

# HP Select Audit Software

for the Windows<sup>®</sup>, HP-UX<sup>®</sup>, Linux<sup>®</sup>, and Solaris<sup>®</sup> operating systems

Software Version: 1.03

---

## Administration Guide

Document Release Date: January 2008

Software Release Date: January 2008



## 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.

HP provides third-party products, software, and services that are not HP Branded “AS IS” without warranties or representations of any kind from HP, although the original manufacturers or third party suppliers of such products, software and services may provide their own warranties, representations or conditions. By using this software you accept the terms and conditions.

The information contained herein is subject to change without notice.

### 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 Notices

© Copyright 2006- 2008 Hewlett-Packard Development Company, L.P.

Java™ is a US trademark of Sun Microsystems, Inc.

### Trademark Notices

HP Select Audit includes software developed by third parties. The software HP Select Audit uses includes:

- ANTLR Copyright 2003-2007 Terrence Parr.
- commons-logging from the Apache Software Foundation.
- InstallAnywhere, Copyright 2002-2006 Macrovision Corporation.
- Jasper Decisions Copyright 2000-2006 JasperSoft Corporation.
- JavaScript Tree, Copyright 2002-2003 Geir Landro.
- Legion of the Bouncy Castle developed by Bouncy Castle.
- log4J from the Apache Software Foundation.
- Microsoft SQL Server 2005 JDBC Driver
- OpenAdaptor from the Software Conservancy.
- Oracle JDBC Thin Driver
- Quartz, Copyright 2004 - 2005 OpenSymphony
- spring-framework from the Apache Software Foundation.
- Tomahawk from the Apache Software Foundation.
- treeviewjavascript from GubuSoft.
- Xalan-Java from the Apache Software Foundation.
- Xerces-Java version from the Apache Software Foundation.
- Chart2D from Free Software Foundation, Inc.

Please check the <install\_dir>/3rd\_party\_license folder for expanded copyright notices from such third party suppliers.

## Documentation Updates

This guide's title page contains the following identifying information:

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

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

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

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

## Support

You can visit the HP software support web site at:

**[www.hp.com/go/hpsoftwaresupport](http://www.hp.com/go/hpsoftwaresupport)**

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support 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 find more information about access levels and HP Passport, go to:

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

To find more information about HP Passport, go to:

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



# Contents

<b>1</b>	<b>Introduction</b> .....	11
	Audience .....	11
	Administrator Tasks .....	11
	The Select Audit Documentation Set .....	12
	Chapter Summary .....	12
<b>2</b>	<b>Getting Started</b> .....	15
	Starting Select Audit .....	15
	Audit Portal Features .....	17
	Portal Toolbar .....	17
	Workspaces .....	18
	Setting the Portal Logout Time .....	20
	To set the portal logout time in WebLogic .....	20
	To set the portal logout time in WebSphere .....	21
	Configuring Audit Connectors .....	21
	To configure a connector .....	21
	To manually configure a connector on Linux .....	23
	Correlating Users Between Applications .....	23
	Enabling/Disabling User Correlation .....	24
	Oracle .....	24
	To enable user correlation on Oracle .....	24
	To disable user correlation on Oracle .....	24
	MSSQL .....	25
	To enable user correlation on MSSQL .....	25
	To disable user correlation on MSSQL .....	25
	Configuring a Mail Session .....	25
	Configuring Log4j .....	26
	Enabling Logging .....	26
	Setting Appenders .....	26
	log4j.properties File .....	26
	Globally Configuring the Select Audit Administrator Password .....	30
	Administrator Password Tool .....	30
	To run the Administrator Password Tool .....	30
<b>3</b>	<b>Select Identity Integration</b> .....	33
	Select Identity Permissions .....	33
	Report Permission Mapping .....	33
	Select Identity Permission Policies .....	34
	Select Identity Permission Data .....	34

Select Audit Report Access Control . . . . .	35
Report Level Control . . . . .	35
Row Level Control . . . . .	36
Report Access . . . . .	37
Select Identity and J2EE Integration . . . . .	39
Filtering with Select Identity . . . . .	40
Configuring Select Identity . . . . .	40
To configure Select Identity filtering . . . . .	41
Modifying Select Identity Database Information . . . . .	44
Creating New Select Identity Database Information . . . . .	46
To create or modify database information in the WebSphere console . . . . .	48
<b>4 Select Access Integration . . . . .</b>	<b>51</b>
Integrating Select Access with Select Audit in WebLogic . . . . .	51
Task 1: Create Policy Builder Entries . . . . .	52
Task 2: Choose an Identity Location . . . . .	52
Task 3: Copy the Required Select Access Files . . . . .	56
Task 4: Unsign the JAR File . . . . .	56
Task 5: Configure a Generic Enforcer . . . . .	57
Task 6: Create the bea_enforcer.properties File . . . . .	57
Task 7: Modify startWLSelectAudit.cmd . . . . .	57
Task 8: Create SAREalm . . . . .	59
Task 9: Set SAREalm as the Default Realm . . . . .	59
Task 10: Create an Empty sa.login.config File . . . . .	59
Task 11: Set SelectAccessEnable to True . . . . .	60
Task 12: Modify the directory.xml file . . . . .	61
Task 13: Restart WebLogic . . . . .	61
Integrating Select Access with Select Audit in WebSphere . . . . .	61
Report Access . . . . .	69
<b>5 Models . . . . .</b>	<b>71</b>
Overview . . . . .	71
Operations Model . . . . .	72
Compliance Models . . . . .	72
Model Analysis Tree . . . . .	72
Model History . . . . .	74
Loading Compliance Models . . . . .	74
To load a compliance model . . . . .	75
Configuring Models . . . . .	76
To configure loaded models . . . . .	76
To update a model . . . . .	77
To export a model . . . . .	77
To delete a model . . . . .	78
<b>6 Verifying Data . . . . .</b>	<b>79</b>
Configuring Data Integrity . . . . .	79
To configure data integrity for Java and PKCS12 keystores . . . . .	79
To use .pfx files as keystores . . . . .	81



Configuring Select Audit for Keys Stored on Smart Cards and HSMs . . . . .	82
Verifying Data Integrity . . . . .	82
<b>7 Workflow Attestation . . . . .</b>	<b>85</b>
Configuring Attestation Workflows . . . . .	85
To configure an Attestation workflow. . . . .	85
Approving Reports . . . . .	88
<b>8 Using Reports in Select Audit . . . . .</b>	<b>89</b>
Configuring the Report Server . . . . .	89
Performing System Functions . . . . .	90
To view schedules . . . . .	91
To refresh the folder list . . . . .	91
Jasper Reports Library. . . . .	91
Viewing Log Files . . . . .	91
To view log files . . . . .	92
Viewing the Cache . . . . .	92
Viewing Report Generator Statistics . . . . .	92
To view report generator statistics . . . . .	93
Using the Report Center . . . . .	93
Using My Reports . . . . .	95
Using the Library. . . . .	95
Catalog. . . . .	96
Select Audit Reports . . . . .	96
Select Audit Scheduled. . . . .	96
Select Identity-specific Reports . . . . .	97
User Scopes . . . . .	97
Managing Folders . . . . .	97
To create a sub-folder . . . . .	98
To delete a folder . . . . .	98
To change folder permissions . . . . .	99
Uploading Files . . . . .	101
Managing Reports. . . . .	102
To run a report. . . . .	102
To publish a report. . . . .	103
To schedule report execution. . . . .	103
To check report properties. . . . .	104
Running the Ad Hoc Wizard . . . . .	105
Changing the Date Format for Ad Hoc Reports . . . . .	106
To change the date format. . . . .	106
Creating a Tabular Report . . . . .	106
Creating a Chart . . . . .	110
Searching for Reports . . . . .	114
To search for a report. . . . .	115
To search for data in a report . . . . .	115
Setting Preferences . . . . .	116
Editing Report Schedules . . . . .	117

A	Select Identity/Select Audit Data Filtering .....	119
B	Operations Model Thresholds .....	133
	Batch Count Status .....	133
	Batch Delay Status .....	134
	Audit Workflow Status .....	134
	Index .....	137

# 1 Introduction

HP Select Audit software is part of HP's Identity Management Suite. Select Audit provides reporting, monitoring and alerting capabilities to facilitate risk assessment and breach response processes. It outputs data to multiple destinations including databases and files. Different output destinations can be configured based on the type of audit data, such as audit component (administration session, authentication, access query) and event level (information, warning).

Administrators can view reports, monitor dashboards to respond to alerts, run and schedule reports, and define report templates using the Audit Portal. They can also change the message processing configuration, load message processing plugins, configure processing chains and filters, and monitor status of the audit system.

Once you have installed Select Audit, you must perform additional configuration steps using the Audit Portal. The configuration parameters set in the Audit Portal can be updated as necessary.

## Audience

This guide is intended for Administrators who are responsible for creating and maintaining audit policies and reports, and for administering Select Audit. This guide assumes a working knowledge of the following:

- Audit concepts and requirements.
- The audit life cycle and regulatory compliance requirements.
- The reporting requirements of your company's operational and audit policies.

## Administrator Tasks

Administrators can perform some of the following tasks using the Audit Portal:

- Configuring Select Audit after running the Audit Connector and Audit Server installers.
- Verifying data integrity.
- Administering the Report server.
- Loading, unloading and customizing regulation-specific report packs.
- Loading, unloading and configuring models.
- Creating, running and viewing reports.
- Scheduling Attestation workflows.
- Administering integrations with Select Identity and Select Access.

# The Select Audit Documentation Set

This manual refers to the following Select Audit documents. These documents are available online.

- *HP Select Audit 1.03 Administration Guide*, © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. ([administration\\_guide.pdf](#)).
- *HP Select Audit 1.03 User's Guide*, © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. ([user\\_guide.pdf](#)).
- *HP Select Audit 1.03 Sarbanes-Oxley Model Guide*, © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. ([sb\\_model\\_guide.pdf](#)).
- *HP Select Audit 1.03 Concepts Guide*, © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. ([concepts\\_guide.pdf](#)).
- *HP Select Audit 1.03 Upgrade Procedure*, © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. ([SelectAudit103UpgradeProcedure.pdf](#)).

Online help is available with the Audit Portal.

## Chapter Summary

This guide includes the chapters listed in [Table 1](#).



See the *HP Select Audit 1.03 Release Notes* ([SAudit\\_release\\_notes\\_1.03.html](#)) online for known installation issues at the time of this release.

**Table 1 Guide Overview**

Chapter	Description
<a href="#">Chapter 2, Getting Started</a>	This chapter describes how to access the Audit Portal and begin using Select Audit.
<a href="#">Chapter 3, Select Identity Integration</a>	This chapter describes how to integrate Select Identity with Select Audit.
<a href="#">Chapter 4, Select Access Integration</a>	This chapter describes how to integrate Select Access with Select Audit.
<a href="#">Chapter 5, Models</a>	This chapter describes how to use models in Select Audit.
<a href="#">Chapter 6, Verifying Data</a>	This chapter describes how to configure and verify data integrity.
<a href="#">Chapter 7, Workflow Attestation</a>	This chapter describes how to configure Attestation workflows and approve reports.

**Table 1 Guide Overview (cont'd)**

<b>Chapter</b>	<b>Description</b>
Chapter 8, Using Reports in Select Audit	This chapter describes how to configure the Report server and how to use the Report Center.
Appendix A, Select Identity/Select Audit Data Filtering	This appendix contains a table listing how Select Identity report type permissions are mapped in Select Audit.
Appendix B, Operations Model Thresholds	This appendix describes the default thresholds in the Operations model.



## 2 Getting Started

Select Audit is accessed through the Audit Portal. After you have installed Select Audit, you can configure the connectors, Attestation workflow, data integrity and Report server using the Audit Portal. Once configured, the Audit Portal is used to access the Report Library, perform attestation tasks, approve reports and update models. You can also modify the Select Audit configuration.

Select Audit supports the following browsers:

- Internet Explorer 6
- Firefox

This chapter includes the following topics:

- [Starting Select Audit](#) on page 15
- [Audit Portal Features](#) on page 17
- [Configuring Audit Connectors](#) on page 21
- [Correlating Users Between Applications](#) on page 23
- [Configuring a Mail Session](#) on page 25
- [Configuring Log4j](#) on page 26
- [Globally Configuring the Select Audit Administrator Password](#) on page 30

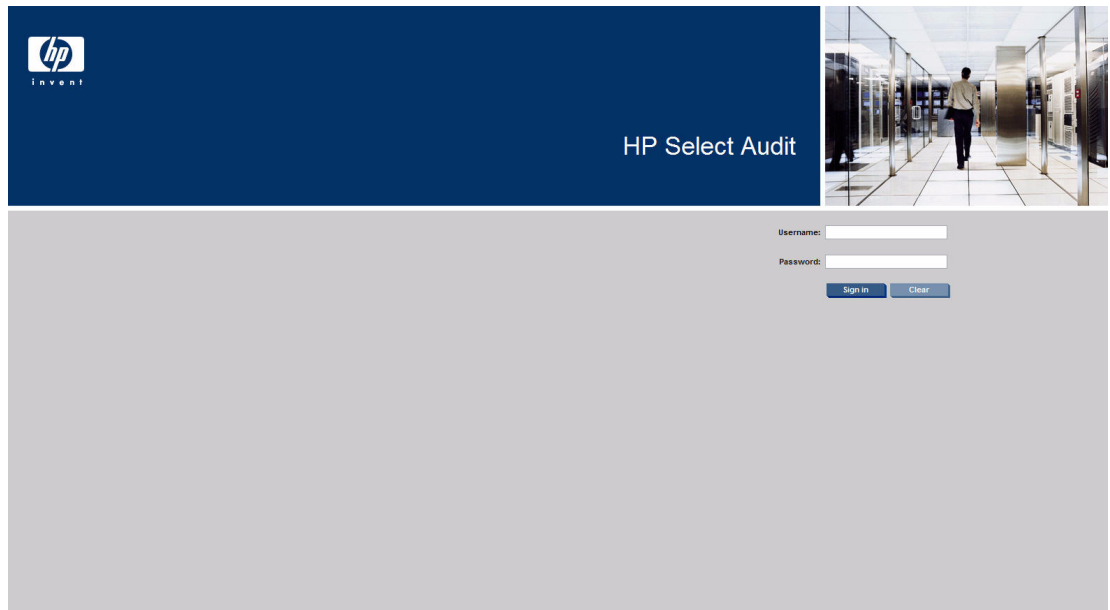
### Starting Select Audit

Once you have installed the Audit Server and Audit Connector, you can access the Select Audit Portal.

