HP EnterpriseView

For the Windows Operating System

Software Version: 2.5

Deployment Guide

Document Release Date: April 2014

Software Release Date: April 2014

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

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

Restricted Rights Legend

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

Copyright Notice

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

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

This document is confidential.

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

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

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

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

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

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

To find more information about access levels, go to:

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

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

Contents

Chapter 1: Welcome to This Guide

Welcome to the HP EnterpriseView 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

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

The main modules in EnterpriseView are:

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

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

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

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

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

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

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

Chapter 2: Install EnterpriseView

This chapter describes how to install and start EnterpriseView.

EnterpriseView integrates with SAP BusinessObjects Enterprise primarily for creating reports and dashboards, but also for user management. Before you install EnterpriseView, you must have a complete installation of BusinessObjects version 3.1 SP 5.0 running on your network.

Note: EnterpriseView supports only a new installation of BusinessObjects, which is delivered with the EnterpriseView installation package. It does not support the installation of EnterpriseView alongside an existing installation of 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 14.
3. Install BusinessObjects. For more information, see "Install SAP BusinessObjects Enterprise " on page 15.
4. Configure SAP BusinessObjects Enterprise. For more information, see "Configure BusinessObjects Enterprise" on page 16.
5. Run the EnterpriseView setup wizard. For more information, see "Run EnterpriseView Setup Wizard" on page 19.

After you have completed the tasks above, proceed to the "Post Installation Tasks" on page 22.

System Requirements

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

Note:

- We recommend installing 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 BusinessObjects and on the server on which you are installing EnterpriseView are synchronized.

EnterpriseView Server System Requirements

Element	Requirement
CPU	• If EnterpriseView is installed separately: 4 CPU Cores (minimum) • If BusinessObjects and EnterpriseView are installed on the same server: 8 CPU Cores (minimum) • If BusinessObjects, EnterpriseView, and Oracle database are installed on the same server: 12 CPU Cores (minimum)
Free Disk Space	25 GB (minimum)
Memory (RAM)	• If EnterpriseView is installed separately: 8 GB (minimum) • If BusinessObjects and EnterpriseView are installed on the same server: 12 GB (minimum) • If BusinessObjects, EnterpriseView, and Oracle database are installed on the same server: 16 GB (minimum)
Operating System	Windows Server 2008 R2 (x64) Enterprise Edition
Java Version	1.7

BusinessObjects Server System Requirements

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

EnterpriseView Database Requirements

Element	Requirement
Type	Oracle Standard Edition 11.2.0.1 or later
CPU	8 CPU Cores (minimum)
Memory (RAM)	8 GB (minimum)
Tablespace for EnterpriseView	50 GB

EnterpriseView Database Requirements, continued

Element	Requirement
Tablespace for User Management Module	0.5 GB
Temporary Tablespace for EnterpriseView	50 GB

BusinessObjects Database Requirements

Element	Requirement
Type	Oracle 11.2.0.1 or later **Note:** The EnterpriseView system is certified to work only with an Oracle database, however, BusinessObjects can also be installed with other databases, such as MySQL and SQL Server. For more information, see the BusinessObjects documentation. The installation described in this chapter assumes that BusinessObjects is installed with an Oracle database.
Tablespace for BusinessObjects	2 GB

Client Requirements

Element	Requirement
Browser	• Microsoft Internet Explorer 9.x and 10.x (compatibility view is not supported) • Mozilla Firefox 27.0 or later (32-bit) • Google Chrome
Adobe Flash Player	Flash Player 11.0
Screen Resolution	Recommended 1440x900

