk Factors Dashboard</li><li>• Risk Register</li><li>• Overall Score Heat Map</li><li>• Risk Indicators</li><li>• Audit Log</li><li>• Settings &gt; Executive View</li><li>• Vulnerability Dictionary</li></ul>
Asset Profiler	<ul style="list-style-type: none"><li>• View Assets</li><li>• Edit Assets</li></ul>	<ul style="list-style-type: none"><li>• Asset Profiling</li></ul>



Role	Permissions	Accessible components
Policy Auditor	<ul style="list-style-type: none"> <li>• View Policies</li> <li>• View Policy Statement of Applicability</li> <li>• View Assets</li> <li>• View Policy Assessments</li> <li>• Edit Policy Assessments</li> <li>• View Policy and Compliance Settings</li> <li>• Edit Policy And Compliance Settings</li> <li>• View Policy Dashboards</li> <li>• View Mappings</li> </ul>	<ul style="list-style-type: none"> <li>• Policy Assessment</li> <li>• Policy Builder</li> <li>• Statement of Applicability</li> <li>• Policy Mapping</li> <li>• Asset Profiling</li> <li>• Control to Threat Mapping</li> <li>• Vulnerability to Control Mapping</li> <li>• Settings &gt; Policy and Compliance</li> <li>• Compliance Dashboard</li> <li>• Compliance by Policy Dashboard</li> <li>• Policy Compliance Map</li> </ul>

Role	Permissions	Accessible components
Policy Compliance Manager	<ul style="list-style-type: none"> <li>• View Policies</li> <li>• View Policy Statement of Applicability</li> <li>• Edit Policy Statement of Applicability</li> <li>• View Assets</li> <li>• View Policy Assessments</li> <li>• View Policy and Compliance Settings</li> <li>• Edit Policy And Compliance Settings</li> <li>• Edit Task Management</li> <li>• View Policy Dashboards</li> <li>• View Mappings</li> </ul>	<ul style="list-style-type: none"> <li>• Statement of Applicability</li> <li>• Policy Builder</li> <li>• Policy Assessment</li> <li>• Policy Mapping</li> <li>• Asset Profiling</li> <li>• Control to Threat Mapping</li> <li>• Vulnerability to Control Mapping</li> <li>• Settings &gt; Policy and Compliance</li> <li>• Compliance Dashboard</li> <li>• Compliance by Policy Dashboard</li> <li>• Policy Compliance Map</li> </ul>

Role	Permissions	Accessible components
Policy Builder	<ul style="list-style-type: none"> <li>• View Policies</li> <li>• Edit Policies</li> <li>• View Policy and Compliance Settings</li> <li>• Edit Policy and Compliance Settings</li> <li>• Edit Task Management</li> <li>• View Policy Dashboards</li> <li>• View Policy Assessments</li> <li>• View Policy Statement of Applicability</li> <li>• View Assets</li> <li>• View Mappings</li> <li>• Edit Mappings</li> </ul>	<ul style="list-style-type: none"> <li>• Policy Builder</li> <li>• Policy Assessment</li> <li>• Statement of Applicability</li> <li>• Asset Profiling</li> <li>• Policy Mapping</li> <li>• Control to Threat Mapping</li> <li>• Vulnerability to Control Mapping</li> <li>• Settings &gt; Policy and Compliance</li> <li>• Compliance Dashboard</li> <li>• Compliance by Policy Dashboard</li> <li>• Policy Compliance Map</li> </ul>

Role	Permissions	Accessible components
Policy Viewer	<ul style="list-style-type: none"> <li>• View Policies</li> <li>• View Assets</li> <li>• View Policy Statement of Applicability</li> <li>• View Policy Assessments</li> <li>• View Policy and Compliance Settings</li> <li>• View Policy Dashboards</li> <li>• View Mappings</li> </ul>	<ul style="list-style-type: none"> <li>• Policy Assessment</li> <li>• Statement of Applicability</li> <li>• Policy Mapping</li> <li>• Asset Profiling</li> <li>• Control to Threat Mapping</li> <li>• Vulnerability to Control Mapping</li> <li>• Settings &gt; Policy and Compliance</li> <li>• Compliance Dashboard</li> <li>• Compliance by Policy Dashboard</li> <li>• Policy Compliance Map</li> </ul>
Risk Auditor	<ul style="list-style-type: none"> <li>• View Risk Assessment and Treatment</li> <li>• Edit Risk Assessment and Treatment</li> <li>• View Threat Assignment</li> <li>• Edit Threat Assignment</li> <li>• View Assets</li> <li>• View Threat Library</li> <li>• View Risk Modeling Settings</li> <li>• Edit Risk Modeling Settings</li> <li>• Edit Task Management</li> <li>• View Risk Modeling Dashboards</li> <li>• View Mappings</li> </ul>	<ul style="list-style-type: none"> <li>• Risk Assessment and Treatment</li> <li>• Threat Assignment</li> <li>• Threat Library Builder</li> <li>• Asset Profiling</li> <li>• Control to Threat Mapping</li> <li>• Vulnerability to Control Mapping</li> <li>• Settings &gt;Risk Modeling</li> <li>• Risk Modeling Dashboard</li> <li>• Risk Scorecard and Heat Map</li> </ul>