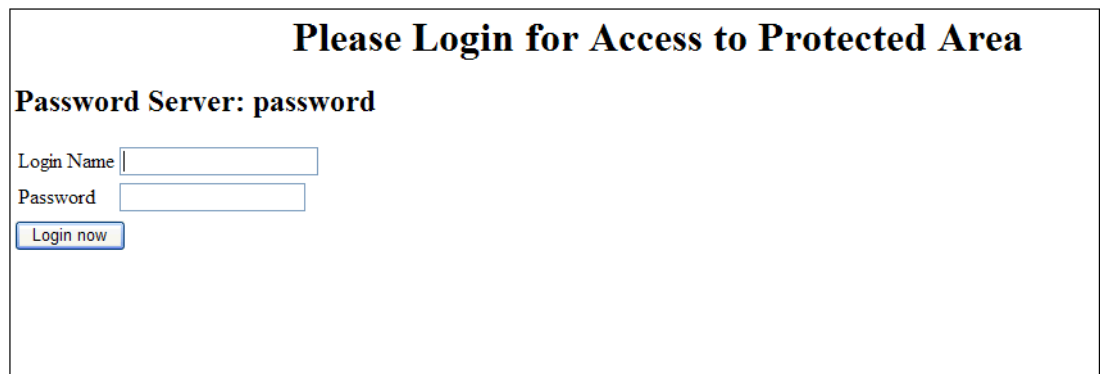
- 1 Open a web browser and type the following URL:

```
http(s)://<host>:<port>/auditportal/
```

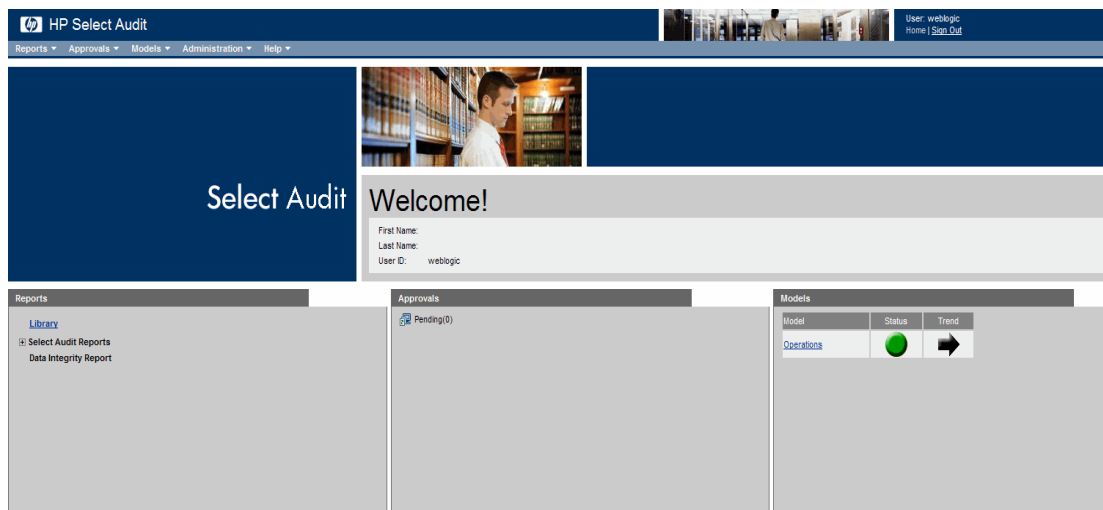
where <host> is the host name of your web server and <port> is its port number. The **Select Audit Login** page opens.



If you are using Select Audit with a Select Access integration, the following screen opens.



- 2 Type your Select Audit user name and password in the appropriate fields and click **Sign In**. The appropriate **Select Audit Portal** opens.





From the Audit Portal you can manage audit functions such as running and scheduling reports in the Report Library, approving reports, loading models and performing administration tasks.

## Audit Portal Features

The Audit Portal is divided into two regions. There is a toolbar at the top of the Portal. The lower portion of the Portal is divided into three workspaces: **Reports**, **Approvals** and **Models**. The toolbar and the workspaces are described below.

### Portal Toolbar

The Portal toolbar is used to setup and maintain different aspects of Select Audit. It contains the following menus: **Reports**, **Models**, **Approvals**, **Administration** and **Help**.

The menus are described in [Table 2](#).

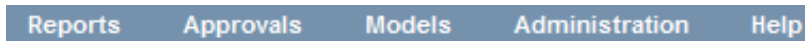
**Table 2 Administrator Toolbar**

Menu Item	Description
Reports	<p>The <b>Reports</b> menu has three entries: <b>Library</b>, <b>My Reports</b> and <b>Search</b>. Clicking any of these menu items opens the <b>Report Center</b>.</p> <p>The Reports menu items are described below:</p> <ul style="list-style-type: none"> <li>• <b>Library</b> opens the Report Library in the Report Center. In the Library, you can upload reports to the Report server.</li> <li>• <b>My Reports</b> opens the My Reports area of the Report Center, which contains the contents of the application server's My Reports folder. From here you can run, publish and schedule reports. You can also generate Ad Hoc reports using the Ad Hoc Wizard.</li> <li>• <b>Search</b> opens the search engine in the Report Center. You can search for reports using any or all of the criteria listed.</li> </ul> <p>For detail information about using the Report Center, refer to <i>HP Select Audit 1.03 Report Center User's Guide</i>.</p>
Approvals	<p>The <b>Approvals</b> menu is used to view pending approvals assigned to you. See <a href="#">Approving Reports</a> on page 88 for more information about approving reports.</p>
Models	<p>The <b>Models</b> menu has three standard submenus: <b>Overview</b>, <b>Model History</b>, and <b>Manage Models</b>.</p> <ul style="list-style-type: none"> <li>• <b>Overview</b> opens the high-level view of the currently-loaded models.</li> <li>• <b>Model History</b> lets you view detailed model run information chosen by date and time.</li> <li>• <b>Manage Models</b> is used export, load, update and delete models.</li> </ul> <p>See <a href="#">Chapter 5, Models</a> for more information about approving reports.</p>

**Table 2 Administrator Toolbar**

Menu Item	Description
Administration	<p>The <b>Administration</b> menu is used to change configuration settings, view schedules for reports, load report packs, and verify the integrity of data.</p> <p>The Administration menu items are described below:</p> <ul style="list-style-type: none"><li>• <b>Verify Audit Data Integrity</b> opens the <b>Data Verification Configuration</b> screen. In this screen you can specify start and end dates to run data verification.</li><li>• <b>View Report Schedules</b> opens to the <b>Schedules</b> screen, under the <b>Admin</b> menu in the Report Center.</li><li>• <b>Manage Models</b> is used export, load, update and delete models.</li><li>• <b>Configuration</b> opens the <b>Configuration</b> screen. Use this page to change the configuration settings for connectors, data integrity and the report client.</li></ul>
Help	<p>The <b>Help</b> menu is used to access online help for Select Audit. It also contains copyright and version information. Administrators should refer to the <b>Adminstrator Guide</b> menu item.</p>

**Figure 1 Audit Portal Toolbar**



## Workspaces

The lower part of the Portal is divided into three workspaces: **Reports**, **Approvals** and **Models**.

### Reports Workspace

The **Reports** workspace is on the left-hand side of the lower portion of the Audit Portal and provides quick access to commonly-used report features:

- **Library** opens the Library in the Report Center.
- **Select Audit Reports** expands to show a list of the most frequently-used Select Audit reports. When you click on a Select Audit report name, the report opens in a new browser window showing by default the last 7 days worth of audit data.
- **Data Integrity Report** expands to show the most recent run time for the Data Integrity report. It has links to the Data Integrity report, the Data Integrity Data Errors report and the Data Integrity Signature Errors report. See [Chapter 8, Using Reports in Select Audit](#) for more information about the Report Center.

**Figure 2 Report Workspace**



## Approvals Workspace

The **Approvals** workspace is in the center of the lower portion of the Audit Portal. It provides quick access to your pending report approvals. When you click a report name, the report opens in the browser. See [Approving Reports](#) on page 88 for more information about approving reports.

**Figure 3 Approvals Workspace**



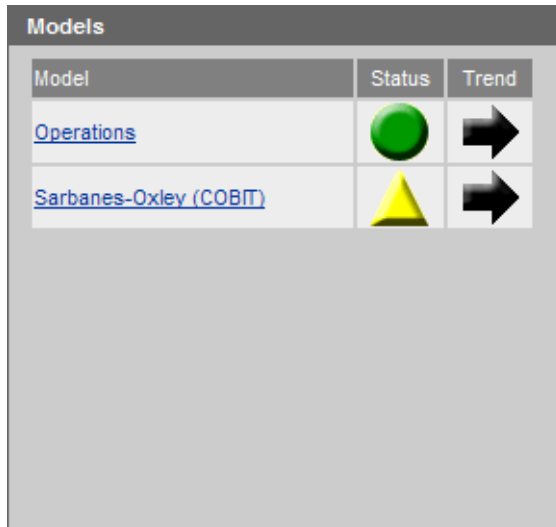
## Models Workspace





The **Models** workspace is on the right-hand side of the lower portion of the Audit Portal. It is displayed differently, depending on the type of user you are. If you are an Administrator, it contains a high-level view of the currently-loaded models, showing the status and trend. See [Chapter 5, Models](#) for more information about Select Audit models.



If the status and trend of the Operations model are updated when the model is run, the changes will be not updated on the Audit Portal Welcome page in the Model workspace unless you log out and log back in to the Audit Portal.

**Figure 4 Models Workspace**



Model	Status	Trend
<a href="#">Operations</a>		
<a href="#">Sarbanes-Oxley (COBIT)</a>		

## Setting the Portal Logout Time

During the Audit Server installation, the session expiry time is set to 20 minutes. You can modify this setting.

### To set the portal logout time in WebLogic

You modify the logout time in WebLogic by modifying the `web.xml` files.

- 1 Unpack the `<SelectAudit_Install_Directory>/dist/auditserver.ear` file and locate the `AuditPortalWeb.war` file.
- 2 Unpack the `AuditPortalWeb.war` file and open the `web.xml` file.
- 3 Change the `<session-timeout>` element in the `web.xml` file to the desired value. For example:

```
<session-config>
<session-timeout>30</session-timeout>
</session-config>
```

- 4 Repack the `AuditPortalWeb.war` and `auditserver.ear` files.
- 5 Redeploy the `SelectAuditServer` application in WebLogic administration console.
- 6 Open the `<SelectAudit_Install_Directory>/dist/reporting/ReportServer/WEB-INF/web.xml` file.
- 7 Repeat [step 3](#).
- 8 Redeploy the `SelectAuditReportServer` web application in the WebLogic administration console.

## To set the portal logout time in WebSphere

You modify the logout time in WebSphere by modifying the `web.xml` files.

- 1 Unpack the `<SelectAudit_Install_Directory>/dist/auditserver.ear` file and locate the `AuditPortalWeb.war` file.
- 2 Unpack the `AuditPortalWeb.war` file and open the `AuditPortalWeb.xml` file.
- 3 Change the `<session-timeout>` element in the `web.xml` file to the desired value. For example:

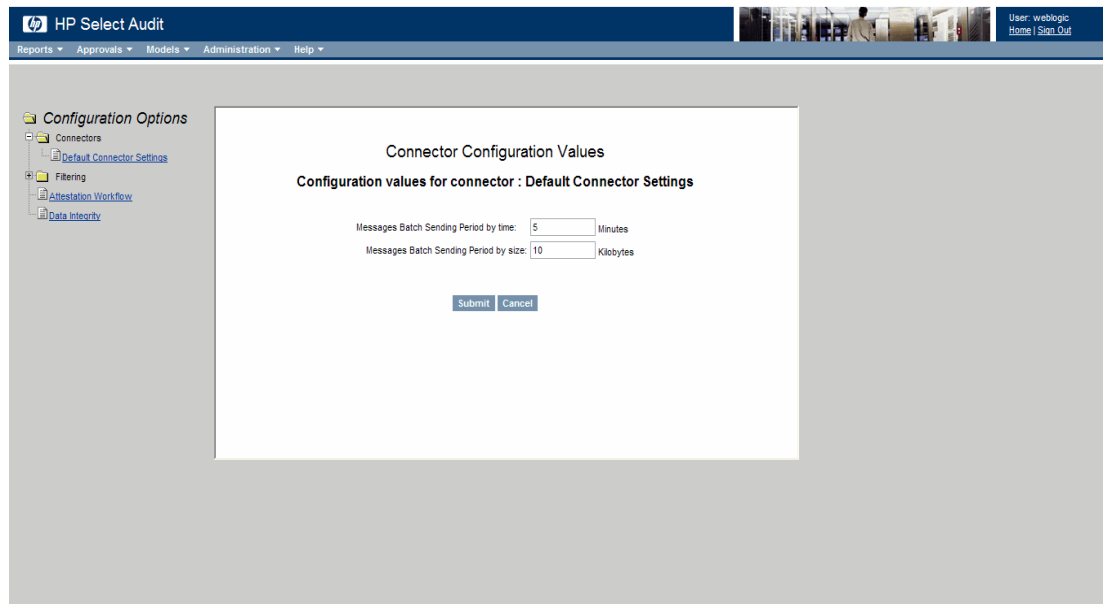
```
<session-config>
<session-timeout>30</session-timeout>
</session-config>
```
- 4 Repack the `AuditPortalWeb.war` and `auditserver.ear` files.
- 5 Update and start the `SelectAuditServer` application in the WebSphere administration console. Use the existing configuration settings for the application during the update process.
- 6 Open the `<SelectAudit_Install_Directory>/dist/reporting/ReportServer.war` and open the `web.xml` file.
- 7 Repeat [step 3](#).
- 8 Repack the `ReportServer.war` file.
- 9 Update and restart the `SelectAuditReportServer` web application in the WebSphere administration console. Use the existing configuration settings for the application during the update process.

## Configuring Audit Connectors

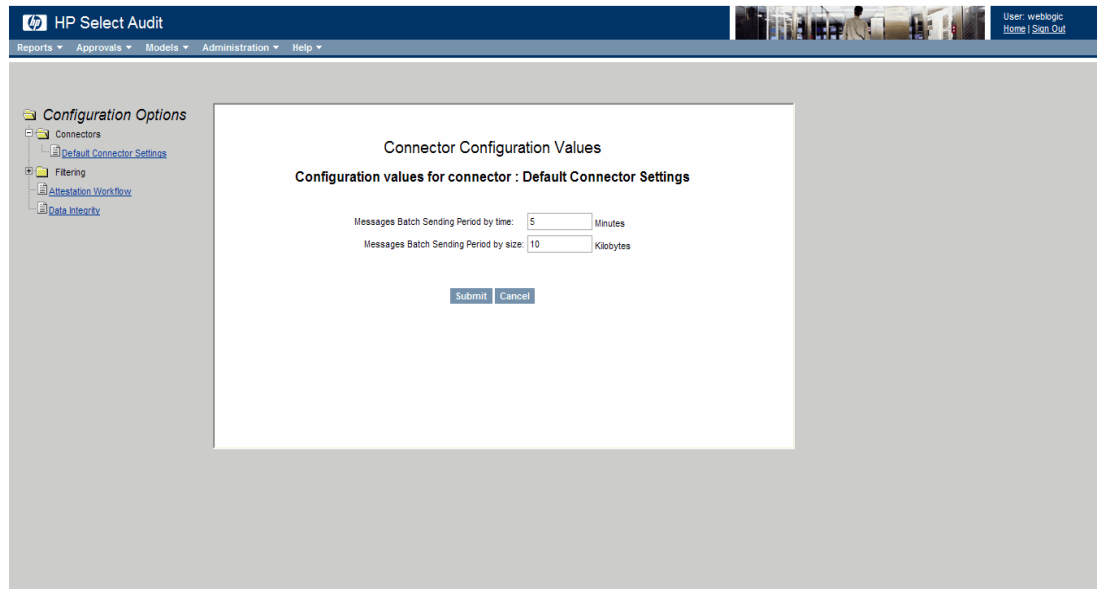
Audit Connectors are deployed on systems running client applications. They collect audit messages from the client applications, temporarily store these messages, and send them to the Audit Server. Connectors are installed using either SSL or Basic Authentication using the Audit Connector installer. See *Installing the Audit Connector* in the *HP Select Audit 1.02 Installation Guide* for more information. You can configure the connectors to specify when rollovers occur using the Audit Portal.