Integration Matrix

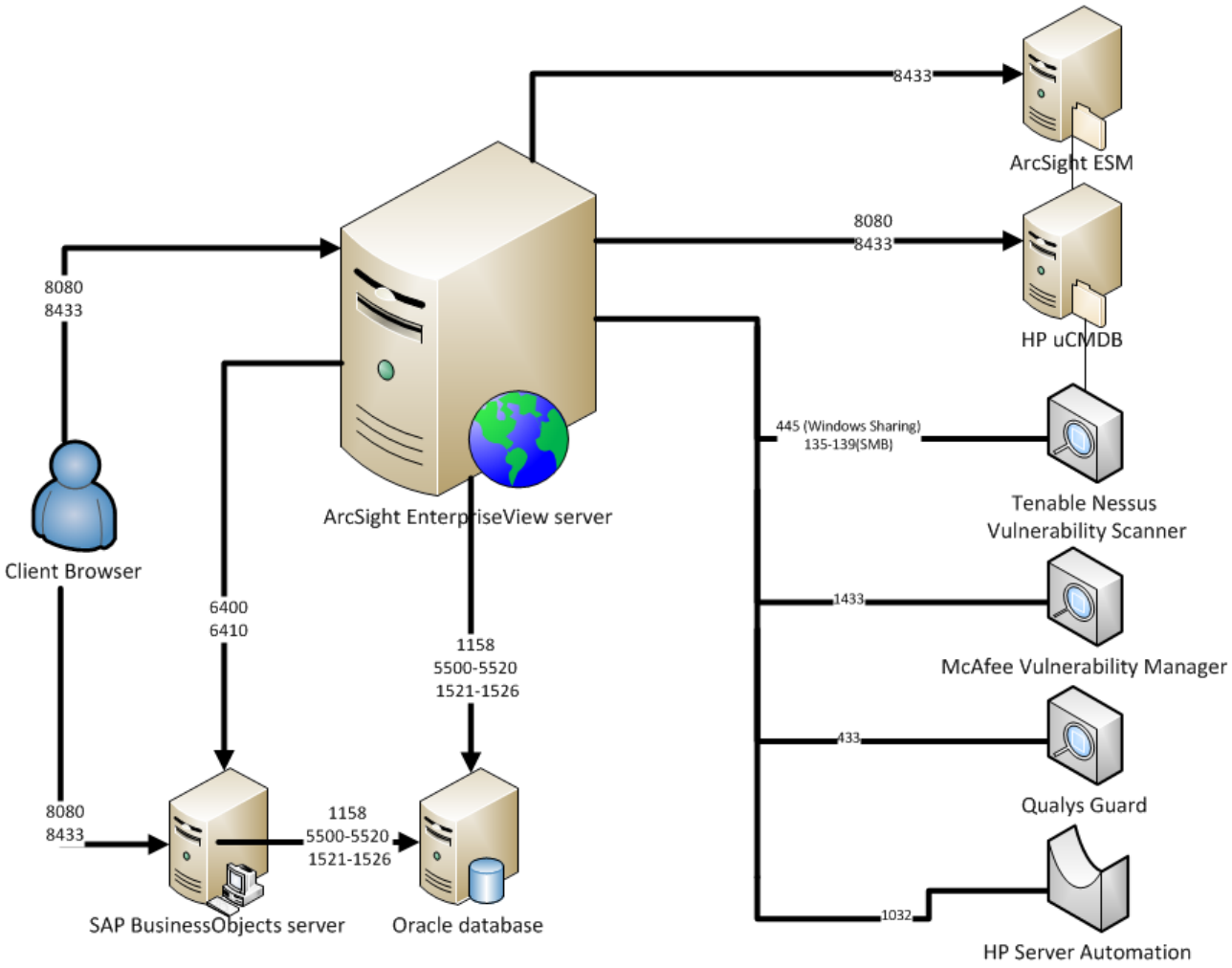
The following table includes the supported versions of products that EnterpriseView integrates with.

Product	Version
HP Universal CMDB	9.x, 10.x
HP Configuration Manager	10.10 Build 8
ArcSight Enterprise Security Manager	6.0c, 6.5

Product	Version
ArcSight Express	4.0
HP Server Automation (SA)	9.10
ArcSight SmartConnector	6.0.5.6782
Tenable Nessus Vulnerability Scanner	3.2.x, 4.x, 5.x
McAfee Vulnerability Manager (Foundscan)	7.0
Qualys Guard	6.05, 7.1
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 start installing EnterpriseView, perform the following tasks:

- Allocate new Oracle user schemas; for EnterpriseView 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 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 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 BusinessObjects is installed has a firewall installed, make sure that all BusinessObjects ports are open.
- 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

Note: SAP BusinessObjects Enterprise installation alongside EnterpriseView is supported only in the English language.