Role	Permissions	Accessible components
Risk Viewer	<ul style="list-style-type: none"> <li>• View Risk Assessment and Treatment</li> <li>• View Threat Assignment</li> <li>• View Assets</li> <li>• View Threat Library</li> <li>• View Risk Modeling Settings</li> <li>• View Risk Modeling Dashboards</li> <li>• View Mappings</li> </ul>	<ul style="list-style-type: none"> <li>• Risk Assessment and Treatment</li> <li>• Threat Library Builder</li> <li>• Asset Profiling</li> <li>• Control to Threat Mapping</li> <li>• Vulnerability to Control Mapping</li> <li>• Settings &gt;Risk Modeling</li> <li>• Risk Modeling Dashboard</li> <li>• Risk Scorecard and Heat Map</li> </ul>

Role	Permissions	Accessible components
Security Officer	<ul style="list-style-type: none"> <li>• View ESM Threats</li> <li>• View Risk Assessment and Treatment</li> <li>• View Threat Assignment</li> <li>• Edit External Risk Factor Settings</li> <li>• View External Risk Factor Settings</li> <li>• Edit Task Management Settings</li> <li>• View Task Management Settings</li> <li>• View Assets</li> <li>• View Threat Library</li> <li>• View Policies</li> <li>• View Policy Statement of Applicability</li> <li>• View Policy Assessments</li> <li>• View Vulnerabilities</li> <li>• Edit Executive View Settings</li> <li>• View Risk Modeling Settings</li> <li>• View Vulnerabilities Settings</li> <li>• View Policy And Compliance Settings</li> <li>• View ESM Threat Settings</li> <li>• Edit Task Management</li> <li>• View Risk Modeling Dashboards</li> </ul>	<ul style="list-style-type: none"> <li>• Policy Compliance Map</li> <li>• Risk Assessment and Treatment</li> <li>• Control to Threat Mapping</li> <li>• Vulnerability to Control Mapping</li> <li>• Settings (all pages)</li> <li>• Risk Modeling Dashboard</li> <li>• Risk Scorecard and Heat Map</li> <li>• Compliance Dashboard</li> <li>• Compliance by Policy Dashboard</li> <li>• Vulnerability Dashboard</li> <li>• ESM Threat View</li> <li>• Threat Library Builder</li> <li>• Threat Assignment</li> <li>• Vulnerability Assignment</li> <li>• Vulnerability Management</li> <li>• Policy Builder</li> <li>• Statement of Applicability</li> <li>• Policy Assessment</li> <li>• Asset Profiling</li> </ul>

Role	Permissions	Accessible components
	<ul style="list-style-type: none"> <li>• View Policy Dashboards</li> <li>• View Vulnerability Dashboards</li> <li>• View Mappings</li> <li>• Edit Mappings</li> </ul>	
Threat Library Administrator	<ul style="list-style-type: none"> <li>• View Risk Assessment and Treatment</li> <li>• Edit Risk Assessment and Treatment</li> <li>• View Threat Assignment</li> <li>• Edit Threat Assignment</li> <li>• View Assets</li> <li>• View Threat Library</li> <li>• Edit Threat Library</li> <li>• Edit Risk Assessment</li> <li>• View Risk Modeling Settings</li> <li>• Edit Risk Modeling Settings</li> <li>• Edit Task Management</li> <li>• View Risk Modeling Dashboards</li> <li>• View Mappings</li> <li>• Edit Mappings</li> </ul>	<ul style="list-style-type: none"> <li>• Threat Library Builder</li> <li>• Threat Assignment</li> <li>• Asset Profiling</li> <li>• Risk Assessment and Treatment</li> <li>• Control to Threat Mapping</li> <li>• Vulnerability to Control Mapping</li> <li>• Settings &gt; Risk Modeling</li> <li>• Risk Modeling Dashboard</li> <li>• Risk Heat Map and Scorecard</li> </ul>
Security Threat Viewer	<ul style="list-style-type: none"> <li>• View ESM Threats</li> <li>• View Assets</li> <li>• View ESM Threat Settings</li> </ul>	<ul style="list-style-type: none"> <li>• ESM Threat View</li> <li>• Settings &gt; ESM Threat View</li> <li>• Asset Profiling</li> </ul>

Role	Permissions	Accessible components
Vulnerability Manager	<ul style="list-style-type: none"> <li>• View asset</li> <li>• View vulnerabilities</li> <li>• Edit vulnerabilities</li> <li>• View Vulnerability Settings</li> <li>• Edit Vulnerability Settings</li> <li>• Edit Task Management</li> <li>• View Vulnerability Dashboards</li> <li>• View Mappings</li> </ul>	<ul style="list-style-type: none"> <li>• Vulnerability Management</li> <li>• Vulnerability Assignment</li> <li>• Asset Profiling</li> <li>• Settings &gt; Vulnerabilities</li> <li>• Vulnerability Dashboard</li> <li>• Vulnerability to Control Mapping</li> <li>• Control to Threat Mapping</li> </ul>
Vulnerability Viewer	<ul style="list-style-type: none"> <li>• View asset</li> <li>• View vulnerabilities</li> <li>• View Vulnerability Settings</li> <li>• View Vulnerability Dashboards</li> </ul>	<ul style="list-style-type: none"> <li>• Vulnerability Management</li> <li>• Vulnerability Assignment</li> <li>• Asset Profiling</li> <li>• Vulnerability Dashboard</li> </ul>
Task Management Template Manager	<ul style="list-style-type: none"> <li>• Edit Task Management</li> <li>• Edit Template Management</li> <li>• View Task Management Settings</li> <li>• Edit Task Management Settings</li> </ul>	Manage Templates (dialog box)
Workflow Administrator	<ul style="list-style-type: none"> <li>• Edit Task Management</li> <li>• Edit Template Management</li> <li>• View All Workflows</li> <li>• View Task Management Settings</li> <li>• Edit Task Management Settings</li> </ul>	Manage Templates (dialog box)