### To configure a connector

- 1 Click **Administration** → **Configuration**. The **Configuration** screen opens.



- 2 Expand the **Connectors** menu item on the left of the **Configuration** screen to see a list of all installed connectors.
  - ▶ You can change the configuration for specific connectors or configure default settings for all your connectors. This guide shows the **Default Connector** screens.
- 3 Click **Default Connector Settings** or one of the installed connectors listed. The **Connector Configuration Values** screen opens.



- 4 Type a time in the **Messages Batch Sending Period by time** field or a batch size in the **Messages Batch Sending Period by size** field to specify when rollovers occur.
- 5 Click **Submit**. The configuration settings are applied.

The `connector.properties` file is updated with the values defined in the **Connector Configuration Values** screen.

▶ The `connector.properties` file is generated when the Audit Configuration server pushes configuration parameters to the connector, after it has been changed on the GUI. These parameters overwrite the values in the `connector.props` file. The `connector.properties` file is updated when you change the connector settings on the **Connector Configuration Values** screen.

⚠ Do not manually edit the `connector.properties` file.

## To manually configure a connector on Linux

For Linux, you can manually configure a connector to run as a user other than `root`.

- 1 Create a new group `saud`. Then, create a new user `saud` using the shell `/sbin/nologin` belonging to group `saud`. Ensure that user `saud` has a non-empty password.

This ensures that if that shell ever gets changed (or if some other shell is used instead of `/bin/nologin`) that logging in as user `saud` cannot occur without specifying a password.

- 2 Stop the connector as follows:

```
/opt/HP/SelectAudit/connector/SAudConn stop
```

- 3 Using the following command, change the ownership and group ownership of the connector installation directory and its content to user `saud` and group `saud`. The default installation directory is `/opt/HP/SelectAudit/connector`.

```
chown -R saud:saud /opt/HP/SelectAudit/connector
```

- 4 Change the ownership of `/var/run/SAudConnector` to user `saud` and group `saud` as follows:

```
chown -R saud:saud /var/run/SAudConnector
```

- 5 In `SAudConn`, modify the line `USER="root"` to `USER="saud"`.

- 6 Test the connector by running (as `root`) `/etc/init.d/SAudConn start`.

This starts the connector running as user `saud`.

## Correlating Users Between Applications

Not every installation of every product uses the same identifier for the same user. For example, Select Identity uses a unique user ID, while Select Access uses the LDAP DN. In a complex deployment there may be a combination of users that have different account names on different systems and different systems where the same account name refers to different people. To handle this, Select Audit provides a User Correlation feature that allows you to easily audit users across applications that use different identities. Select Audit defines a table called `GlobalUsers` that is used to map the user application identities to a single identity that can be shown in the audit reports. The `GlobalUsers` table contains the following four columns:

- A unique ID that is the primary key.
- A column called `GUID` for the global user ID.
- A column called `APPID` that specifies the application name.

- A column called `USERNAME` that specifies the application specific user ID.

For example, if a user has a user ID of `john doe` in `Select Identity` and `dn=jdoe` in `Select Access`, the mapping in the `GlobalUsers` table will be:

GUID	APPID	USERNAME
john doe	SelectIdentity	john doe
john doe	SelectAccess	dn=jdoe

If the `GUID` column has a value, the reports will pick up and show this value. If not, the reports will show the application-specific user ID that is read from the `Fact` tables and stored at the time the message was normalized. Refer to *HP Select Audit 1.03 Concepts Guide* for more information about `Audit Facts` and `Fact` tables.

In the case of messages with more than one user ID (for example, when an administrator changes a user's properties), both IDs are mapped.

The `GlobalUsers` table is initially populated and maintained by the customer. You can populate the `GlobalUsers` table using `SQL` statements.

## Enabling/Disabling User Correlation

You can turn user correlation on or off. Use one of the following procedures for your specific database type



By default, the user correlation feature is disabled.

## Oracle

Use the following procedures to enable and disable user correlation on Oracle.

### To enable user correlation on Oracle

- 1 Populate the table `GlobalUsers`.
  - ▶ Make sure the exact values of the `USERNAME` are inserted into the table, with no leading or trailing spaces. Spaces will prevent finding the user name in the table.
- 2 Open up a `SQLPlus` session.
- 3 Turn on user correlation by typing the following into your `SQLPlus` terminal:
 

```
set serveroutput on;
exec enableUserCorrelation('on');
```

### To disable user correlation on Oracle

- 1 Open up a `SQLPlus` session.
- 2 Turn off user correlation by typing the following into your `SQLPlus` terminal:
 

```
set serveroutput on;
exec enableUserCorrelation('off');
```



## MSSQL

Use the following procedures to enable and disable user correlation on MSSQL.

### To enable user correlation on MSSQL

- 1 Populate the `GlobalUsers` table.
  - ▶ Make sure the exact values of the `USERNAME` are inserted into the table, with no leading or trailing spaces. Spaces will prevent finding the user name in the table.
- 2 Open up SQL Server Query Analyzer.
- 3 Connect to the database housing the audit data.
- 4 Turn on user correlation by executing the following SQL command:

```
exec enableUserCorrelation 'on'
```

### To disable user correlation on MSSQL

- 1 Open up SQL Server Query Analyzer.
- 2 Connect to the database housing the audit data.
- 3 Turn off user correlation by typing the following SQL command:

```
exec enableUserCorrelation 'off'
```

## Configuring a Mail Session

During installation, **Mail Server** and **Sender Address (Workflow)** entries are stored in `<install_dir>/dist/config/properties/workflow.properties` as:

```
mail.smtp.host=[host-name]
mail.from=[sender-address]
```

If you did not specify a workflow sender addresses on the **Application Configuration** screen of the Audit Server installer, an invalid **Sender** address may be rejected by your SMTP server which will lead to a workflow email notification failure. To change the SMTP server and/or the **Sender** address, update these entries manually and restart the application server.

Also, open

```
<install_dir>/dist/reporting/ReportServer/WEB-INF/conf/scopeserver.xml
```

and update the `<Mail>` section as follows:

```
<Mail>
  <Server>[host-name]</Server>
  <Protocol>smtp</Protocol>
  <Port>25</Port>
  <SenderAddress>[sender-address]</SenderAddress>
</Mail>
```

## Configuring Log4j

When the Select Audit Server is installed, `<install_dir>/dist/config/properties/log4j.properties` is installed on the classpath. It is essential that this properties file is used, otherwise Report server events will not be logged to the Audit Server.



In WebSphere, an additional file, `commons-logging.properties`, is also installed.

If you have an existing `log4j.properties` or `log4j.xml` file in use, merge the two files together. You may specify only one `log4j` configuration file per JVM.

## Enabling Logging

The default setting for all loggers is `WARN`, except for the custom `SA_AUDITOR` loggers, which should remain set to `INFO`. To enable logging to the Console or a file, change the appropriate logger from `ERROR` to one of the following, depending on how much output is desired:

- `DEBUG`
- `INFO`
- `WARN`
- `FATAL`

For more information on configuring `log4j` loggers, see the `log4j` manual at <http://logging.apache.org/log4j/docs/manual.html>.

## Setting Appenders

`log4j.rootCategory` defines the default log behavior for any loggers that are not explicitly defined otherwise. It is set to use both the `MAIN` file appender, which writes to `sa.log`, and the `CONSOLE` appender, which writes out to the Console. All other loggers are descendents of this logger and can be configured to give output from specific modules of the application.

At the end of the `LOGGERS` section, there are a series of loggers that log to the `SA_AUDITOR` appender. These loggers should not be edited. They are used to send audit logs from the Report server to the Audit Server so that they can be recorded and viewed in reports.

In the `APPENDERS` section, there are a series of file appenders. For each file appender, there is an option to configure the output file created, the maximum file size before rollover occurs, and the number of files to keep on disk, for example, keep only the last 10 files rolled over, at 2MB per file.

Once changes have been made to the `log4j.properties` file, the server should be restarted for the changes to take effect.

## log4j.properties File

The `log4j.properties` file is shown below:

```
##### LOGGERS #####
```

```

# Root Logger
log4j.rootLogger=WARN, MAIN, CONSOLE

# HP App Log Level - Select Audit log messages
log4j.logger.com.hp.ov=WARN
log4j.logger.com.hp.ov.selectaudit.auditserver.common.analysis=INFO

# Spring Log Level - for normalizer SQL output
log4j.logger.org.springframework=WARN

# Workflow Manager Logger - make a separate log containing a duplicate
copy of only workflow messages
# log4j.logger.com.hp.ov.selectaudit.workflow.manager=WARN, WORKFLOW

# Report Server loggers
log4j.logger.com.panscopic=ERROR, CONSOLE, SERVER-FILE
log4j.logger.SQL=ERROR, SQL-FILE
log4j.logger.PERFORMANCE=ERROR, PERFORMANCE-FILE
log4j.logger.com.panscopic.scopeserver.renderer.FOPRenderer=ERROR
log4j.logger.org.apache.struts=WARN

# Report Server filtering loggers
#!!!! WARNING, DO NOT SET THIS TO DEBUG, OTHERWISE THE USER'S PASSWORD
WILL BE LOGGED.
log4j.logger.com.panscopic.security.auth=INFO, FILTERING-FILE
log4j.logger.com.panscopic.directory=INFO, FILTERING-FILE
log4j.logger.com.hp.ov.selectaudit.report.security=INFO, FILTERING-FILE

# These loggers log to the Select Audit Server - do not disable
log4j.logger.AUDITRDLEXECUTION=INFO, SA_AUDITOR
log4j.logger.AUDITJREXECUTION=INFO, SA_AUDITOR
log4j.logger.AUDITREPOSITORY=INFO, SA_AUDITOR
log4j.logger.AUDITSCHEDULING=INFO, SA_AUDITOR
log4j.logger.AUDITCONFIGURATION=INFO, SA_AUDITOR

# set logger additivity to false so INFO level output will not display on
# CONSOLE and sa.log
log4j.additivity.AUDITRDLEXECUTION=false

```

```

log4j.additivity.AUDITJREXECUTION=false
log4j.additivity.AUDITREPOSITORY=false
log4j.additivity.AUDITSCHEDULING=false
log4j.additivity.AUDITCONFIGURATION=false

log4j.additivity.com.panscopic.security.auth=false
log4j.additivity.com.panscopic.directory=false
log4j.additivity.com.hp.ov.selectaudit.report.security=false

##### APPENDERS #####

# CONSOLE appender writes to a console
log4j.appender.CONSOLE=org.apache.log4j.ConsoleAppender
log4j.appender.CONSOLE.layout=org.apache.log4j.PatternLayout
log4j.appender.CONSOLE.layout.ConversionPattern=%d %5p (%F:%L) - %m%n

# MAIN appender writes all output to a file [sa.log]
log4j.appender.MAIN=org.apache.log4j.RollingFileAppender
log4j.appender.MAIN.File=C:/Program Files/HP Software/Select Audit/
auditserver/log/sa.log
log4j.appender.MAIN.MaxFileSize=2MB
log4j.appender.MAIN.MaxBackupIndex=10
log4j.appender.MAIN.layout=org.apache.log4j.PatternLayout
log4j.appender.MAIN.layout.ConversionPattern=%d %5p (%F:%L) - %m%n

# WORKFLOW - appender writes workflow messages to a file [wf.log]
log4j.appender.WORKFLOW=org.apache.log4j.RollingFileAppender
log4j.appender.WORKFLOW.File=C:/Program Files/HP Software/Select Audit/
auditserver/log/wf.log
log4j.appender.WORKFLOW.MaxFileSize=2MB
log4j.appender.WORKFLOW.MaxBackupIndex=10
log4j.appender.WORKFLOW.layout=org.apache.log4j.PatternLayout
log4j.appender.WORKFLOW.layout.ConversionPattern=%d %5p (%F:%L) - %m%n

# SERVER-FILE - appender writes report messages to a file
log4j.appender.SERVER-FILE=org.apache.log4j.RollingFileAppender

```

```

log4j.appender.SERVER-FILE.File=C:/Program Files/HP Software/Select
Audit/auditserver/dist/reporting/ReportServer/WEB-INF/logs/
ScopeServerLog.txt

log4j.appender.SERVER-FILE.MaxFileSize=1MB

log4j.appender.SERVER-FILE.MaxBackupIndex=10

log4j.appender.SERVER-FILE.layout=org.apache.log4j.PatternLayout
log4j.appender.SERVER-FILE.layout.ConversionPattern=%d [%x] %-5p %c{1}:
%m %n

# SQL-FILE - appender writes report execution SQL strings to a file
log4j.appender.SQL-FILE=org.apache.log4j.RollingFileAppender
log4j.appender.SQL-FILE.File=C:/Program Files/HP Software/Select Audit/
auditserver/dist/reporting/ReportServer/WEB-INF/logs/SQLLog.txt
log4j.appender.SQL-FILE.MaxFileSize=1MB
log4j.appender.SQL-FILE.MaxBackupIndex=10
log4j.appender.SQL-FILE.layout=org.apache.log4j.PatternLayout
log4j.appender.SQL-FILE.layout.ConversionPattern="%d [%x] %-5p %c{2}: %m
%n

# PERFORMANCE-FILE - appender writes report server performance stats to a
file
log4j.appender.PERFORMANCE-FILE=org.apache.log4j.RollingFileAppender
log4j.appender.PERFORMANCE-FILE.File=C:/Program Files/HP Software/Select
Audit/auditserver/dist/reporting/ReportServer/WEB-INF/logs/
PerformanceLog.txt
log4j.appender.PERFORMANCE-FILE.MaxFileSize=1MB
log4j.appender.PERFORMANCE-FILE.MaxBackupIndex=10
log4j.appender.PERFORMANCE-FILE.layout=org.apache.log4j.PatternLayout
log4j.appender.PERFORMANCE-FILE.layout.ConversionPattern=%d %m%n

# FILTERING-FILE - appender writes report server filtering stats to a
file
log4j.appender.FILTERING-FILE=org.apache.log4j.RollingFileAppender
log4j.appender.FILTERING-FILE.File=C:/Program Files/HP Software/Select
Audit/auditserver/dist/reporting/ReportServer/WEB-INF/logs/FilterLog.txt
log4j.appender.FILTERING-FILE.MaxFileSize=1MB
log4j.appender.FILTERING-FILE.MaxBackupIndex=10
log4j.appender.FILTERING-FILE.layout=org.apache.log4j.PatternLayout
log4j.appender.FILTERING-FILE.layout.ConversionPattern=%d %5p %c{2} -
%m%n

```

```
# SA_AUDITOR - logs report server messages to select audit server
log4j.appender.SA_AUDITOR=com.hp.ov.selectaudit.log.report.SAudAppender
log4j.appender.SA_AUDITOR.layout=org.apache.log4j.PatternLayout
log4j.appender.SA_AUDITOR.layout.ConversionPattern=%m%n
```

## Globally Configuring the Select Audit Administrator Password

The Administrator Password Tool is used to change the Administrator password. If the Select Audit Administrator password is changed after Select Audit is installed, all the Administrator password entries must be updated, otherwise, Select Audit will not work properly. For the Audit Server, the Administrator password must be changed in the following XML files:

- `AUDIT_HOME/config/audit_config.xml`
- `AUDIT_HOME/reporting/ReportServer/WEB-INF/conf/directory.xml`
- `AUDIT_HOME/reporting/ReportServer/WEB-INF/conf/scopeserver.xml`

You must change the Audit Connector password configuration by editing the `connector.props` file. Select Audit includes a component that enables you to change all Select Audit Administrator password entries at once.