The following procedure includes the installation of SAP BusinessObjects Enterprise, BusinessObjects client tools, and a partial configuration of BusinessObjects. After you complete this procedure, complete the BusinessObjects configuration, as described in "Configure BusinessObjects Enterprise" on the next page.

before you begin the installation, you must disable all anti-virus applications installed on the BusinessObjects server. After you complete the installation, you can enable the anti-virus applications again.

After you install BusinessObjects, use the following credentials to log on:

- User name: **Administrator**
- Password: **admin123**

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*.

Perform the following procedure as an Administrator.

To install BusinessObjects

1. From the HP EnterpriseView installation medium, copy the following folder to the server on which you are installing BusinessObjects:

   Installations\SAP BusinessObjects

2. Open the **Installations\SAP BusinessObjects** folder, and run the following file

   installbo.bat

   The installation begins. You will be prompted to enter Oracle database and Tomcat server information. Enter the required information.

   Note: Default values are displayed in parenthesis.

Configure BusinessObjects Enterprise

After BusinessObjects is installed, perform the following procedures:

Configure the maximum number of simultaneous connections

1. Open SAP BusinessObjects Enterprise.
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 *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 *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 BusinessObjects

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

1. Open SAP BusinessObjects Enterprise.
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**.

Update the time zone

1. Open InfoView (BusinessObjects client tool) using the following URL:

   http://[server_name]:8081/InfoViewApp

2. On the top right corner, click **Preferences**.
3. From the **Current Time Zone** list, select your time zone.
4. Save the changes.

Restart the BusinessObjects server

1. In the 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 BusinessObjects servers, see the *BusinessObjects Administrator Guide*.

After the configuration is complete, it is recommended that you run the 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 *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 "Post Installation Tasks" on page 22.

Perform the following procedure as an Administrator.

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 BusinessObjects in the folders that you have defined during the installation.
   >
   > Reports: Folders > All Folders > <EnterpriseViewFolder>
   >
   > Universe: Universes > Universes > <EnterpriseViewUniverse>
4. EnterpriseView is installed with the default port 8080. If you want to change this port, open the following files and change all instances of 8080 to the port that you want to set for EnterpriseView:
   - **<EnterpriseView Installation Folder>\tomcat\conf\server.xml**

     > **Note:** If required, change the default shutdown port (8005) and the default redirect port (8443).
   - **<EnterpriseView Installation Folder>\bsf\conf\client-config.properties**
   - **<EnterpriseView Installation Folder>\bsf\conf\resource.properties**

- **<EnterpriseView Installation Folder>\tomcat\webapps\activiti-modeler\WEB-INF\classes\configuration.properties**

5. Restart the computer.

   The EnterpriseView application starts automatically. The service name is:

   HP EnterpriseView

6. Log on to EnterpriseView, as described in "Log On To EnterpriseView" on page 21.

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

Chapter 3: 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 27.

For details on Web browser requirements, see "System Requirements" on page 9.

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 through **http://<server IP or host name>: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 BusinessObjects, and then click **Login**.

Chapter 4: 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 23.

2. Configure your User Management system, as described in "User Management" on page 25. Users and groups must already be defined either in BusinessObjects or in a security system integrated with 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 27. You can also create new roles, as described in "Add Roles" on page 26.

3. Define named users in BusinessObjects. For more information, see "Define a Named User in BusinessObjects Enterprise" on page 40.

4. If required, integrate with an external system, as described in "Synchronize Assets with External Asset Repository" on page 41 and "Import Vulnerabilities From Vulnerability Assessment Tools" on page 59.

Chapter 5: Connect to Active Directory

If you are using Active Directory (AD) for authenticating users, then you have already configured it in 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>\conf\ad\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 **MYDCHOSTNAME.MYDOMAIN.COM** to the full computer name of the server where AD is installed. Enter the name in upper-case.

   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 = **MYDCHOSTNAME.MYDOMAIN.COM**

   default_domain = **MYDOMAIN.COM**

```
}
```

4. Start the EnterpriseView service.

Chapter 6: User Management

EnterpriseView integrates with SAP BusinessObjects Enterprise primarily for delivering robust reporting functionality, but also for user management. Users and groups are managed in BusinessObjects, but are displayed in EnterpriseView as well. Any changes that are made to users and groups in BusinessObjects are automatically reflected in EnterpriseView. If BusinessObjects is integrated with a security system, such as an LDAP server, then any change made in the security system is propagated to both 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 *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 27. 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 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 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 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 *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 (asterisk) 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 through 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 25.