## Define a Named User in BusinessObjects Enterprise

Perform this task after you define users, as described in the *SAP BusinessObjects Enterprise Administrator's Guide*.

### To define a named user in SAP BusinessObjects

1. Open SAP BusinessObjects Enterprise CMC.
2. Under **Organize**, click **Users and Groups**.
3. In the left pane, click **User List**.
4. In the right pane, click the user that you want to define as a named user.
5. In the **Properties** page, under **Connection Type**, select **Named User**.

**Note:** The administrator user must be set as a named user.



## Chapter 8

# Synchronize Assets with External Asset Repository

You can synchronize the EnterpriseView business model with a single 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 56](#).

**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" below](#).
- ArcSight Enterprise Security Manager. For more information see ["Integrate with ArcSight Enterprise Security Manager" on page 58](#).

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 63](#).

You can synchronize assets with only one external asset repository.

## Integrate with HP Universal CMDB

Integrating with UCMDB requires preparation in both EnterpriseView and 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 the next page](#).

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 56](#). To learn more about the Synchronization job, see ["About UCMDB Asset Synchronization Job" below](#).

## 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 the facing page](#).
2. The fields in UCMDB elements are compared against fields in assets/relationships and are loaded to a temporary table.
3. UCMDB elements are converted into EnterpriseView assets and relationships.
4. The process checks the EnterpriseView database for each of the assets/relationships.

**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 relationships (meaning that they no longer exist in the UCMDB database) are deleted from the EnterpriseView database.
  6. The new assets are located in the **Unattached** tab in the **Asset Profiling** page. For information on connecting these assets to the business model, see the *Connect an Asset to the Business Model* section in the *HP EnterpriseView User Guide*.

You can check the status of the job in the Job Management module. For more information, see the *Troubleshoot Batch Jobs* section in the *HP EnterpriseView Administration Guide*.

## 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" above](#), in addition to 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 Relationship Direction" on page 57](#).
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" below](#).
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 the next page](#) 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 55](#) 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 56](#).
6. **Schedule and activate the Synchronization job** to complete the process, as described in ["Schedule and Activate the UCMDB Asset Synchronization Job" on page 56](#).

## 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. 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 **Connector**, and then enter the parameters for connecting with UCMDB, as described in the following table:

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

4. Save and apply the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).


## 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. Therefore, the asset **Type** field is populated automatically during the import process.

## To map asset categories

1. 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 the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).

## 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. 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 the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).

## 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 (CMS), 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. 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 the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).

## 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 52](#).

### To schedule and activate a synchronization job

1. 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 the following:  
  
**0 0 0/1 \* \* ?**  
  
For more information, see ["Appendix B: Learn About Cron Expressions" on page 103](#).
  - Select the **Activate Job** check box.
4. Save and apply the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).

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

## Reverse Relationship 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 relationship direction, for any UCMDB relationship type defined in EnterpriseView.

### To reverse relationship direction

1. 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 **Relationship**, and then select the **Reverse** check box for the type of relationship that you want to reverse.
4. Save and apply the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).

## 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 100](#). The name of the file is **Assets\_and\_Threats.arb** and it is located in <EnterpriseView 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.

**Note:** Make sure that the ESM entities that are included in the file do not have a "," character (comma) in their name. The file generated by the report includes a "," delimiter, so if this character is used in an ESM entity name, then the name will be split into two.

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 the facing page](#) and in ["How to Integrate with ESM to Import Threats" on page 71](#).

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" below](#). To learn more about the security threats import job, see ["About ESM Security Threats Job" on page 71](#).

### About ArcSight ESM Asset Synchronization Job

The Asset Synchronization Job periodically imports ArcSight ESM entities 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 relationships. For more information on mapping logic, see ["Map Asset Types with ESM" on page 61](#).

4. The process checks the EnterpriseView database for each of the assets/relationships.
  - 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 relationships are deleted from the EnterpriseView database (meaning that they no longer exist in the database).

You can check the status of the job in the Job Management module. For more information, see the *Troubleshoot Batch Jobs* section in the *HP EnterpriseView Administration Guide*.

## 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 71](#).

1. **Change the session timeout in ArcSight ESM.** The default session timeout in ArcSight ESM is 10 minutes; this amount of time is not always enough to generate the asset report. If your business model has more than 50,000 assets, then you need to change the session timeout in ArcSight ESM.

**Note:** Changing the session timeout requires restarting ArcSight ESM.

For more information, see ["Change ESM Session Timeout" on the next page](#).