### Administrator Password Tool

The Administrator Password Tool contains the following files:

- `adminpwd.jar`
- `scopeserver.jar`
- `log4j-1.2.9.jar`
- `adminpwd.bat` (Windows) or `adminpwd.sh` (UNIX)
- `xercesImpl.jar`
- `xmlParserAPIs.jar`

The scripts `adminpwd.bat` and `adminpwd.sh` are used to run the Administrator Password Tool.

### To run the Administrator Password Tool

Use the following steps to the Administrator password.

- 1 Make sure your `jdk1.4.2` is “visible” by typing `java` in the command line. If Java is not found, add the `jdk1.4.2 bin` directory to the system `PATH`.

- 2 Check the Java version:

```
java -version
```

The version should be `1.4.2`. The Administrator Password tool may not work properly if using an incorrect Java version.

- 3 Run the `adminpwd` shell (batch) script.

**On Windows:**

- a Run `adminpwd -s` to change the Audit Server password files.
- b Run `adminpwd -c` to change the Audit Connector password file.

**On Linux, Solaris, and HP-UX:**

- a Run `./adminpwd.sh -s` to change the Audit Server password files.
  - b Run `./adminpwd.sh -c` to change the Audit Connector password file.
- 4 Follow the screen prompts. The following message is shown when the password configuration successfully completed.  

```
Password has been successfully changed.
```
  - 5 After using the Administrator Password Tool to change the Administrator password in the Select Audit configuration files, change the Administrator password in the application server's LDAP user store (embedded or external).
  - 6 Restart all servers to which Select Audit is deployed.





## 3 Select Identity Integration

Select Audit is designed so that you can control who is allowed to view which report. For Select Identity integration, Select Audit applies the same access control rules that are defined in Select Identity and uses J2EE authentication to authenticate Select Identity users.



Select Identity has specific configuration requirements in order to log to Select Audit. Unless it is configured properly, Select Identity will not log to Select Audit. Refer to the *HP Select Identity* documentation for more information about configuring Select Identity.

This chapter contains the following topics:

- [Select Identity Permissions](#) on page 33
- [Select Audit Report Access Control](#) on page 35
- [Select Identity and J2EE Integration](#) on page 39
- [Filtering with Select Identity](#) on page 40
- [Configuring Select Identity](#) on page 40

### Select Identity Permissions

Select Identity has two report types: audit reports and configuration reports. An administrator can view reports based on his or her role permission settings. When Select Audit integrates with Select Identity, the same permission policies defined in Select Identity are applied in Select Audit.

#### The Select Audit Administrator and Select Audit Auditor Roles

Select Audit Administrators and Select Audit Auditors are special users in Select Audit who can view all the reports and all the events. Members of these roles have access to all the reports and events in Select Audit. For both Select Audit Administrators and Auditors, Select Audit does not contact Select Identity for permission policies.

#### Report Permission Mapping

When an administrator is granted permission to view a certain report type in Select Identity, the administrator is allowed to view, modify, run and schedule the report. If the same kind of report exists in Select Audit, the administrator is given the same permissions for the Select Audit report. If a corresponding report does not exist in Select Audit, the events in the report type are used and the administrator is given the same permissions for the Select Audit events as for the Select Identity events.

## Select Identity Permission Policies

Select Identity uses the following three permission policies to implement data filtering:

- Report Type permissions.
- Services and Contexts permissions.
- User Management permissions.

### Report Type Permissions

Report Type permissions control who is allowed to view what types of reports. Because a report contains certain types of events, the Report Type permission also determines who is allowed to view what event types.

### Services and Contexts Permissions

A Select Identity administrator is allowed to manage certain services and contexts (including context attribute names and context attribute values).

There are five types of management an administrator can perform:

- All services and all contexts.
- All services, certain context attributes and all attribute values.
- All services, certain context attributes and certain attribute values.
- Certain services (thus certain context attributes because one service has only one context attribute) and all context attribute values.
- Certain services and certain context attribute values.

### User Management Permissions

In Select Identity, a user is a member of a service if one of the user's attribute values is equal to the service's context attribute value. A user can be managed by an administrator if the user is a member of one of the administrator's managed services.

If a Select Audit report is user activity-related, the event records are filtered according to the user management permission (an administrator can only see his or her managed user's event records).

## Select Identity Permission Data

When an administrator logs in to Select Audit, Select Identity is contacted to ask for the permission data of this administrator.

There are three types of permission data required:

- The granted report types.
- The managed service/context list.
- The managed users.

The Select Identity Web Services API returns the granted report types and the managed service and context list. The Web Services API authenticates Select Audit as a special administrator in Select Identity and passes the log-on administrator's ID to Select Identity to fetch the administrator's data. A database connection is opened to the Select Identity database to fetch the managed user list.

- ▶ When integrating with Select Identity, the Select Audit logon ID must be the same as the administrator ID used in Select Identity.

If the Select Identity server or database is down, or a log-on user is not found in Select Identity, Select Audit does not allow the user to access data covered by Select Identity permissions.

## Storing and Refreshing the Permission Data

When the administrator first logs in to the Report server, Select Audit contacts Select Identity to load the permission data. The loaded permission data is stored into the local database tables. The JDBC Proxy filters the data by joining the relevant Fact tables with the relevant permission tables. The permission table is refreshed upon the administrator's next logon.

- ▶ Only the data for the currently logged in administrator is refreshed, not the entire table.

Each administrator's permission data is identified by the `GUID` in the permission tables. When integrating with Select Identity, the `GUID` in the `GLOBALUSER` correlation table must be the same administrator ID used in Select Identity. In the same way, the user IDs returned in the permission data are the same IDs in the audit events.

## Select Audit Report Access Control

Reports that can be viewed by users can be filtered based on Select Identity access controls, defined in Select Identity. There are two levels of access control in Select Audit.

- Report Level Control
- Row Level Control

### Report Level Control

Report Level Control determines which reports are shown on an administrator's dashboard. There are four scenarios for the Report Level permission mapping.

- Select Audit reports which have a counterpart in Select Identity. For example, the User Summary Report in Select Audit is equivalent to the Audit User Summary Report in Select Identity. In this case, an administrator will have the same permissions for the Select Audit Report as for the Select Identity Report.
- Select Audit reports which consolidate the events of more than one Select Identity report into one report. For example, the Account Change Report covers events across several Select Identity reports (User Creation, User Deletion, User Termination, User Password and User Hint). If an administrator is granted permission to ANY of the Select Identity reports listed above, then the corresponding Select Audit report is shown on the dashboard. When the administrator looks at the report content, Row Level Control filters out the unused events.

- Select Audit reports which have no related report in Select Identity, such as the Attestation Report and the Raw Audit Message Report. By default, all users have “full” permissions for these reports. Administrators can change the permissions for these reports in the Report Center.
- Select Identity reports which have no related Select Audit reports, for example, some Select Identity configuration reports. The Select Identity report permissions associated with such reports have no effect on any Select Audit reports.

## Row Level Control

Row Level Control determines which audit events are listed inside a report. There are two kinds of audit events:

- Select Audit events that can be identified by Select Identity report types, for example, UserAdd, UserChange and UserDelete. The permissions for these reports will have the same affect on the audit events.

Some audit events may be contained in more than one report. For example, the UserAdd event is in the Audit User report and the Audit User Creation report. The permission for those events is the “most permissive” of all the report permissions. In this case, if an administrator is allowed to view Audit User reports but is denied viewing Audit User Creation reports, the administrator is still allowed to view UserAdd events in Select Audit.

- Audit events that cannot be identified by Select Identity reports, for example, some federation events. By default, the administrator is allowed to view those events.

See [Report Access](#) on page 37 for information about how Select Identity report types correspond to events in Select Audit.

## Report Access

The following table shows what reports are viewed with J2EE and Select Identity, and Select Access and Select Identity integrations:

**Table 3 Select Identity and J2EE or Select Access Report Access**

	Users			Administrators	Auditors
	Select Identity User	Non-Select Identity User	Select Identity is unavailable		
Account Change Report	If the user is allowed access in Select Identity to certain report types, the user will have the following permissions on related reports: <ul style="list-style-type: none"> <li>• Read</li> <li>• Execute</li> <li>• Schedule</li> <li>• Ad Hoc</li> </ul>	Denied	Denied	Full permissions including: <ul style="list-style-type: none"> <li>• Read</li> <li>• Write</li> <li>• Delete</li> <li>• Execute</li> <li>• Schedule</li> <li>• Ad Hoc</li> <li>• View permissions</li> <li>• Grant permissions</li> <li>• Revoke permissions</li> </ul>	Read Execute Schedule Ad Hoc
Account Events Report					
Administrator Report					
Change History Report					
Configuration Report					
Password Management Report					
Security Events Report					
Service Report					
System Activity Report					
User Activity Report					
User Summary Report					
Workflow Events Report					
Attestation Report					
Data Integrity Report	Read, Execute, Schedule, Ad Hoc				
Raw Message Report	Denied				

Table 4 lists the Select Identity report types needed to view Select Audit reports.

**Table 4 Select Audit Report Access**

Select Audit Report	You need access to ANY of these report types in Select Identity
Account Change Report	AuditUser
	AuditUserCreation
	AuditUserDeletion
	AuditUserLogin
	AuditUserPassword
	AuditUserTermination
Account Events Report	AuditUser
	AuditUserDeletion
	AuditUserLogin
	AuditUserPassword
Administrator Report	AdminConfiguration
	AuditService
	AuditUser
	AuditUserCreation
	AuditUserDeletion
	AuditUserHint
	AuditUserLogin
	AuditUserPassword
	AuditUserTermination
Change History Report	AdminConfiguration
	AuditService
	AuditUser
	AuditUserCreation
	AuditUserDeletion
	AuditUserLogin
	AuditUserPassword
	AuditUserTermination
Configuration Report	AdminConfiguration

**Table 4 Select Audit Report Access (cont'd)**

Select Audit Report	You need access to ANY of these report types in Select Identity
Password Management Report	AuditUser
	AuditUserLogin
	AuditUserPassword
Security Events Report	AuditUser
	AuditUserLogin
	AuditUserPassword
Service Report	AuditService
System Activity Report	<i>Any report types</i>
User Activity Report	<i>Any report types</i>
User Summary Report	AuditUserSummary
Workflow Events Report	AdminConfiguration
	AuditService
	AuditUser
	AuditUserCreation
	AuditUserDeletion
	AuditUserLogin
	AuditUserPassword
	AuditUserTermination

## Select Identity and J2EE Integration

Authentication and the storage of users and roles is done through LDAP. Select Audit comes with support for three roles:

- Select Audit User
- Select Audit Administrator
- Select Audit Auditor (Users who are Select Audit Administrators or Select Audit Auditors are allowed to view all the reports.)

To integrate with Select Identity, roles are defined in Select Audit that represent a report type in Select Identity. Select Audit has pre-defined access rules for each role. Users who are Select Audit Administrators or Select Audit Auditors have access to view all reports. An Administrator who is granted a report type in Select Identity will be a member of the corresponding role in Select Audit.



You must add Select Identity users to the LDAP repository being used by the application server.

When a user logs in, Select Audit contacts Select Identity to load the report type permissions for that user and assigns the user into the corresponding roles. Subsequently, the Report Center enforces the pre-defined access rules for the user, based on his or her role membership.

If a user is granted permission for more than one report type, the user will belong to multiple report roles. The final permission granted is the most permissive permission of all the roles.

### The SiDirectoryProvider

User permission settings are loaded from Select Identity and the report role memberships are assigned in the SiDirectoryProvider. The SiDirectoryProvider creates the report type roles the first time it runs.

## Filtering with Select Identity

If you are using Select Audit with Select Identity, you must configure filtering options to enable integration with Select Identity. See [Configuring Select Identity](#) on page 40 for more information.

If you enable the "Filtering with Select Identity" option, the permissions to view various reports is controlled by Select Identity. You should have Select Identity installed on a separate application server for integration.

## Configuring Select Identity

When Select Audit integrates with Select Identity, the same permission policy defined in Select Identity is applied in Select Audit. Filtering uses the user's identity to filter out only the data that the user is able to view, determining which reports the user can access in Select Audit.



Select Identity has specific configuration requirements in order to log to Select Audit. Unless it is configured properly, Select Identity will not log to Select Audit. Refer to the *HP Select Identity* documentation for more information about configuring Select Identity.

During installation, if the Select Identity filtering option is enabled, the Audit Server installer performs the following tasks relevant to Select Identity filtering:

- It specifies an authenticator in the application server.
- It configures an LDAP directory provider in the Report Center Administration console.

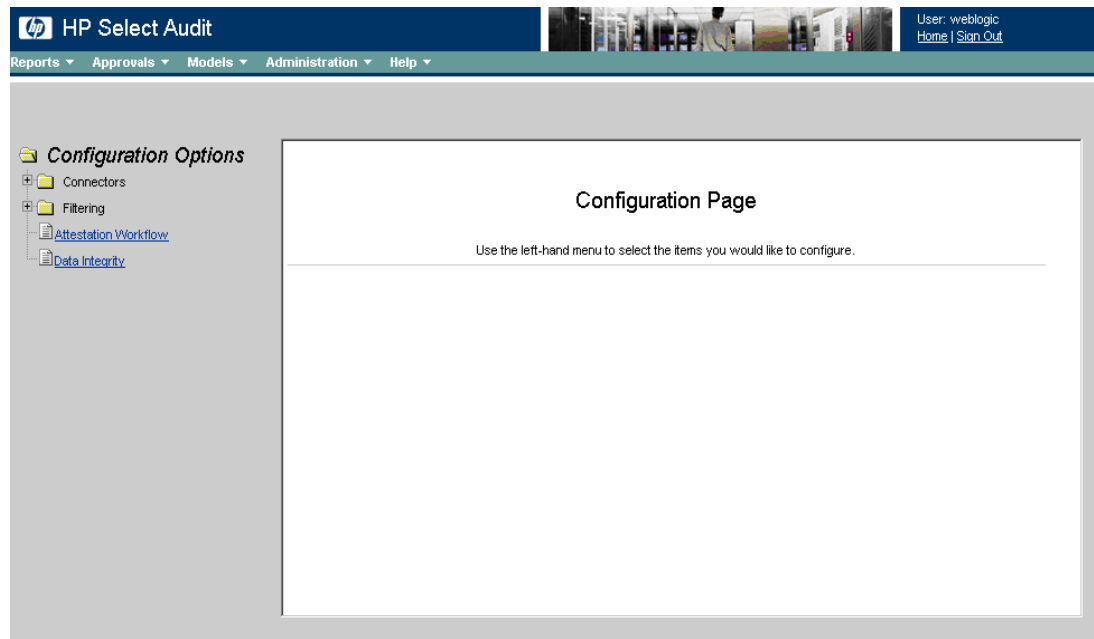


- It creates default users and roles defined in the LDAP repository used by the application server.
  - ▶ The administrator can add new users/roles later where appropriate.
- It deploys access rules defined in the Report Center.
- It creates a JDBC datasource for connecting to the Select Identity database.
- It enables the option to filter with Select Identity.