Role	Permissions	Accessible components
All roles	• Login • View Executive View Settings • View Task Management • View Task Management Settings • View External Risk Factor Settings • View Executive View Dashboards	• Task Management Dashboard • Workflow Management • My Tasks • External Risk Factors Dashboard • External Risk Factor Management • Risk Register • Overall Score Heat Map • Risk Indicators • Audit Log • Settings > Executive View • Settings > Task Management • Settings > External Risk Factors • Vulnerability Dictionary **Note:** All roles can view the Executive View module (Settings and Dashboards) except for: • Task Management Template Manager • Task Management Administrator
Asset Profiler	• View Assets • Edit Assets	• Asset Profiling

Role	Permissions	Accessible components
Policy Auditor	• View Policies • View Policy Statement of Applicability • View Assets • View Policy Assessments • Edit Policy Assessments • View Policy and Compliance Settings • Edit Policy And Compliance Settings • View Policy Dashboards • View Mappings	• Policy Assessment • Policy Builder • Statement of Applicability • Policy Mapping • Asset Profiling • Control to Threat Mapping • Control to Vulnerability Mapping • Settings > Policy and Compliance • Compliance Dashboard • Compliance by Policy Dashboard • Policy Compliance Map

Role	Permissions	Accessible components
Policy Compliance Manager	• View Policies • View Policy Statement of Applicability • Edit Policy Statement of Applicability • View Assets • View Policy Assessments • View Policy and Compliance Settings • Edit Policy And Compliance Settings • Edit Task Management • Edit Task management Settings • View Policy Dashboards • View Mappings	• Statement of Applicability • Policy Builder • Policy Assessment • Policy Mapping • Asset Profiling • Control to Threat Mapping • Control to Vulnerability Mapping • Settings > Policy and Compliance • Compliance Dashboard • Compliance by Policy Dashboard • Policy Compliance Map

Role	Permissions	Accessible components
Policy Builder	• View Policies • Edit Policies • View Policy and Compliance Settings • Edit Policy and Compliance Settings • Edit Task Management • Edit Task Management Settings • View Policy Dashboards • View Policy Assessments • View Policy Statement of Applicability • View Assets • View Mappings • Edit Mappings	• Policy Builder • Policy Assessment • Statement of Applicability • Asset Profiling • Policy Mapping • Control to Threat Mapping • Control to Vulnerability Mapping • Settings > Policy and Compliance • Compliance Dashboard • Compliance by Policy Dashboard • Policy Compliance Map

Role	Permissions	Accessible components
Policy Viewer	• View Policies • View Assets • View Policy Statement of Applicability • View Policy Assessments • View Policy and Compliance Settings • View Policy Dashboards • View Mappings	• Policy Assessment • Statement of Applicability • Policy Mapping • Asset Profiling • Control to Threat Mapping • Control to Vulnerability Mapping • Settings > Policy and Compliance • Compliance Dashboard • Compliance by Policy Dashboard • Policy Compliance Map

Role	Permissions	Accessible components
Risk Auditor	• View Risk Assessment and Treatment • Edit Risk Assessment and Treatment • View Threat Assignment • Edit Threat Assignment • View Assets • View Threat Library • View Risk Modeling Settings • Edit Risk Modeling Settings • Edit Task Management • Edit task Management Settings • View Risk Modeling Dashboards • View Mappings	• Risk Assessment and Treatment • Threat Assignment • Threat Library Builder • Asset Profiling • Control to Threat Mapping • Control to Vulnerability Mapping • Settings >Risk Modeling • Risk Modeling Dashboard • Risk Heat Map and Scorecard

Role	Permissions	Accessible components
Risk Viewer	• View Risk Assessment and Treatment • View Threat Assignment • View Assets • View Threat Library • View Risk Modeling Settings • View Risk Modeling Dashboards • View Mappings	• Risk Assessment and Treatment • Threat Library Builder • Asset Profiling • Control to Threat Mapping • Control to Vulnerability Mapping • Settings >Risk Modeling • Risk Modeling Dashboard • Risk Scorecard and Heat Map