2. **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 the next page](#).
3. **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 61](#) to tailor the mapping to your needs.
4. **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 56](#).
5. **Schedule and activate the Synchronization job** in order to complete the process, as described in ["Schedule and Activate ArcSight ESM Job" on page 63](#).

## Change ESM Session Timeout

**Note:** Changing the session timeout requires restarting ArcSight ESM.

### To change the session timeout

1. On the server on which ArcSight ESM is installed, open a command window or shell window on **<ARCSIGHT\_HOME>/manager/config**.

2. Type the following file name, and then press **ENTER**:

**/server.properties**

3. Change the session timeout by typing the following line, and then press **ENTER**:

**servletcontainer.jetty311.session.timeout.default=20**

4. Restart the ESM Manager by typing the following command, and then press **ENTER**:

**/sbin/service arcsight\_services restart manager**

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

**ArcSight ESM Integration Parameters**

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

#### ArcSight ESM Integration Parameters, continued

Parameter	Description
<b>Username</b>	Credentials for accessing ArcSight ESM, provided by the ArcSight ESM administrator.
<b>Password</b>	Credentials for accessing ArcSight ESM, provided by the ArcSight ESM administrator.

4. Save and apply the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).

## Map Asset Types with ESM

**Note:** Before you begin, you should have a clear vision of what you want your business model to look like. If at any time you want to change the business model, then you can change the mapping configuration; the business model will be updated after the next Asset Synchronization Job runs.

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. Only assets that have a zone are imported.

To help you create a hierarchical business model that reflects the ArcSight ESM network model but also provides business context, in addition to assets, the Asset Synchronization Job imports the following ArcSight ESM entities:

- Asset Group
- Asset Category
- Zone Group
- Zone

All of these entities have a corresponding asset type in EnterpriseView, and they all belong to the Business Asset category, as presented in the following table.

ESM Entities	EnterpriseView Asset Category	EnterpriseView Asset Type
Asset Group	Business Asset	Asset Group
Asset Category	Business Asset	Category
Zone Group	Business Asset	Zone Group
Zone	Business Asset	Zone

The asset zone and zone group are reflected in the business model by design, because the zone is mandatory. You can decide whether to reflect the asset group and asset category in the business model. If you choose to reflect the asset group and the asset category, then two additional hierarchies will be created. So, potentially, you can have numerous hierarchies under the Organization asset.

By default, each of the ArcSight ESM entities is mapped to its corresponding asset type in EnterpriseView, but you can map them to any asset type defined in EnterpriseView. You can also create exceptions. For example, if you mapped a zone in ArcSight ESM to a zone in EnterpriseView, but you want to map one specific zone to a subnet, then you can create an exception.

The following procedure describes how to select which hierarchies will be created, map asset types, and create exceptions.

### To map asset types with ArcSight ESM

1. Click **Administration > Configuration**.
2. In the left pane, click **Integrations > ArcSight ESM > Asset Synchronization > Asset Type Mapping**.
3. In the **Asset Type Mapping** page, depending on the number of hierarchies that you want to create, select the following:
  - **Create a Group-based Model**
  - **Create a Category-based Model**
4. If required, change the default mapping in the mapping table.
5. To create an exception, do the following:
  - a. Click a new row in the mappings table to create a new record.
  - b. From the **ESM Entities** list, select the ESM entity for which you want to create an exception.
  - c. In the **ESM Entity Exception** cell, enter the name of the ESM entity for which you want to create a separate mapping.
  - d. From the **EnterpriseView Asset Category** list, select the category of the EnterpriseView asset type that you want to map.
  - e. In the **EnterpriseView Asset Type** enter the asset type to which you want to map the exception.
6. Save and apply the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).

## 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, the Event Import job, or both.

For more information on the jobs, see ["About ArcSight ESM Asset Synchronization Job" on page 58](#) and ["About ESM Security Threats Job" on page 71](#).

### To schedule and activate a synchronization job

1. 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. In the **Job** page, do the following:
  - **Job Schedule:** enter a Cron expression.  
  
For example, to run the job once every hour, every day, enter the following:  
  
**0 0 0/1 \* \* ?**  
  
For more information, see ["Appendix B: Learn About Cron Expressions" on page 103](#).
  - Select the **Activate Job** check box.
4. Save and apply the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).

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 66](#).

The business model information from your asset repository needs to be extracted into two files: one that includes asset information and one that includes relationship information. The asset file is mandatory and the relationships file is optional. If the asset file is missing, then the job fails; if the relationships file is missing, the assets are imported without relationships. For more information on the synchronization job, see ["About CSV Asset Synchronization Job" on page 65](#).

### 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
- Type (mandatory)
- External ID (mandatory)
- Address Line1
- Address Line2
- City
- State
- Country
- Zip Code
- coordinate Latitude
- coordinate Longitude
- Criticality Level
- Business Value
- Operating System Name
- Operating System Version



- Application Name
- Application Version
- DNS Name
- IP Address
- MAC Address
- Role
- Document Version
- Release Date
- Document Purpose
- Document Classification
- CPE List

**Relationship file header**

- SourceExternalId
- DestinationExternalId

## About CSV Asset Synchronization Job

The CSV Asset Synchronization Job periodically imports assets and relationships 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. Relationships are read from the relationship 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.
External ID field is empty.	Job fails.
External ID column is missing.	Job fails.