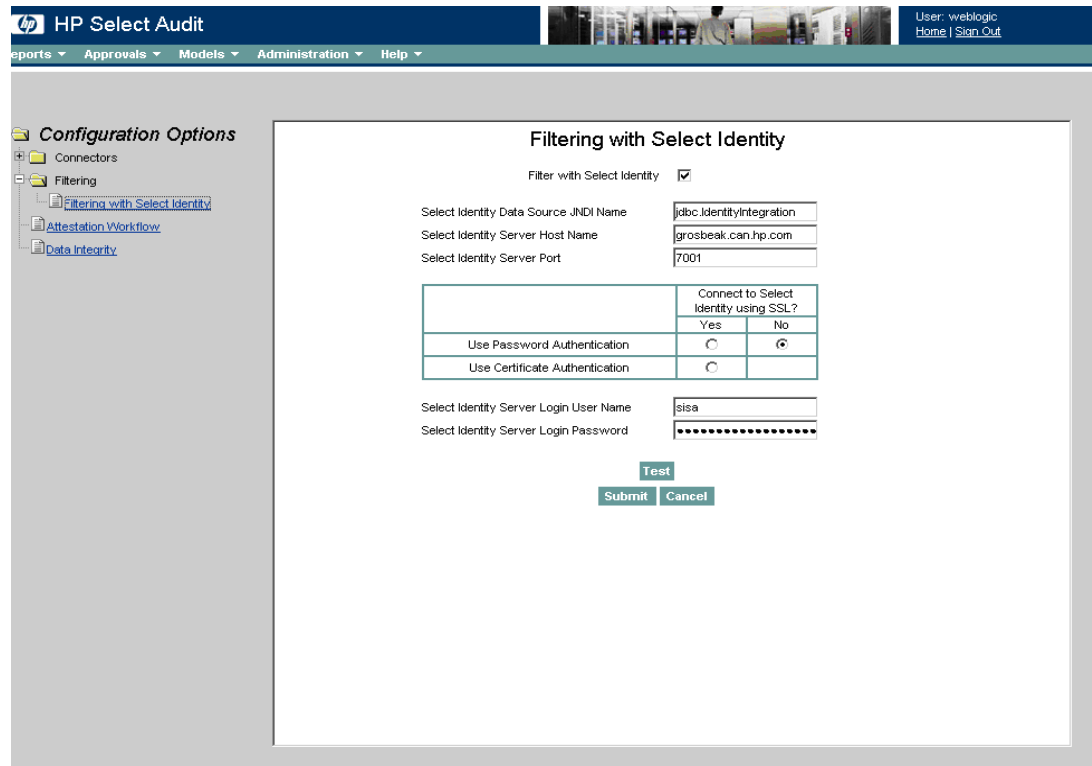
After installation, you can configure the filtering options using the Audit Portal. For details, see [To configure Select Identity filtering](#). To modify the Select Identity database information, use the WebLogic Administration console. See [Modifying Select Identity Database Information](#) for details. If Select Identity is not enabled at install time, the datasource for accessing the Select Identity database has to be added before filtering is enabled on the portal.

## To configure Select Identity filtering

- 1 Select **Administration** → **Configuration**. The Configuration screen opens.



- 2 Expand the **Filtering** folder and click **Filtering with Select Identity**. The **Filtering with Select Identity** screen opens.



- 3 Select the **Filter with Select Identity** check box to enable the screen fields.
- 4 Complete the **Filtering with Select Identity** screen as follows:
  - Enter the **Select Identity Data Source JNDI Name**. See section [Modifying Select Identity Database Information](#) and [Creating New Select Identity Database Information](#) for more details.
  - Enter the **Select Identity Server Host Name**.
  - Enter the **Select Identity Server Port** number.
- 5 There are three options determining the way Select Audit communicates with Select Identity and performs mutual authentication. Make sure the option you choose matches the settings in Select Identity.
  - a User Name and Password with SSL disabled. Select the radio button as shown below for this option. You will have to enter the user name and password to be used for authentication with SI.

	Connect to Select Identity using SSL?	
	Yes	No
Use Password Authentication	<input type="radio"/>	<input checked="" type="radio"/>
Use Certificate Authentication	<input type="radio"/>	<input type="radio"/>

Select Identity Server Login User Name

Select Identity Server Login Password

- b User Name and Password with SSL enabled. Select the radio button as shown below for this option.

	Connect to Select Identity using SSL?	
	Yes	No
Use Password Authentication	<input checked="" type="radio"/>	<input type="radio"/>
Use Certificate Authentication	<input type="radio"/>	<input type="radio"/>

Select Identity Server Login User Name

Select Identity Server Login Password

Trust Keystore Location

Trust Keystore Type

Trust Keystore Password

Enable Certificate Revocation List Validation

CRL refresh every  days

You will have to enter the user name and password to be used for authentication with SI. In addition, you must enter the following information to be used for enabling SSL:

**Trust Keystore Location:** The location of the file (along with the file name) containing the certificate to be used for enabling SSL. This certificate is used to verify the Select Identity server's certificate. Either the Select Identity server certificate itself or the certificate's signer certificate must be in the trust keystore.

**Trust Keystore Type:** Such as JKS or PKCS.

**Trust Keystore Password:** The password for reading from the file entered in **Trust Keystore Location**.

**Enable Certificate Revocation List Validation:** Check this to enable CRL validation.

**CRL refresh every \_\_\_ days:** Specifies your CRL refresh frequency if CRL validation is enabled. If this interval is set to zero, the CRL list will not be cached and will be loaded every time CRL verification is needed.

- c Certificate Authentication with SSL enabled. Select the radio button as shown below for this option.

	Connect to Select Identity using SSL?	
	Yes	No
Use Password Authentication	<input type="radio"/>	<input type="radio"/>
Use Certificate Authentication	<input checked="" type="radio"/>	<input type="radio"/>

Keystore Location

Keystore Type

Keystore Password

Key Password

Trust Keystore Location

Trust Keystore Type

Trust Keystore Password

Enable Certificate Revocation List Validation

CRL refresh every  days

**Test**

**Submit** **Cancel**

If this option is selected, a user certificate is used to authenticate with SI in place of user name and password. In addition to all the information entered in option (b) above, you must enter the following information:

**Keystore Location:** The location of the file (along with the file name) containing the certificate to be used for authentication.

**Keystore Type:** Such as JKS or PKCS.

**Keystore Password:** The password for reading from the file entered in **Keystore Location**.

**Key Password:** The password to protect the private key of the certificate.

The keystore should contain only one private key that represents the client.

For details on Select Identity Authentication, see “Select Audit Authentication Options” in the *HP Select Audit 1.02 Installation Guide*.

- 6 Click **Test** to ensure the Select Identity Integration setup is valid and that both the Select Identity server and Select Identity database can be contacted by the Audit Server.
- 7 Click **Submit**. The field entries are validated, the configuration values are committed to the database tables, and the report server is restarted. If the Report Server restart was successful, the message "Changes successfully applied" is shown at the top of the Select Identity Integration screen.

## Modifying Select Identity Database Information

After you have installed Select Audit and enabled Select Identity integration in the installation, you may need to modify the Select Identity database information. These tasks can be performed using the application server console.

- 1 Log on to WebLogic as the administrator.
- 2 In the Domain Structure tree, select **Services** → **JDBC** → **Data Sources**. The **Summary of JDBC Sources** screen opens.

**WEBLOGIC SERVER**  
ADMINISTRATION CONSOLE

Welcome, weblogic Connected to: base\_domain Home Log Out Preferences Help

Home > Summary of JDBC Data Sources

**Summary of JDBC Data Sources**

A JDBC data source is an object bound to the JNDI tree that provides database connectivity through a pool of JDBC connections. Applications can look up a data source on the JNDI tree and then borrow a database connection from a data source.

This page summarizes the JDBC data source objects that have been created in this domain.

Customize this table

**Data Sources**

Click the *Lock & Edit* button in the Change Center to activate all the buttons on this page.

New Delete Showing 1 - 5 of 5 Previous Next

Name	JNDI Name	Targets
SelectAuditDataSource	jdbc/SelectAudit	AdminServer
SelectAuditProxyDataSource	jdbcproxy/SAudDataSource	AdminServer
SelectAuditReportDataSource	jdbc/SAudDataSource	AdminServer
SelectAuditWorkflowDataSource	jdbc/TruAccess	AdminServer
SelectIdentityIntegrationDataSource	jdbc/IdentityIntegration	AdminServer

New Delete Showing 1 - 5 of 5 Previous Next

- 3 Click **Lock & Edit** to enable data entry.
- 4 Click the JDBC data source name **SelectIdentityIntegrationDataSource**. The **Settings for SelectIdentityIntegrationDataSource** screen opens.

**Settings for SelectIdentityIntegrationDataSource**

Configuration Targets Monitoring Control Security Notes

General Connection Pool Transaction Diagnostics Identity Options

Save

Applications get a database connection from a data source by looking up the data source on the (JNDI) tree and then requesting a connection. The data source provides the connection to the ap connections.

This page enables you to define general configuration options for this JDBC data source.

**Name:** SelectIdentityIntegrationDataSource A uni  
sourc

**JNDI Name:** jdbc.IdentityIntegration The :  
bound  
name

**Row Prefetch Enabled** Enab  
"prefi  
the c

**Row Prefetch Size:** 48 If row  
numb  
client

**Stream Chunk Size:** 256 Spec  
data

Save

- 5 Click the **Connection Pool** tab. The following screen opens:

**Settings for SelectIdentityIntegrationDataSource**

Configuration | Targets | Monitoring | Control | Security | Notes

General | **Connection Pool** | Transaction | Diagnostics | Identity Options

The connection pool within a JDBC data source contains a group of JDBC connections that apply to the pool. The connection pool and the connections within it are created when the connector starts up WebLogic Server or when deploying the data source to a new target.

Use this page to define the configuration for this data source's connection pool.

**URL:**

**Driver Class Name:**

**Properties:**

**Password:**

**Confirm Password:**

- 6 Modify the URL as necessary. For example:  

```
jdbc:bea:sqlserver://<database host name>:<port>
```
- 7 Modify the following values under **Properties** as necessary:
  - databaseName
  - serverName
  - user
  - portNumber
- 8 Change the **password** for accessing the database, if necessary.
- 9 When done, click **Save** and **Activate Changes** to finish.

## Creating New Select Identity Database Information

If you installed Select Audit with Select Identity disabled, you must manually add a Select Identity data source.

- 1 Log on to WebLogic as the administrator.
- 2 In the Domain Structure tree, select **Services** → **JDBC** → **Data Sources**. The **Summary of JDBC Sources** screen opens.

**Summary of JDBC Data Sources**

A JDBC data source is an object bound to the JNDI tree that provides database connectivity through a pool of JDBC connections. Applications can look up a data source on the JNDI tree and then borrow a database connection from a data source.

This page summarizes the JDBC data source objects that have been created in this domain.

[Customize this table](#)

**Data Sources**

Click the **Lock & Edit** button in the Change Center to activate all the buttons on this page.

Name	JNDI Name	Targets
SelectAuditDataSource	jdbc/SelectAudit	AdminServer
SelectAuditProxyDataSource	jdbcproxy/SAudDataSource	AdminServer
SelectAuditReportDataSource	jdbc/SAudDataSource	AdminServer
SelectAuditWorkflowDataSource	jdbc/TruAccess	AdminServer
SelectIdentityIntegrationDataSource	jdbc/IdentityIntegration	AdminServer

- 3 Click **Lock & Edit** to enable data entry.
- 4 In the **Summary of JDBC Sources** screen, click **New**. The **Create a New JDBC Data Source** screen opens:

**Create a New JDBC Data Source**

Back Next Finish Cancel

**JDBC Data Source Properties**

The following properties will be used to identify your new JDBC data source.

What would you like to name your new JDBC data source?

Name:

What JNDI name would you like to assign to your new JDBC Data Source?

JNDI Name:

What database type would you like to select?

Database Type:

What database driver would you like to use to create database connections?

Database Driver:

Back Next Finish Cancel

- 5 Enter:
  - `SelectIdentityIntegrationDataSource` for **Name**.
  - `jdbc.IdentityIntegration` for **JNDI Name**.
- 6 Select your **Database Type** from the dropdown list.
- 7 Select a drivers as follows:
  - use BEA's MS SQL Server Driver (Type 4 XA) Versions 7.0, 2000, 2005 for MSSQL.
  - use BEA's Oracle Driver (Type 4 XA) Versions 9.0.1, 9.2.0, 10 for Oracle.

Click **Next** to continue.

- 8 Click **Next** to continue and accept the **Transaction Options** screen. The **Connection Properties** screen displays:

**Create a New JDBC Data Source**

Back Next Finish Cancel

**Connection Properties**  
Define Connection Properties.

What is the name of database you would like to connect to?

**Database Name:** SIDB

What is the name or IP address of the database server?

**Host Name:** databasehost.can.hp.com

What is the port on the database server used to connect to the database?

**Port:** 1433

What database account user name do you want to use to create database?

**Database User Name:** dbUser

What is the database account password to use to create database connection?

**Password:** .....

**Confirm Password:** .....

Back Next Finish Cancel

- 9 Enter values for:
  - **Database Name**
  - **Host Name**
  - **Port**
  - **Database User Name**
  - **Password**

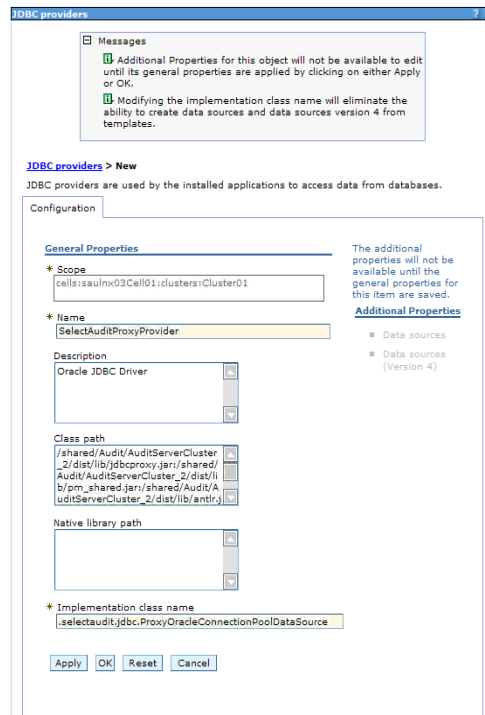
Click **Next** to continue. The **Test Database Connection** screen displays.

- 10 Press the **Test Configuration** button to test the settings. If successful, click **Next** to continue. Otherwise, correct the settings and try again.
- 11 On the **Select Targets** screen, select the checkbox for your server. Click **Finish** to complete the configuration process.
- 12 Click **Activate Changes**.