Role	Permissions	Accessible components
Security Officer	• View Risk Assessment and Treatment • View Threat Assignment • Edit External Risk Factor Settings • View External Risk Factor Settings • Edit Task Management Settings • View Assets • View Threat Library • View Policies • View Policy Statement of Applicability • View Policy Assessments • View Vulnerabilities • Edit Executive View Settings • View Risk Modeling Settings • View Vulnerabilities Settings • View Policy And Compliance Settings • Edit Task Management • View Risk Modeling Dashboards	• Policy Compliance Map • Risk Assessment and Treatment • Control to Threat Mapping • Control to Vulnerability Mapping • Settings (all pages) • Risk Modeling Dashboard • Risk Scorecard and Heat Map • Compliance Dashboard • Compliance by Policy Dashboard • Vulnerability Dashboard • Threat Library Builder • Threat Assignment • Vulnerability Assignment • Vulnerability Management • Policy Builder • Statement of Applicability • Policy Assessment • Asset Profiling

Role	Permissions	Accessible components
	• View Policy Dashboards • View Vulnerability Dashboards • View Mappings • Edit Mappings	

Role	Permissions	Accessible components
Threat Library Administrator	• View Risk Assessment and Treatment • Edit Risk Assessment and Treatment • View Threat Assignment • Edit Threat Assignment • View Assets • View Threat Library • Edit Threat Library • View Risk Modeling Settings • Edit Risk Modeling Settings • Edit Task Management • Edit Task Management Settings • View Risk Modeling Dashboards • View Mappings • Edit Mappings	• Threat Library Builder • Threat Assignment • Asset Profiling • Risk Assessment and Treatment • Control to Threat Mapping • Control to Vulnerability Mapping • Settings > Risk Modeling • Risk Modeling Dashboard • Risk Heat Map and Scorecard
Security Threat Viewer	• View Assets	• Asset Profiling

Role	Permissions	Accessible components
Vulnerability Manager	• View asset • View vulnerabilities • Edit vulnerabilities • View Vulnerability Settings • Edit Vulnerability Settings • Edit Task Management • Edit Task Management Settings • View Vulnerability Dashboards • View Mappings	• Vulnerability Management • Vulnerability Assignment • Asset Profiling • Settings > Vulnerabilities • Vulnerability Dashboard • Control to Vulnerability Mapping • Control to Threat Mapping
Vulnerability Viewer	• View asset • View vulnerabilities • View Vulnerability Settings • View Vulnerability Dashboards	• Vulnerability Management • Vulnerability Assignment • Asset Profiling • Vulnerability Dashboard
Task Management Template Manager	• Edit Task Management • Edit Template Management • Edit Task Management Settings	Manage Templates (dialog box)

Role	Permissions	Accessible components
Task Management Administrator	• Edit Task Management • Edit Template Management • View All Workflows • Edit Task Management Settings	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 BusinessObjects

1. Open SAP BusinessObjects Enterprise.
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 7: 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 45.

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 "Import Assets from HP Universal CMDB" below.
- ArcSight Enterprise Security Manager. For more information see "Import Assets from ArcSight ESM" on page 47.

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 a CSV File" on page 52.

You can synchronize assets with only one external asset repository.

Import Assets from 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 46. To learn more about the Synchronization job, see "About UCMDB Asset Synchronization Job" on the next page.

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 next 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 47.

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 45 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 45.

6. **Schedule and activate the Synchronization job** to complete the process, as described in "Schedule and Activate the UCMDB Asset Synchronization Job" on page 46.

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 > HP Universal CMDB**.

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

Parameters	Description
Communication Protocol	Select either **HTTP** or **HTTPS**, according to the specifications received from the UCMDB administrator.

Parameters	Description
Communication Host	The host name or IP address of the UCMDB server, provided by the UCMDB administrator.
Communication Port	The UCMDB server port, provided by the UCMDB administrator.
UCMDB User Name	Credentials for accessing UCMDB, provided by the UCMDB administrator.
UCMDB Password	Credentials for accessing UCMDB, provided by the UCMDB administrator.
Application Context	Credentials for accessing UCMDB, provided by the UCMDB administrator.
TQL Query Name	The name of the TQL query that EnterpriseView activates for retrieving assets, provided by the UCMDB administrator.
Max Bulk Size	Defines the maximum number of UCMDB entities (assets and relationships) that the query returns to EnterpriseView at a time.