Error	Action
The relationships file includes a circular connection between assets.	Job fails.
One of the following mandatory fields is missing: 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 relationships.
4. The process checks the EnterpriseView database for each asset and relationship.

**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 relationships (meaning that they no longer exist in the CSV file) are deleted from the EnterpriseView database.
  6. The new assets are located in the **Unattached** tab in the **Asset Profiling** page. For information on connecting these assets to the business model, see the *Connect an Asset to the Business Model* section in the *HP EnterpriseView User Guide*.

You can check the status of the job in the Job Management module. For more information, see the *Troubleshoot Batch Jobs* section in the *HP EnterpriseView Administration Guide*.

## 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 the previous page](#).

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 the facing page](#).

2. **Map Asset Categories.** Follow the instructions in ["Map Asset Categories with CSV" on the next page](#).
3. **Define Imported Asset Type properties.** Decide which asset properties will be imported from the CSV file, as described in ["Define Imported Asset Type Properties" on page 56](#).
4. **Schedule and activate the Synchronization job.** In order to complete the process, as described in ["Schedule and Activate CSV Job" on the next page](#).

## Configure CSV File Settings

### To configure CSV file settings

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


Parameter	Description
<b>Connector Name</b>	A logical name for the asset repository from which you are importing. This is the name that is displayed in the <b>Source</b> property of the asset.
<b>Asset File path</b>	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.
<b>Relationship File Path</b>	The location of the relationship file that is imported into EnterpriseView. The file can be placed anywhere in the network, as long as EnterpriseView can access the path.
<b>Max Business Criticality Level in Source</b>	<p>The upper limit of the business criticality in the asset repository from which you are importing your business model.</p> <p>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.</p>

4. Save and apply the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).

## Map Asset Categories with CSV

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

### To map asset categories

1. Click **Administration > Configuration**.
2. In the left pane, click **Integrations > CSV File > Asset Category Mapping**.
3. In 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 the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).

## 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 65](#).

### To schedule and activate a synchronization job

1. 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 the following:

**0 0 0/1 \* \* ?**

For more information, see ["Appendix B: Learn About Cron Expressions" on page 103](#).

- Select the **Activate Job** check box.

4. Save and apply the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).

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



## Chapter 9

# Import Security Threats from an SIEM System

EnterpriseView enables 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 (both physical assets and business assets). This information is displayed graphically, either per asset or for multiple assets and enables 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 log on, log off, 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, that uses 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 58](#). For information on the event import job, see ["About ESM Security Threats Job" below](#).

## 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 the next page](#). The information is displayed graphically via the ESM Threat View component.

You can check the status of the job in the Job Management module. For more information, see the *Troubleshoot Batch Jobs* section in the *HP EnterpriseView Administration Guide*.

## 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 59](#).

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

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 60](#).

**Note:** Skip this step if you have already configured integration for asset synchronization with ESM.

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" below](#).
3. **Schedule and activate the Synchronization job** in order to complete the process, as described in ["Schedule and Activate ArcSight ESM Job" on page 63](#).

## 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 100](#).

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. Click **Administration > Configuration**.
2. In the left pane, click **Integrations > ArcSight ESM > Asset Threat Synchronization > ESM Priority Factors**.
3. In 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 98](#).
4. Save and apply the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).



## Chapter 10

# Import Vulnerabilities From Vulnerability Assessment Tools

EnterpriseView enables 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 by using ArcSight SmartConnectors. For an overview on the Vulnerabilities module, see the *Vulnerability Management* chapter in the *HP 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)	McAfee Vulnerability Manager DB
Qualys Guard	Qualys Vulnerability Scanner File
HP WebInspect	ArcSight FlexConnector XML file
Rapid7 Nexpose	Rapid7 NeXpose XML 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 SmartConnector is 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.

**Note:** HP WebInspect does not generate reports automatically. In order to load vulnerability information into EnterpriseView, you must manually export the scans in Full XML format, as described in the *Export scan details in WebInspect* task, in the *Web Application Firewall Integration Tool* section, in the *HP WebInspect User Guide*.

After you export the scan, copy it to the reports folder that you defined when you installed the connector.

To import vulnerabilities, first ["Install and Configure ArcSight SmartConnector"](#) on the facing page and then ["Schedule and Activate Vulnerabilities Import Job"](#) on page 78.

## 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 the *Vulnerability Properties* section in the *HP EnterpriseView User Guide*.
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 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 78.
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 EnterpriseView User Guide*.

You can check the status of the job in the Job Management module. For more information, see the *Troubleshoot Batch Jobs* section in the *HP EnterpriseView Administration 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
- McAfee Vulnerability Manager DB
- Qualys Vulnerability Scanner File
- ArcSight FlexConnector XML file (for HP WebInspect)
- Rapid7 NeXpose XML 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

**Note:** ArcSight FlexConnector XML file installation is only supported on a Windows operating system.

1. On the server that you want to install, open the following folder:

**HP EnterpriseView installation medium\Connectors**

2. Start the ArcSight SmartConnector Installer by running one of the following:

**ArcSight-<version>-Connector-Win.exe**

**ArcSight-<version>-Connector-Linux.bin**

3. 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. If you are installing a SmartConnector for WebInspect, do the following:
    - i. When you are prompted to select the SmartConnector, select **ArcSight FlexConnector XML file**.
    - ii. When you are prompted to enter the SmartConnector parameters, in the **Configuration File** box, enter **WI**.
  - c. When prompted to select a **Mode**, select **Automatic**.
  - d. 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. Based on the type of SmartConnector that you installed, do the following:
  - 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 medium>\Connectors\ArcSight SmartConnectors\Add-ons:**