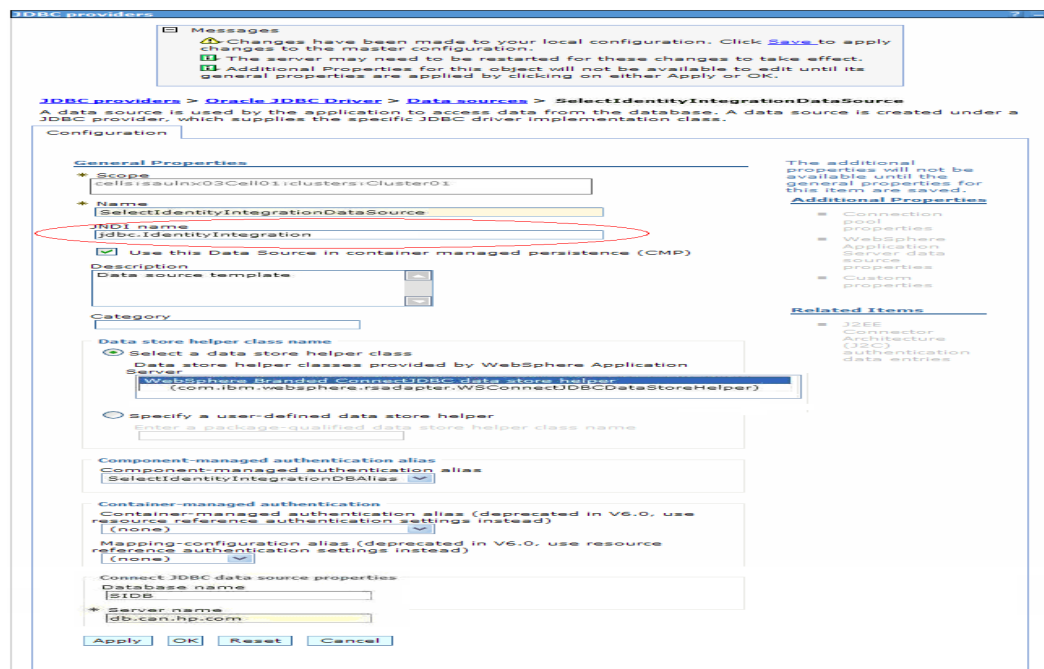
## To create or modify database information in the WebSphere console

- 1 Log on to WebSphere as the administrator.
- 2 Click **JDBC** → **Data Sources**, click **Lock & Edit**, and select your existing Select Identity data source, or click **New** to create a new data source. Then click **Connection Pool**. The settings screen opens.





- 3 Create a connection pool pointing to the Select Identity database or if Select Identity integration has been turned on, modify the pool that has been created by the installer.
- 4 Click **General**. The **General Settings** screen opens.



- 5 Create a data source using the pool or modify the data source that has been created by the installer.

➤ Remember the JNDI name. You will need it in the **Configuration** screen.

- 6 Log on to the Audit Portal as an administrator and follow the steps in [To configure Select Identity filtering](#) on page 41.
  - ▶ Type the data source JNDI name you just created in the **Select Identity Server JNDI Name** field.

## 4 Select Access Integration

You must perform integration tasks in order to use Select Access with Select Audit. This chapter describes the tasks necessary to integrate Select Access with Select Audit for WebLogic and WebSphere.



Select Access has specific configuration requirements in order to log to Select Audit. Unless it is configured properly, Select Access will not log to Select Audit. Refer to the *HP Select Access* documentation for more information about configuring Select Access.

In addition, please note that Select Access v6.2 SP1 is currently supported for integration with Select Audit.

In addition, the following step must be performed prior to integrating Select Audit with Select Access:



Before you begin Select Access integration, you must configure Select Audit to use external LDAP. For details, see “Configuring an External LDAP Server Post-installation” in the *HP Select Audit 1.02 LDAP Configuration Guide*.

This chapter contains the following topics:

- [Integrating Select Access with Select Audit in WebLogic](#) on page 51
- [Integrating Select Access with Select Audit in WebSphere](#) on page 61
- [Report Access](#) on page 69

### Integrating Select Access with Select Audit in WebLogic

There are fourteen tasks you must perform to integrate Select Access with Select Audit:

- 1 Create Policy Builder entries.
- 2 Choose an Identity Location.
- 3 Copy the required Select Access files.
- 4 Unsign the JAR file.
- 5 Configure a generic Enforcer.
- 6 Create the `bea.enforcer.properties` file.
- 7 Modify `startWLSelectAudit.cmd`.
- 8 Create SAREalm.
- 9 Set SAREalm as the default realm.
- 10 Create an empty `sa.login.config` file.
- 11 Set `SelectAccessEnable` to true.
- 12 Modify `directory.xml` for Select Access.

### 13 Restart WebLogic.

These tasks are described below. In the code samples, <hostname> is the name of the WebLogic server and <port> is its port number.



Before you begin the Select Access integration, you must backup the LDAP directory. Once you have completed the integration, you must restore the LDAP directory.

## Task 1: Create Policy Builder Entries

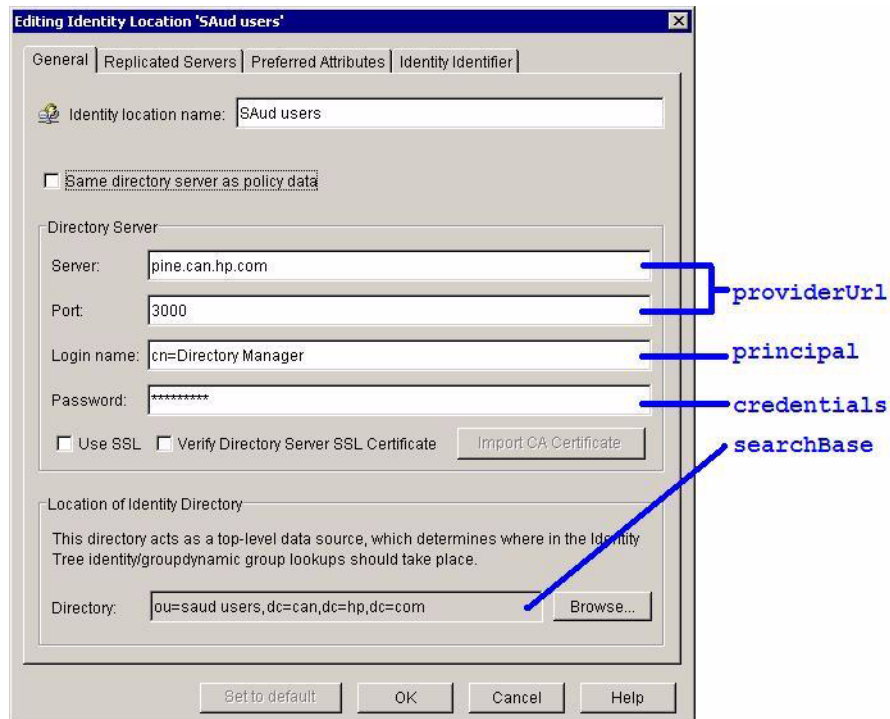
- 1 Create Policy Builder entries by uploading the SA\_policy.LDIF into your policy area under ou=securitypolicy.
- 2 Copy the selectaudit-login.html file from the Select Access integration folder to the Select Access install folder under the content folder, for example, C:\Program Files\HP Software>Select Access\content.

## Task 2: Choose an Identity Location

Although Select Access supports multiple Identity Locations, Select Audit supports only a single Identity Location.

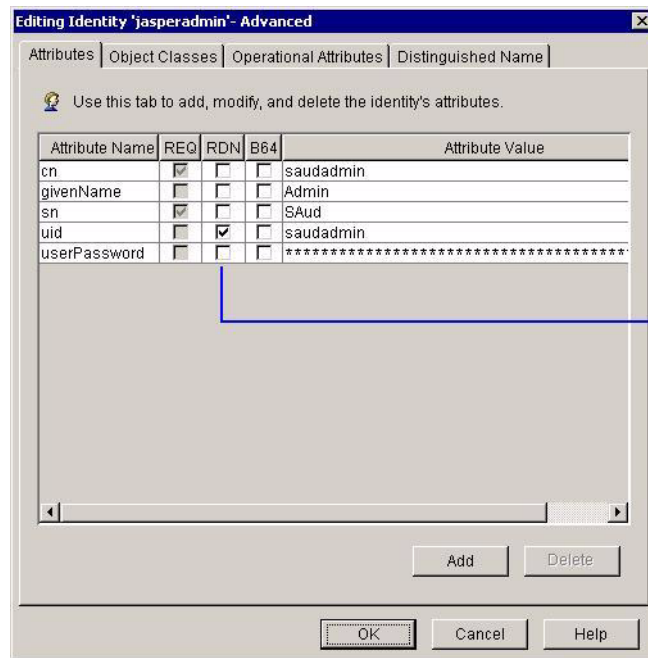
- 1 Select an Identity Location. Only users in this Identity Location will be able to access Select Audit.

Remember the directory server information of this Identity Location. You will need this in [Task 12: Modify the directory.xml file](#) on page 61.



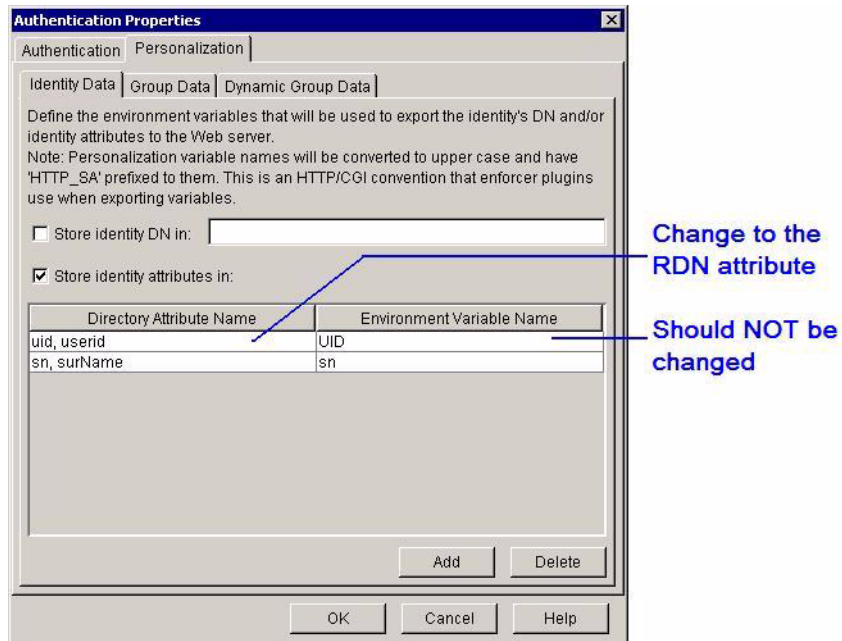
- 2 Each identity in the Identity Location should be using a single attribute as RDN and all the identities should be using the same attribute as their RDN. To check which attribute is being used, go to the identity's **Properties** screen and click **Advanced**. There should only be one attribute selected as the RDN.

▶ In [Task 12: Modify the directory.xml file](#) on page 61, this RDN attribute will be the userSearchAttribute.



Only one attribute should be chosen as the RDN, and all the identities should be using the same attribute.

- a The Policy Builder entries imported in Task 1 are configured to support uid as the RDN. If you need to change it, you must expand the Resources Tree, click **Resource Access - <your host name>** and modify the **Select Auth Properties**. Click the **Personalization** tab and change the **Directory Attribute Name** to the RDN attribute that is used by your identities. You should not change the **Environment Variable Name**, it should always be UID.



- b If Select Audit is also integrated with Select Identity, make sure of the following:
- The identity provisioned into this Identity Location is using the same RDN attribute. The RDN attribute is defined in the Select Identity resource mapping file. Refer to the Select Identity documentation for more information.
  - The authenticator used in WebLogic Security Realm is using the same attribute to identify the user. For example, if you are using Sun ONE directory server, your IPlanetAuthenticator configuration should look like the following:

The screenshot shows the 'Settings for test' configuration page in the WebLogic Server Administration Console. The page is divided into 'Configuration' and 'Performance' tabs, with 'Configuration' selected. The 'Provider Specific' section contains numerous fields for configuring the iPlanet LDAP server connection and search parameters. A blue arrow points from the text 'should be the RDN attribute' to the 'ou=groups, o=example.com' value in the 'Group Base DN' field.

Key configuration fields include:

- Group Base DN:** ou=groups, o=example.com
- User Name Attribute:** uid
- Results Time Limit:** 0
- Dynamic Member URL Attribute:** memberURL
- Static Group Object Class:** groupofuniqueNames
- Parallel Connect Delay:** 0
- Ignore Duplicate Membership:**
- Follow Referrals:**
- Port:** 389
- User Base DN:** ou=people, o=example.com
- Group Search Scope:** subtree
- User Object Class:** person
- All Groups Filter:** (empty)
- Connection Retry Limit:** 1
- SSL Enabled:**
- Propagate Cause For Login Exception:**
- User Dynamic Group DN Attribute:** (empty)
- Static Group Name Attribute:** cn
- Dynamic Group Object Class:** groupofURLs
- Connect Timeout:** 0
- Principal:** (empty)
- User Search Scope:** subtree
- Dynamic Group Name Attribute:** cn
- Use Retrieved User Name as Principal:**
- Credential:** (empty)
- Confirm Credential:** (empty)
- Host:** localhost
- Bind Anonymously On Referrals:**
- Keep Alive Enabled:**
- Static Group DNs from Member DN Filter:** (&(uniqueMember=%M)(o=))
- Cache TTL:** 60
- Static Member DN Attribute:** uniqueMember
- All Users Filter:** (empty)
- Cache Size:** 32
- User From Name Filter:** (&(uid=%u)(objectclass=\*))
- Cache Enabled:**
- Group From Name Filter:** (&(cn=%g)(objectclass=\*))
- Group Membership Searching:** unlimited
- Max Group Membership Search Level:** 0

- 3 Create identities and groups used by Select Audit.
  - a In the Identity Location, create the following items:

- A group called “Select Audit Administrators”. All the Select Audit administrators should be a member of this group.
- A group called “Select Audit Auditors”. All the Select Audit auditors should be a member of this group.
- A group called “Select Audit Users”. Anyone that needs to access Select Audit should be a member of this group.
- A group called “Select Audit Report Developers”. Members of this group will be able to run the Report Designer to design reports.

▶ Select Audit Report Developers must also be a member of another Select Audit group to access the Audit Portal.

- A group that will be mapped to the WebLogic “Admin” role. You can either create a group called “Administrators” or create a different group and add the group name into the WebLogic “Admin” role, “Caller is a member of a group” statement list.
- An admin identity called “weblogic”. This identity should be a member of two groups, the “Select Audit Administrators” group and the “Administrators” group (or the group that will be mapped to the WebLogic “Admin” role). Note that you should select the valid RDN attribute. The RDN attribute value “weblogic” will be used in [Task 12: Modify the directory.xml file](#) on page 61, as the `adminUser`.