4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 70.

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 > HP Universal CMDB**.
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 70.

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 > HP Universal CMDB**.
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 70.

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

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 70.

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 42.

To schedule and activate a synchronization job

1. Click **Administration > Configuration**.
2. In the left pane, click **Integrations > UCMDB > Asset Synchronization > HP Universal CMDB**.
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.
   - In **Job Schedule**, select the options for the recurrence pattern you want (every number of

minutes, every number of hours, every number of days, or on certain days of the week).

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

4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 70.

   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 > HP Universal CMDB**.
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 70.

Import Assets from ArcSight ESM

You can integrate with ArcSight ESM in order to synchronize the EnterpriseView business model with ArcSight ESM assets.

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 the Risk_Insight.arb (ArcSight Resource Bundle) file in ESM. 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 "Import EnterpriseView Reports into ArcSight ESM" on page 81. The file 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 information.

The ArcSight ESM administrator should provide you with connection parameters, described in "Define Connection Parameters with ESM" on page 49. 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 next page.

After EnterpriseView is fully integrated with ArcSight ESM, the Synchronization job runs periodically, according to the schedule that you defined. To learn more about the Asset Synchronization job, see "About ArcSight ESM Asset Synchronization Job" on the next page.

About ArcSight ESM Asset Synchronization Job

The Asset Synchronization Job periodically imports ArcSight ESM entities from ArcSight ESM into EnterpriseView, as follows:

1. The EnterpriseView Asset Report is created based on the EnterpriseView_Assets.arb ArcSight Resource Bundle (*.arb) file.
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 50.
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.

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 ESM Manager.

   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 the next page 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 45.

5. **Schedule and activate the Synchronization job** in order to complete the process, as described in "Schedule and Activate the ESM Job" on page 52.

Change ESM Session Timeout

Note: Changing the session timeout requires restarting ESM Manager.

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

4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 70.

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.

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. 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 70.

Schedule and Activate the 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 48.

To schedule and activate a synchronization job

1. Click **Administration > Configuration**.
2. In the left pane, click **Integrations > ArcSight ESM > Asset Synchronization > Schedule Job**.
3. In the **Job** page, do the following:
   - In **Job Schedule**, select the options for the recurrence pattern you want (every number of minutes, every number of hours, every number of days, or on certain days of the week).
   - Select the **Activate Job** check box.
4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 70.

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

Import Assets From a CSV File

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 56.

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 54.

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 (in any order):

- 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.
3. If any errors occur during this process, then they are written to the **all-errors.log** file located in **<EnterpriseView installation folder>/logs**. Each log record includes the line number of the faulty CSV record. For example:

   Line 1: Asset External ID field is empty.

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.
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.
The string in one of the fields is longer than 255 characters.	Record is skipped.
The CPE is unknown (not defined in EnterpriseView).	CPE information is not imported for the asset.

4. The elements in the CSV file are converted into EnterpriseView assets and relationships.
5. 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.
6. Outdated assets and their relationships (meaning that they no longer exist in the CSV file) are deleted from the EnterpriseView database.
7. 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 page 54.

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" below.
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 45.
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
Connector Name	A logical name for the asset repository from which you are importing. This is the name that is displayed in the **Source** property of the asset.
Asset File path	The location of the asset file that is imported into EnterpriseView. The file can be placed anywhere in the network, as long as EnterpriseView can access the path.
Relationship File Path	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.

Parameter	Description
Max Business Criticality Level in Source	The upper limit of the business criticality in the asset repository from which you are importing your business model. The criticality level range in the asset repository from which you are importing your business model might be different than the one employed by EnterpriseView. EnterpriseView uses a range of 0 to 10. During the import process, the criticality level is normalized according to this parameter.

4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 70.

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 asset category name as defined in EnterpriseView. 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 70.

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 54.

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:
   - In **Job Schedule**, select the options for the recurrence pattern you want (every number of minutes, every number of hours, every number of days, or on certain days of the week).
   - Select the **Activate Job** check box.
4. Save and apply the configuration changes. For more information, see "Save and Apply Configuration Changes" on page 70.

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

Chapter 8: 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)	McAffee 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 page 61 and then "Schedule and Activate Vulnerabilities Import Job" on page 64.