To:

**<ArcSight SmartConnector root folder>\<Nessus folder>\user\agent\fcpl\nessus\_file**

- If you installed a **Tenable Nessus .nessus File** SmartConnector and if your Nessus scanner is lower than version 4.2, do the following:

Copy file **nessus\_dotnessus\_v1.vulns.xqueryparser.properties**

From:

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

To:

**<ArcSight SmartConnector root folder>\<Nessus folder>\user\agent\fcpl\nessus\_file**

- If you installed a Rapid7 NeXpose XML File SmartConnector, do the following:

Copy file **nexpose\_xml\_vulns.xqueryparser.properties**

From:

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

To:

**<ArcSight SmartConnector root folder>\<Nexpose folder>\user\agent\fcpl\nexpose\_xml**

2. ■ If you installed an **ArcSight FlexConnector XML file** SmartConnector, do the following:
  - i. Open the following file:

**<ArcSight SmartConnector root folder>\<WebInspect folder>\bin\scripts\connectors.bat**

- ii. Locate the **ARCSIGHT\_MEM\_OPTIONS** parameter.
- iii. Modify the number marked in bold below to three times the size of the average XML file size exported by your WebInspect scanner. For example, if an average scan is 100MB, modify this number to 300.

**ARCSIGHT\_MEM\_OPTIONS= -XX:MaxNewSize=128m -Xms256m -Xmxnnnnm**

- iv. Save the changes in the file.

3. From your HP EnterpriseView installation medium, copy the following:

**\Connectors\ArcSight SmartConnectors\Tools\ArcSight SmartConnector Configuration tool.zip**

To this directory:

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

For example: ArcSightSmartConnectors\current

4. Extract the zip file to a separate folder.

5. 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

6. 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.

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 74](#).

### To schedule and activate the Vulnerabilities Import Job

1. Click **Administration > Configuration**.
2. In the left pane, click **Vulnerability Management > Schedule Import Job**.
3. In 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 the following:

**0 0 2 \* \* ?**

For more information, see ["Appendix B: Learn About Cron Expressions" on page 103](#).

- 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 should be changed to Automatically Closed.
4. Save and apply the configuration changes. For more information, see ["Save and Apply Configuration Changes" on page 87](#).





# Chapter 11

## 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 EnterpriseView User Guide*. Policy assessments can be imported regularly from external systems, both commercial and in-house, by using EnterpriseView REST API, as described in the *HP EnterpriseView REST API Developer Guide*.

EnterpriseView integrates with HP Server Automation (SA), by 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" below](#). 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 UCF control "PCI 2.0, Establish and maintain an identification, authentication, and access rights management plan." Is mapped to numerous security check, including the following:

- "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 the SA connector, as described in ["Install Server Automation Connector" below](#).
2. Define the SA connection parameters, as described in ["Define Server Automation Connection Parameters " below](#).
3. Run the SA connector for the first time, as described in ["Run SA Connector for the First Time \(Manual\)" on the facing page](#).
4. Schedule and activate the SA connector:
  - In Windows, use the Task Scheduler
  - In Linux, use a Cron job

**Note:** We recommend synchronizing the schedule of the SA connector with the automatic checks in SA.

5. Monitor and troubleshoot (if necessary) the SA connector, as described in ["Monitor and Troubleshoot the Server Automation Connector" on page 84](#).

## 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 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 by 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)

We recommend scheduling 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.

# Chapter 12

## Manage Configuration Sets

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

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

A new configuration set is initially saved as a draft. A draft is a configuration set that has not yet been activated. A draft can be edited only until it is first activated. The new configuration properties are only applied to EnterpriseView after a draft is activated. For details on how to activate a draft, see ["Save and Apply Configuration Changes" on page 87](#).

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 on to EnterpriseView again.

### To select a configuration set

1. Click **Administration > Configuration**.
2. In the **Configuration** window, in the left pane, click the **Open Configuration Set**  button.  
  
The currently active configuration set is displayed in bold.
3. In the **Open Configuration Set** window, from the list of configuration sets, click the one that you want to run, and then click **Open**.

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

- **Activated**
- **Drafts**



4. In the left pane, click the **Activate current configuration set**  button.  
In the **Activate Configuration Set** dialog box, click **Yes**.
5. Close the EnterpriseView application, and then access the application again.

## Migrate Configuration Data

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

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

### To migrate configuration data

1. In the source application, click **Administration > Configuration**.
2. On the **Configuration** toolbar, click the **Export configuration set to a zip file**  button.
3. In the **Export Configuration Set** dialog box, clear the following check boxes, and then click **Export**:
  - **Connector** in the following paths:
    - Integrations > ArcSight ESM**
    - Integrations > UCMDB > Asset Synchronization > HP Universal CMDB 8.x**
    - Integrations > UCMDB > Asset Synchronization > HP Universal CMDB 9.x**If there are more UCMDB integrations, clear their **Connector** check box, as well.
  - **SAP BusinessObjects**
4. Save the zip file to a location that can be accessed from the target application.
5. In the target application, click **Administration > Configuration**.
6. On the **Configuration** toolbar, click the **Import configuration set**  button.
7. In the **Import Configuration Set** dialog box, do the following and then click **Import**:
  - a. Click **Browse** and select the zip file that you want to import.
  - b. In the **Draft name** box, enter a name for the configuration set.