### Task 3: Copy the Required Select Access Files

Copy the following files from the Select Access CDs:

- Copy `SASecurityProviders.jar` from the `solution/weblogic` folder to `<BEA_HOME>/weblogic92/server/lib/mbeantypes/` where `<BEA_HOME>` represents the WebLogic home directory.
- Copy the `SAPrincipal.jar` file from the `solution/weblogic` folder to `<BEA_HOME>/weblogic92/server/lib/sa.`
- Copy the following files from the `servlet/servletfilter.war` file to `<BEA_HOME>/weblogic92/server/lib/sa:`

```
bcprov-jdk14.jar
castor-0.9.3.19-xml.jar
EnforcerAPI.jar
jakarta-oro-2_0.jar
jdom.jar
ldapjdk.jar
msgsresources.jar
protomatter.jar
shared.jar
xercesImpl.jar
xml-apis.jar
xml.jar
```

### Task 4: Unsign the JAR File

- 1 Copy the script `unsign.bat` (Windows) or `unsign.sh` (UNIX) from the Select Access integration folder to `<BEA_HOME>/weblogic92/server/lib/sa.`



- 2 Copy `setEnv.bat` (Windows) or `setEnv.sh` (UNIX) to `<BEA_HOME>/weblogic92/server/lib/sa` and modify the it accordingly. You may need to modify the path to the `jdk`.
- 3 Run one of the following JAR files:

**For Windows:**

```
unsign.bat xercesImpl.jar
```

**For Linux, Solaris, HP-UX:**

```
./unsign.sh xercesImpl.jar
```

## Task 5: Configure a Generic Enforcer

- 1 Run the Select Access Setup Tool and configure a generic Enforcer with the name `enforcer_bea.xml`. Save this file in `<BEA_HOME>/user_projects/domains/mydomain/`. Ensure this directory is in the path.
- 2 Select a custom setup on the **Generic Enforcer Plugin Setup - General** screen.
- 3 Proceed through the Setup Tool.
- 4 On the **Generic Enforcer Plugin Setup - Ignored Filenames** screen specify the following filenames to be ignored by the Enforcer:
  - `*.gif`
  - `*.jpg`
  - `*.jpeg`
  - `*.css`
  - `*.js`
  - `*.ico`

## Task 6: Create the `bea_enforcer.properties` File

Create the file `<BEA_HOME>/user_projects/domains/mydomain/bea_enforcer.properties` as shown below.

```
EnforcerAPIConfigFile=enforcer_bea.xml
Service=<hostname>:<port>
Resource=/
LogLevel=info
SecurityRealm=SARealm
```

## Task 7: Modify `startWLSelectAudit.cmd`

In `startWLSelectAudit.cmd`, and `stopWeblogic.cmd`, add the following lines.

**For Linux, Solaris, and HP-UX:**

```
SA_LIB="{WL_HOME}/server/lib/sa"

SA_CLASSPATH="{SA_LIB}"
```

```

SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/bcprov-jdk14.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/jdom.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/castor-0.9.3.19.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/castor-0.9.3.19-xml.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/commons-pool-1.2.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/EnforcerAPI.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/jakarta-oro-2_0.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/ldapjdk.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/msgsresources.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/protomatter.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/sa-j2ee-util.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/sa-wl9.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/selectauditclient.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/servletenforcer.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/shared.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/xerces.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/xml-apis.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/xml.jar"

WEBLOGIC_CLASSPATH="${WEBLOGIC_CLASSPATH}:${SA_CLASSPATH}"

JAVA_OPTIONS="-Dweblogic.security.fullyDelegateAuthorization=true
${JAVA_OPTIONS}"

export WEBLOGIC_CLASSPATH
export JAVA_OPTIONS

```

### For Windows:

```

set SA_LIB=%WL_HOME%\server\lib\sa

set SA_CLASSPATH=%SA_LIB%
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\bcprov-jdk14.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\jdom.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\castor-0.9.3.19.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\castor-0.9.3.19-xml.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\commons-pool-1.2.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\EnforcerAPI.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\jakarta-oro-2_0.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\ldapjdk.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\msgsresources.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\protomatter.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\sa-j2ee-util.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\sa-wl9.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\selectauditclient.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\servletenforcer.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\shared.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\xerces.jar

```

```

set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\xml-apis.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\xml.jar

set WEBLOGIC_CLASSPATH=%WEBLOGIC_CLASSPATH%;%SA_CLASSPATH%

set JAVA_OPTIONS=-Dweblogic.security.fullyDelegateAuthorization=true
%JAVA_OPTIONS%

```

After modifying the appropriate file for your environment, restart WebLogic.

## Task 8: Create SAREalm

Create the SAREalm using the WebLogic console.

- 1 In the WebLogic console, create SAREalm.
- 2 Select **web apps and EJBs protected in DD** from the **Check roles and policies** drop-down list.
- 3 In the **Providers** tab, click **Add a new Default Adjudicator**.
- 4 Type `DefaultAdjudicator` and click **Create**.
- 5 In the **Details** tab, clear the **Require Unanimous Permit** check box and click **Apply**.
- 6 In the **Authentication** tab, add the authenticators listed below in the following order:
  - SAAAuthenticator
  - IPlanetAuthenticator

Point this authenticator to the same LDAP used by Select Access. See [Configuring an External LDAP Server Post-installation](#) in the *HP Select Audit 1.02 LDAP Configuration Guide*.
  - SAIdentityAsserter (clear **Base64Decoding Required** and move `PolicyUser` to **Chosen**)
  - DefaultIdentityAsserter (move `AuthenticatedUser` to **Chosen**)
- 7 In the **Authorization** tab, add the following authorizers:
  - DefaultAuthorizer
  - SAAuthorizer
- 8 In the **Credential Mapping** tab, add a `DefaultCredentialMapper`.
- 9 In the **Role Mappers** tab, add a `DefaultRoleMapper`.

## Task 9: Set SAREalm as the Default Realm

- 1 Click **Security** in the WebLogic console.
- 2 Select **SAREalm** in the **Default Realm** field.
- 3 Click **Apply**.

## Task 10: Create an Empty sa.login.config File

Create an empty `sa.login.config` file in the `<WLS_HOME>/weblogic92/server` directory.

## Task 11: Set SelectAccessEnable to True

To integrate with Select Access, `SelectAccessEnable` must be set to “true” in `audit_config.xml` file in the `/dist/config` folder:

```
<SelectAccessEnabled>true</SelectAccessEnabled>
```

## Task 12: Modify the directory.xml file

- 1 Change the DirectoryProvider from:

```
com.hp.ov.selectaudit.report.security.SaudWeblogicDirectoryProvider  
to
```

```
com.hp.ov.selectaudit.report.security.selectaccess.SaDirectoryProvider
```

- 2 Change <providerName>DefaultAuthenticator</providerName>

to

```
<providerName>IPlanetAuthenticator</providerName>
```



**NOTE:** If you get the following error from Java (Windows only):

```
Exception in thread "main" java.lang.NoClassDefFoundError: ûcp
```

Try the following commands:

- At the command prompt, go to the Select Audit install directory, typically C:\Program Files\HP Software\Select Audit\auditserver
- set classpath=../setup/ReplaceText.jar;../dist/reporting/ReportServer/WEB-INF/lib/scopeserver.jar;../dist/reporting/ReportServer/WEB-INF/lib/log4j.jar

- java

```
com.hp.ov.selectaudit.build.ModifyTextFileIAProps
```

```
"dist/reporting/ReportServer/WEB-INF/conf/directory.xml"
```

```
"SA_LDAP_LOGIN_PSWD_ENCRYPT=<password>", "PASSWORD_ENCRYPT_ON=true".
```



**NOTE:** If any of the passwords are not encrypted, verify isEncrypted="false".

## Task 13: Restart WebLogic

- 1 Restart WebLogic.
- 2 Log on to Select Audit using the uids of users in your Select Access Identity Location.



**NOTE:** The default policy provided by HP in the LDIF file should be used only as a template. You should adjust the policy to suit your security needs..

# Integrating Select Access with Select Audit in WebSphere

Before you begin integrating Select Access with Select Audit, read the *Select Access Integration Paper for IBM WebSphere 6.0.2 Guide* to understand how Select Access integration works.

- 1 Install Select Audit using an LDAP server that is supported both by Select Audit and Select Access.

Before proceeding make sure everything, especially reports, are working correctly.

- 2 Log on to the WebSphere Administrative Console and click **Security** → **Global Security**.
- 3 Clear the following two check boxes:
  - **Enable global security**
  - **Enforce Java 2 security**
- 4 Click **Save** and restart the server.
- 5 Integrate Select Access by following the instruction in the *Select Access Integration Paper for IBM WebSphere 6.0.2 Guide*.
  - Use the same identity location in LDAP as you used during the installation of Select Audit in [step 1](#).
  - Before performing the final step “To enable external security mechanisms”, restart the server so that the Select Access classes get loaded.
  - Perform the following tasks in Chapter 3 of the *Select Access Integration Paper for IBM WebSphere 6.0.2 Guide*:
    - Configuring WebSphere for External Authentication and Authorization
    - The Select Access Enforcer Properties File for WebSphere
    - The Administration Console Configuration Parameters
    - To configure Custom User Registries parameters
    - To configure Trust Association parameters
    - To configure JACC provider settings
    - To enable external security mechanisms
    - To stop and restart the WebSphere server
    - The WebSphere-specific Settings for Select Access
    - To add Select Access JAAS module to the default configuration
    - Configuring WebSphere for the JAAS Login
    - Protecting a Web Service
  - Ensure you are able to secure the WebSphere Administration Console and sample applications like `snoop servlet` using Select Access as described at the end of section “*The WebSphere-specific Settings for Select Access*”.
- 6 Set the registry.



Do not use `Select Access Registry`. Certain required functions are not implemented and therefore, it cannot be used with Select Audit. Instead use the `LDAP User Registry` as is used by Select Audit during installation.

- a On the Admin console, click **Security** → **Global Security**.
- b Click **Configuration** → **General Properties** → **Active User Registry** and select Lightweight Directory Access Protocol (LDAP) user registry.
- c Click **OK** and save settings.
- d Restart the server.

7 Copy the `selectaudit-login-ws.html` file from the install CD folder `Extras\SA_Integration` to the `Select Access` folder under `Select Access\content`, for example, `C:\Program Files\HP Software>Select Access\content`.

8 Edit the `SA_policy_WebSphere6.0.LDIF` file using a text editor and type appropriate values for your installation for `<hostname>` and `<port>`.

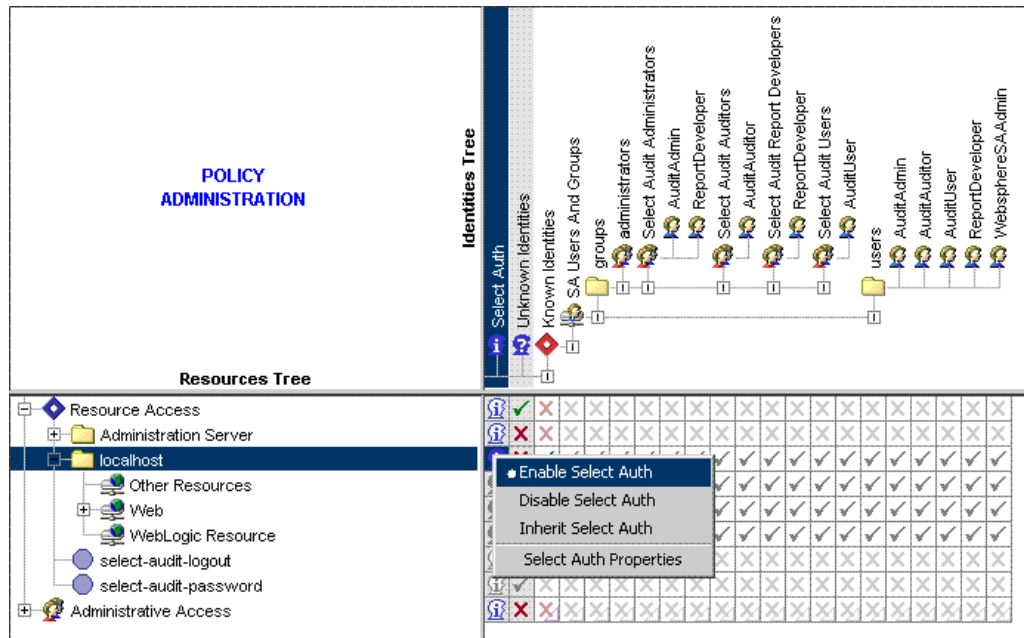
The `SA_policy_WebSphere6.0.LDIF` file can be found on the install CD under the `Extras\SA_Integration` folder.

9 Create Policy Builder entries by uploading the `SA_policy_WebSphere6.0.LDIF` file edited in [step 8](#) into your policy area under `nxresource=network,ou=securitypolicy` in your LDAP server.

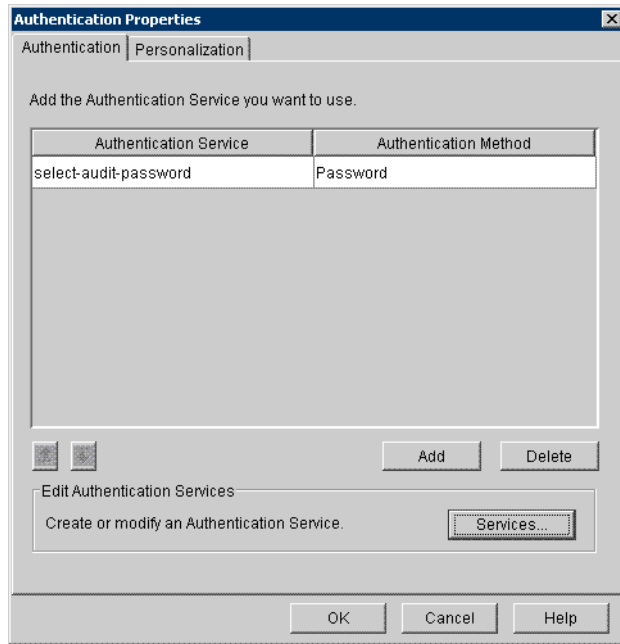
An LDAP browser is necessary to upload the LDIF file. Consult your LDAP server documentation for more information about uploading LDIF files.

10 In the Policy Builder, make sure `Select Auth` is enabled for the resource you uploaded.

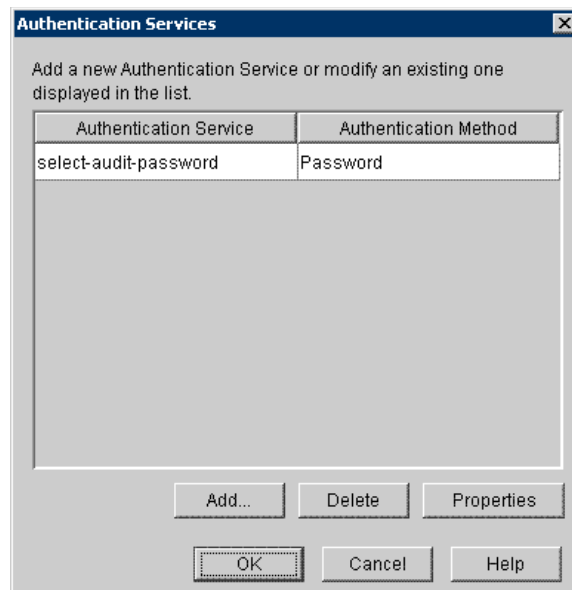
a Right click the `Select Auth` icon.



b Click `Select Auth Properties`.

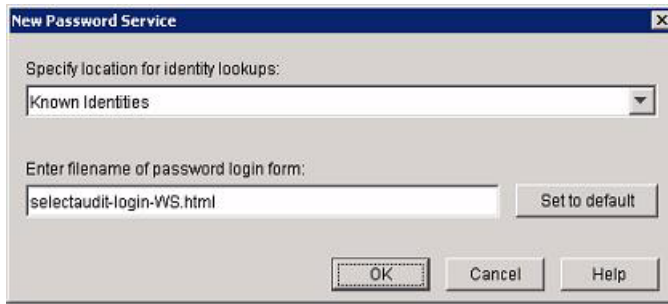


- c Click **Services** and make sure the authentication service `select-audit-password` has been assigned to the authentication method `Password`. Click **Add** to do this if it is not already done.