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 days) 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 64.

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

You can either install a new connector or add a destination to an existing connector. For more information on destinations, see the *SmartConnector Destinations* chapter in the *ArcSight SmartConnector User's Guide*. Connectors do not have to be installed on the ESM server.

If you are installing a new connector, 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 QualysGuard File
- ArcSight FlexConnector XML file (for HP WebInspect)
- Rapid7 NeXpose XML File

The configuration tool is used to configure new connectors and to add a destination to an existing connector.

Note: It is important that you perform the configuration procedure immediately after you install the connector.

In order for EnterpriseView to work with ArcSight SmartConnectors, you need to run the configuration tool for each connector, this means that if you have two connectors, then you need to run the tool twice, once for each connector. 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>

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

To install a connector

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

1. From the EnterpriseView installation medium, open the **Connectors** folder.
2. Start the ArcSight SmartConnector Installer by running one of the following (depending on the operating system installed on the server):

   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. When prompted to select a **Mode**, select **Automatic**.

   c. When prompted, select **Yes, I want to configure the SmartConnector to run as a service**.

   For each connector that you install, a dedicated folder (for example, ArcSight SmarConnector Nessus) is created under the root/Program Files folder.

To configure a connector or add a destination to an existing connector

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

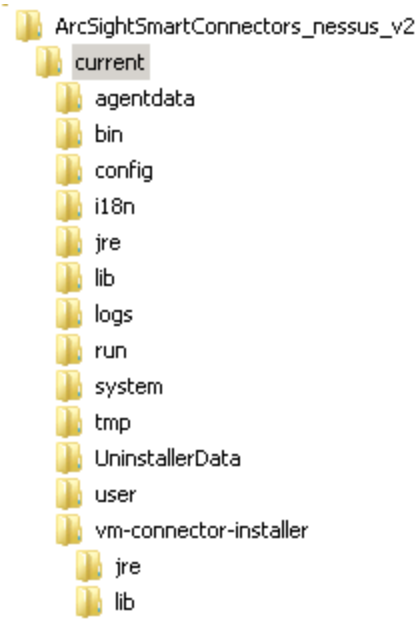
   \Connectors\ArcSight SmartConnectors\Tools\ArcSight SmartConnector Configuration tool.zip

   To this directory:

   <Connector Installation Folder>\current

   For example: ArcSightSmartConnectors Nessus\current
2. Extract the zip file to the **current** folder. The content of the zip file should be directly under the **Current** folder.

   For example:



3. Open the following folder from the command line:

   <Connector Installation Folder>\current\bin

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

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

4. Do one of the following:

   - Configure a new connector by running the following command:

     run_vm_connector_config_*.* <EnterpriseView installation folder>\vm\import\pending

   - Add a destination to an existing connector by running the following command:

     run_vm_connector_config_*.* <EnterpriseView installation folder>\vm\import\pending - extend

Note: Make sure that the connector has **write** permissions for the following folder in EnterpriseView:

<EnterpriseView installation folder>\vm\import\pending

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

5. 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 60.

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 **Job Schedule**, select the options for the recurrence pattern you want (every number of minutes, every number of hours, every number of days, or on certain days of the week).
   c. 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 70.

Chapter 9: 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 next 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 68.

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 through EnterpriseView; it is monitored using 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 10: Manage Configuration Sets

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

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

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

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

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

Select Configuration Set

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

To select a configuration set

1. Click **Administration > Configuration**.

2. In the **Configuration** window, in the left pane, click the **Open Configuration Set**  button.

   The currently active configuration set is displayed in bold.

3. In the **Open Configuration Set** window, from the list of configuration sets, click the one that you want to run, and then click **Open**.

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

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

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

   In the **Activate Configuration Set** dialog box, click **Yes**.

Migrate Configuration Data

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

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

To migrate configuration data

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

     Integrations > ArcSight ESM

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

Save and Apply Configuration Changes

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

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

To create a new configuration set

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

   EnterpriseView applies the new configuration settings when you activate the draft.

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

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

Chapter 11: 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 75. 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 77.

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" on the next page.