8. Click the **Activate current configuration set**  button to activate the draft and apply the new configuration settings to EnterpriseView.

## Save and Apply Configuration Changes

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



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

### To create a new configuration set

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

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





# Chapter 13

## Security

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

- Encrypting the various passwords in EnterpriseView as described in ["Encrypt Password" below](#)
- Enabling SSL (Secure Socket Layer) on the server, as described in ["Enable SSL on the Server" on page 92](#). You can also review a step by step example of how to enable SSL on the server by using a self-signed certificate, as described in ["Enable SSL on the Server with a Self-Signed Certificate" on page 93](#).

EnterpriseView uses Apache Tomcat 7.0 as an application server. So in addition to the procedures described in this section, EnterpriseView also supports the same security capabilities as Apache Tomcat 7.0. For more information on these security capabilities, see Apache Tomcat 7.0 documentation.

Verify that EnterpriseView is fully functioning before starting the hardening procedures.

## Encrypt Password

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

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

### To encrypt a password

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

**<EnterpriseView Installation Folder>\bin**

2. Run the following utility:

**encrypt-password.bat -p <new password>**

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

## Change Encryption Algorithm

You can change the encryption properties in order to change the encryption algorithm. For more information on encryption properties, see ["Encryption Properties" below](#).

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

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

### To change the encryption properties

1. Open the following file:

**<EnterpriseView Installation Folder>\conflencryption.properties**

2. Make the required changes. For more information on the encryption properties, see ["Encryption Properties" below](#).
3. Run **generate-keys.bat**.

The following file is created:

**<EnterpriseView Installation Folder>\security\encrypt\_repository**

4. Regenerate all the encrypted passwords, as described in ["Encrypt Password" on the previous page](#).
5. In EnterpriseView, click **Administration > Configuration**.
6. Modify all password configured via the EnterpriseView Configuration module. For example, the password for the ArcSight ESM connector (**Administration > Configuration > Integrations > ArcSight ESM > Connector**).
7. Save the changes, as described in ["Save and Apply Configuration Changes" on page 87](#)

## Encryption Properties

The following table lists the parameters included in the **encryption.properties** file used for password encryption. For details on encrypting a password, see ["Encrypt Password" on the previous page](#).

Parameter	Description
cryptoSource	<p>The infrastructure implementing the encryption algorithm. The available options are:</p> <ul style="list-style-type: none"> <li>• <b>lw</b>: Uses Bouncy Castle lightweight implementation (Default option)</li> <li>• <b>jce</b>: Java Cryptography Enhancement (standard Java cryptography infrastructure)</li> </ul>
storageType	The type of the key storage. Currently, only binary file is supported.
binaryFileStorageName	The place in the file where the master key is stored.
cipherType	The type of the cipher. Currently, only symmetricBlockCipher is supported.
engineName	<p>The name of the encryption algorithm. The following options are available:</p> <ul style="list-style-type: none"> <li>• <b>AES</b>: American Encryption Standard. This encryption is FIPS 140-2 compliant. (Default option)</li> <li>• <b>Blowfish</b></li> <li>• <b>DES</b></li> <li>• <b>3DES</b>: (FIPS 140-2 compliant)</li> <li>• <b>Null</b>: No encryption</li> </ul>
keySize	<p>The size of the master key. The size is determined by the algorithm:</p> <ul style="list-style-type: none"> <li>• <b>AES</b>: 128, 192, or 256 (Default option is 256)</li> <li>• <b>Blowfish</b>: 0-400</li> <li>• <b>DES</b>: 56</li> <li>• <b>3DES</b>: 156</li> </ul>
encodingMode	<p>The ASCII encoding of the binary encryption results. The following options are available:</p> <ul style="list-style-type: none"> <li>• <b>Base64</b> (Default option)</li> <li>• <b>Base64Url</b></li> <li>• <b>Hex</b></li> </ul>

Parameter	Description
algorithmModeName	The mode of the algorithm. Currently, only <b>CBC</b> is supported.
algorithmPaddingName	The padding algorithm used. The following options are available: <ul style="list-style-type: none"><li>• <b>PKCS7Padding</b> (Default option)</li><li>• <b>PKCS5Padding</b></li></ul>
jceProviderName	The name of the JCE encryption algorithm.  <b>Note:</b> Only relevant when cryptSource is <b>jce</b> .  For <b>lw</b> , engineName is used.

## Enable SSL on the Server

You can configure EnterpriseView to support authentication and encryption that uses an SSL channel. SSL can be configured by using either a self-signed certificate or a certificate issued by a Certification Authority (CA). For a detailed example of how to enable SSL on the server by using a self-signed certificate, see ["Enable SSL on the Server with a Self-Signed Certificate" on the facing page](#).

**Note:** All directory and file locations depend on your specific platform, operating system, and installation preferences.