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 through 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>\conf\encryption.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 passwords 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 70

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	The infrastructure implementing the encryption algorithm. The available options are: • **lw**: Uses Bouncy Castle lightweight implementation (Default option) • **jce**: Java Cryptography Enhancement (standard Java cryptography infrastructure)
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	The name of the encryption algorithm. The following options are available: • **AES**: American Encryption Standard. This encryption is FIPS 140-2 compliant. (Default option) • **Blowfish** • **DES** • **3DES**: (FIPS 140-2 compliant) • **Null**: No encryption
keySize	The size of the master key. The size is determined by the algorithm: • **AES**: 128, 192, or 256 (Default option is 256) • **Blowfish**: 0-400 • **DES**: 56 • **3DES**: 156
encodingMode	The ASCII encoding of the binary encryption results. The following options are available: • **Base64** (Default option) • **Base64Url** • **Hex**

Parameter	Description
algorithmModeName	The mode of the algorithm. Currently, only **CBC** is supported.
algorithmPaddingName	The padding algorithm used. The following options are available: • **PKCS7Padding** (Default option) • **PKCS5Padding**
jceProviderName	The name of the JCE encryption algorithm. **Note:** Only relevant when crytpSource is **jce**. For **lw**, 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 page 77.

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://<EnterpriseView server hostname>: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="<EnterpriseView_installation_ folder>\jre\windows\lib\security\tomcat.keystore"**
   - **keystorePass="${key.store.pass}"**

8. Comment the following line:

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

9. Create an encrypted password, as described in "Encrypt Password" on page 72. Save the password for step 11.

10. Open the following file:

    <EnterpriseView Installation Folder>\tomcat\conf\catalina.properties

11. Copy the following line to the beginning of the file:

    - **org.apache.tomcat.util.digester.PROPERTY_ SOURCE=com.hp.onyx.commons.encryption.tomcat.PropertyDecryptor**

      Note: This is one line. Make sure that there is no space after the underscore **PROPERTY_SOURCE**.

    - **key.store.pass=<ENCRYPTED PASSWORD>**

    Note: The ENCRYPED PASSWORD parameter is the password that you created in step 9.

12. Find the following line:

    common.loader=${catalina.base}/lib,${catalina.base}/lib/*.jar,${catalina.home} /lib,${catalina.home}/lib/*.jar

    Add the part in red to the end of the line:

    common.loader=${catalina.base}/lib,${catalina.base}/lib/*.jar,${catalina.home} /lib,${catalina.home}/lib/*.jar,${catalina.home}/webapps/redcat/WEB-INF/lib/*.jar

13. Save and close the file.

14. Restart the server.

15. 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://<EnterpriseView server hostname>: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\windows\lib\security\tomcat.keystore"**
    - **keystorePass="${key.store.pass}"**
11. Comment the following line:

    <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
12. Create an encrypted password, as described in "Encrypt Password" on page 72. Save the password for step 14.
13. Open the following file:

    <EnterpriseView Installation Folder>\tomcat\conf\catalina.properties
14. Copy the following lines to the beginning of the file:

    - **org.apache.tomcat.util.digester.PROPERTY_ SOURCE=com.hp.onyx.commons.encryption.tomcat.PropertyDecryptor**

> **Note:** This is one line. Make sure that there is no space after the underscore **PROPERTY_SOURCE**.

- **key.store.pass=<ENCRYPTED PASSWORD>**

> **Note:** The ENCRYPED PASSWORD parameter is the password that you created in step 12.

15. Find the following line:

    common.loader=${catalina.base}/lib,${catalina.base}/lib/*.jar,${catalina.home}/lib,${catalina.home}/lib/*.jar

    Add the part in red to the end of the line:

    common.loader=${catalina.base}/lib,${catalina.base}/lib/*.jar,${catalina.home}/lib,${catalina.home}/lib/*.jar,${catalina.home}/webapps/redcat/WEB-INF/lib/*.jar

16. Save and close the file.

17. Restart the server.

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

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

Appendix A: Asset Reporting

The following sections describe this report and provide additional information about accessing it and interpreting its content. For more information about integration with EnterpriseView, see "Import Assets from ArcSight ESM" on page 47.

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
- Zone Name
- Zone ID

- Asset URI
- All Categories

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

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

Import EnterpriseView Reports into ArcSight ESM

EnterpriseView reports are available from a bundled file, EnterpriseView_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 EnterpriseView_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 Console 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