### To enable SSL on the server

1. Generate a Certificate Authority (CA) signed certificate or a self-signed certificate.
2. If the certificate used by the EnterpriseView Web server is issued by a well-known CA, it is most likely that your browsers can validate the certificate without any further action. If it is not, for all clients that need to communicate with EnterpriseView, place the certificate in the client's trusted store.
3. Open the following file:  
  
**<EnterpriseView Installation Folder>\bsf\conf\client-config.properties**
4. Change the value of **bsf.server.url** to **https://127.0.0.1:8443/bsf**.
5. Open the following file:  
  
**<EnterpriseView Installation Folder>\tomcat\conf\server.xml**
6. Locate the section beginning with **<Connector port="8443"** which appears in comments. Activate the script by removing the comment character.

7. Add the following properties to the tag:

- **keystoreFile**="**<tomcat.keystore file location>**"
- **keystorePass**="**<password>**"

8. Comment the following line:

```
<Listener className="org.apache.catalina.core.AprLifecycleListener"  
SSLEngine="on" />
```

9. Restart the server.

10. To verify the procedure, open EnterpriseView using the following URL:

**https://<EnterpriseView server name or IP address>:8443/redcat**

## Enable SSL on the Server with a Self-Signed Certificate

**Note:** All directory and file locations depend on your specific platform, operating system, and installation preferences.

### To enable SSL with a self-signed certificate

1. Make sure that the following file does not exist or is deleted:

**<EnterpriseView Installation Folder>\jre\<Operating System>\lib\security\tomcat.keystore**

2. Create a keystore (JKS type) with a self-signed certificate and matching private key, as described in the following steps:

- a. Open a command line from the following folder:

**<EnterpriseView Installation Folder>\jre\<Operating System>\bin**

- b. Run the following command:

**keytool -genkey -alias tomcat -keyalg RSA -keystore ../lib/security/tomcat.keystore**

- c. Enter the keystore password, and then press **ENTER**.
- d. Answer the series of questions presented to you. When asked for your first and last name, enter **EnterpriseView**. When you are prompted to confirm your answers, enter **yes** or **no**, and then press **ENTER**.

- e. When you are prompted to enter a key password, press **ENTER**.

The key password must be the same as the keystore password.

A JKS keystore is created named **tomcat.keystore** with a server certificate with the name you provided in step b.

3. Open a command line from the following folder:

**<EnterpriseView Installation Folder>\jre\<Operating System>\bin**

4. Run the following command:

**keytool.exe -exportcert -alias tomcat -keystore ../lib/security/tomcat.keystore -file ../lib/security/tomcat.cer**

A certificate named **tomcat.cer** is created in the **<EnterpriseView Installation Folder>\jre\<Operating System>\lib\security** folder.

5. Install the **tomcat.cer** file on all the browsers in the client machines.

6. Open the following file:

**<EnterpriseView Installation Folder>\bsf\conf\client-config.properties**

7. Change the value of **bsf.server.url** to the following:

**https://<domain name>:8443/bsf**

**Note:** Make sure that you change only **bsf.server.url** and not another value.

8. Open the following file:

**<EnterpriseView Installation Folder>\tomcat\conf\server.xml**

9. Locate the section beginning with **Connector port="8443"** which appears in comments. Activate the script by removing the comment character.

10. Add the following properties to the tag:

- **keystoreFile="<EnterpriseView Installation Folder>\jre\<OS>\lib\security\tomcat.keystore"**
- **keystorePass="<password>"**

11. Comment the following line:

**<Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />**

12. Restart the server.
13. To verify the procedure, open EnterpriseView using the following URL:  
**`https://<EnterpriseView server name or IP address>:8443/redcat`**





# 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 58](#).

## 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.

Priority Factor	Description
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	<p>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.</p> <p>/System Asset Categories/Criticality/Very High (+10)</p> <p>/System Asset Categories/Criticality/High (+8)</p> <p>/System Asset Categories/Criticality/Medium (+6)</p> <p>/System Asset Categories/Criticality/Low (+4)</p> <p>/System Asset Categories/Criticality/Very Low (+2)</p> <p>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.</p>

## 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 (Assets\_and\_Threats.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 **Assets\_and\_Threats.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
<b>*</b> (all values)	Used to select all values within a field. For example "*" in the minute field means "every minute".
<b>?</b> (no specific value)	Used 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.
<b>-</b>	Used to specify ranges. For example, "10-12" in the hour field means "the hours 10, 11 and 12".
<b>,</b>	Used to specify additional values. For example, "MON,WED,FRI" in the day-of-week field means "the days Monday, Wednesday, and Friday".
<b>/</b>	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".

### Cron Expression Special Characters, continued

Character	Description
<b>L</b> <b>(last)</b>	When used in the day-of-month field: The value "L" means "the last day of the month" - day 31 for January, day 28 for February on non-leap years. 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 used in the day-of-week field: - Used by itself, it simply means the last day of the week, which is "7" or "SAT". - Used after another value, it means "the last xxx day of the month", for example "6L" means "the last Friday of the month". When using the 'L' option, it is important not to specify lists, or ranges of values, as you'll get confusing/unexpected results.
<b>W</b> <b>(weekday)</b>	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".
<b>#</b>	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.