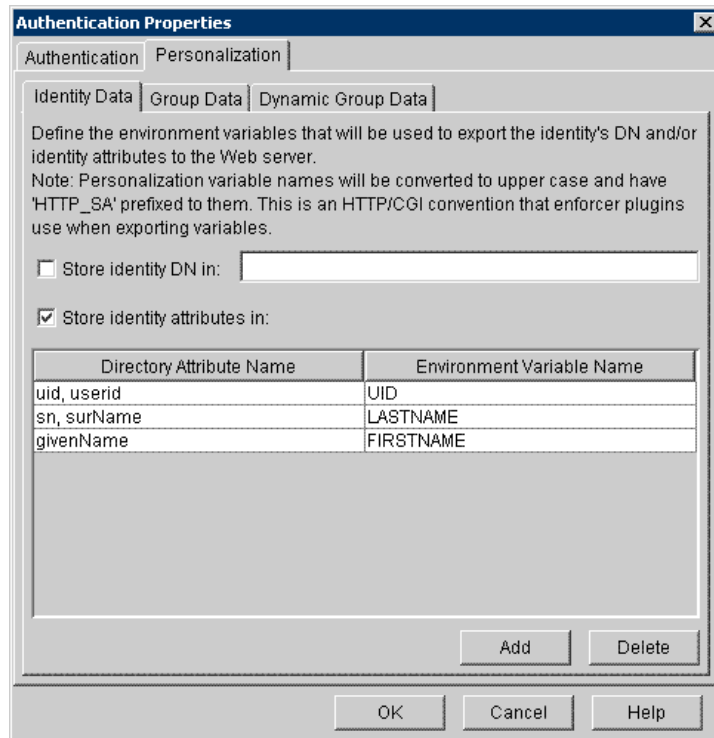


- d Click **select-audit-password Properties**. The **New Password Service** screen opens.





- e Type `selectaudit-login.html` in the **Password login form** field.
- f Add the two personalization parameters `LASTNAME` and `FIRSTNAME` to return the users Last Name and First Name respectively.



A sample Policy Builder screen is shown below:

The screenshot displays the Policy Administration interface. On the left, the **Resources Tree** shows a hierarchy starting with **Resource Access**, followed by **Administration Server**, **localhost**, **Other Resources**, and **Web**. Under **Web**, there are sub-trees for **auditportal** and **scopeserver**. The **auditportal** tree includes files like **clienttimezone.jsp**, **pages**, **approval**, **config**, **configure.jsf**, **head.jsf**, **logout.jsp**, **model**, **modelconfigure.jsf**, **schedule**, **verify**, **verify.jsf**, and **welcome.jsf**. The **scopeserver** tree includes **clienttimezone.jsp**, **logout.html**, **runas**, **scopedesigner**, and **soapservice**. At the bottom of the Resources Tree are **select-audit-logout** and **select-audit-password**, and **Administrative Access** at the very bottom.

On the right, the **Identities Tree** shows a hierarchy starting with **Select Auth**, followed by **Unknown Identities**, **Known Identities**, **SA Users And Groups**, **groups**, **administrators**, **Select Audit Administrators**, **AuditAdmin**, **ReportDeveloper**, **Select Audit Auditors**, **AuditAuditor**, **Select Audit Report Developers**, **ReportDeveloper**, **Select Audit Users**, **AuditUser**, **users**, **AuditAdmin**, **AuditAuditor**, **AuditUser**, **ReportDeveloper**, and **WebsphereSAAdmin**.

A grid of access permissions is visible on the right side of the Resources Tree, showing a grid of icons (checkmarks, X's, and keys) representing access permissions for various identities across different resources.

- 11 Enable the default access to permit access for Unknown Identities by selecting **Unknown Identities** for the very first line under Resource Access.

This is necessary for the SOAP calls from the Report server to work. Please refer to *Protecting a Web Service* in Chapter 3 of the *Select Access Integration Paper for IBM WebSphere 6.0.2*. This section states:

“The Login Module will not be able to retrieve location for authorization therefore it will look for the default authorization in the sa\_enforcer and authenticate against it”.

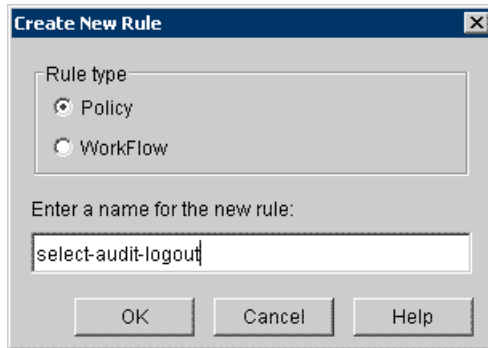
- 12 Make sure that the conditional rule to enable logout from Select Access works for the following two resources:

auditportal/pages/logout.jsp  
scopeserver/logout.html



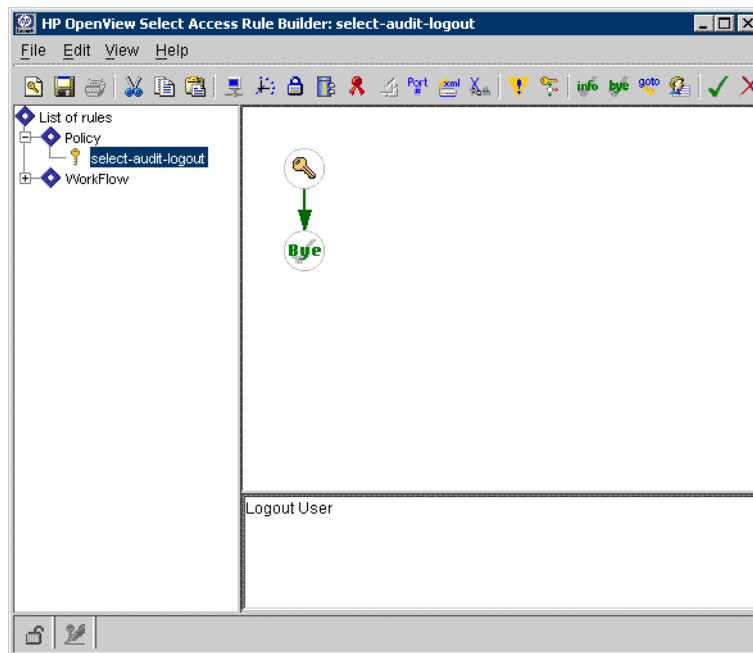
Sometimes the rule does not work when it is uploaded from an LDIF file. If the rule does not work, do the following:

- Allow access to Unknown Identities.
- Add a conditional rule to log out the user every time the `logout.jsp` or `logout.html` is accessed. The procedure is as follows:
  - a Right-click **Known Identities** for `pages/logout.jsp` and select **Inherit Access**.
  - b Right-click **Known Identities** for `pages/logout.jsp` and select **New Conditional Rule**. The **Create New Rule** dialog box opens.

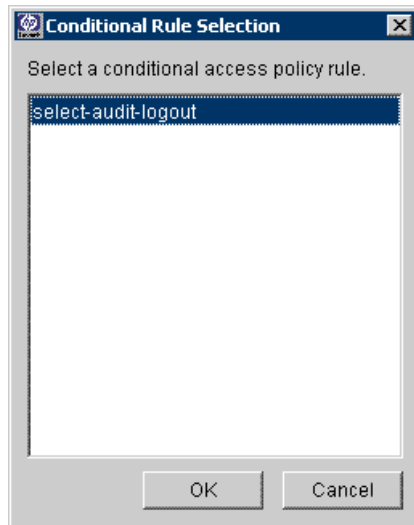


- c Type `select-audit-logout` in the **Name** field and click **OK**.

The **Select Access Rule Builder** screen opens. Create the new rule using “Bye” as shown below:



- d Right-click **Known Identities** for `scopeserver/logout.html` and select **Conditional Access**. The **Conditional Rule Selection** dialog box opens.



- e Select `select-audit-logout` and click **OK**.
- 13 Edit the `<SelectAudit_Install_Directory>/auditserver/dist/config/audit_config.xml` file and set `SelectAccessEnable` to `true`:  

```
<SelectAccessEnabled>true</SelectAccessEnabled>
```
- 14 Restart the server.
- 15 Open the Audit Portal and attempt to log in. The Select Access prompt opens.
- 16 Log in using the appropriate user name and password.
- 17 In the Policy Builder set the appropriate `ALLOW` and `DENY` permissions for users to control what menu items are shown for each class of users.



**NOTE:** The default policy provided by HP in the LDIF file should be used only as a template. You should adjust the policy to suit your security needs..

## Report Access

Report access is set in the Report Center using the **Permissions** screen. Refer to [Managing Reports](#) on page 102 for more information about setting permissions.

The following table shows what reports are viewed with J2EE and Select Access integrations:

**Table 5 Report Access with J2EE or Select Access Integration**

Report	Users	Administrators	Auditors
Account Change Report	Read	Full permissions including: <ul style="list-style-type: none"> <li>• Read</li> <li>• Write</li> <li>• Delete</li> <li>• Execute</li> <li>• Schedule</li> <li>• Ad Hoc</li> <li>• View permissions</li> <li>• Grant permissions</li> <li>• Revoke permissions</li> </ul>	Read
Account Events Report	Execute		Execute
Administrator Report	Schedule		Schedule
Change History Report	Ad Hoc		Ad Hoc
Configuration Report			
Password Management Report			
Security Events Report			
Service Report			
System Activity Report			
User Activity Report			
User Summary Report			
Workflow Events Report			
Attestation Report			
Data Integrity Report			
Raw Message Report	Denied		



# 5 Models

This chapter describes the Select Audit model dashboard, the model report structure, and how to use models in Select Audit. The **Models** menu is used to obtain a high-level view of the loaded models, view model run activity, and load, export and update models.

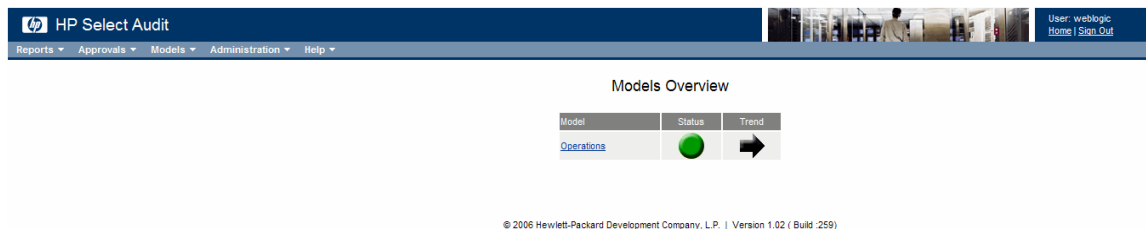
This chapter contains the following topics:

- [Overview](#) on page 71
- [Operations Model](#) on page 72
- [Model Analysis Tree](#) on page 72
- [Loading Compliance Models](#) on page 74
- [Configuring Models](#) on page 76

## Overview

The model overview is a high-level view of the currently-loaded models. Click **Models** → **Overview** on the toolbar. The **Models Overview** screen opens.

**Figure 5 Models Overview Screen**



There are two types of models. The Operations model is run four times a day to capture and analyze normal operations data. Compliance models are run once daily and generate reports based on compliance specifications.

## Operations Model

The Operations model captures and analyzes normal operations data. You can view reports that show the status of the system, as well the trend of the status and the history of the status. See [Appendix B, Operations Model Thresholds](#) for information about the Operations model thresholds.

## Compliance Models

The compliance models are optional add ons. Currently, the Sarbanes-Oxley (CoBIT) report pack is available for purchase. Compliance models for different policies and regulations will be made available periodically. Refer to *HP Select Audit 1.03 Sarbanes-Oxley Model Guide* for more information about the Sarbanes-Oxley (CoBIT) model.

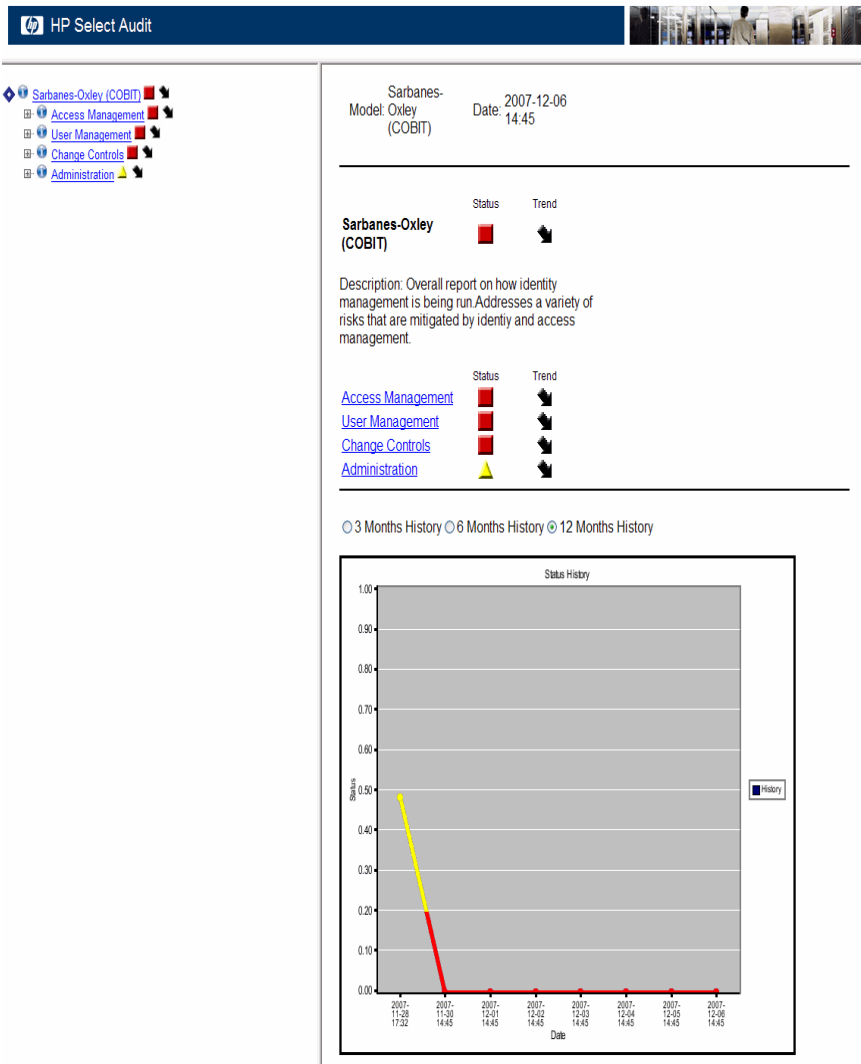
## Model Analysis Tree

The Model Analysis Tree provides a comprehensive look at a compliance model. The analysis tree window is divided into left and right panes. The left pane contains an expandable and collapsible tree containing all model parameters. The right pane contains the status, trends, and history for Select Audit model parameters. These parameters are also described. This information is arranged to provide quick access to compliance information.

The Model Analysis Tree is accessed by clicking a model name in the **Models Overview** screen.




### **Figure 6 The Model Analysis Tree**








By clicking the tree entries in the left pane or the parameter names in the right pane, you can navigate through the entire set of compliance parameters.

The level of the current report is shown at the top of the report, along with the model name and the date the report was generated. The body of the report is divided into two sections. The top section of the report shows the metric being represented, its status and the trend. Status of the level of compliance with the defined control objectives is shown by a status indicator:

-  compliance level is good
-  compliance level is adequate
-  compliance level is poor

The status is calculated from the child nodes and is determined by the lowest level of any child node. For example, if a child node is red, the top-level status will be red, even if all other child nodes are green.

The trend of the level of compliance is shown by arrows:

-  improving level of compliance
-  compliance level staying the same
-  declining level of compliance

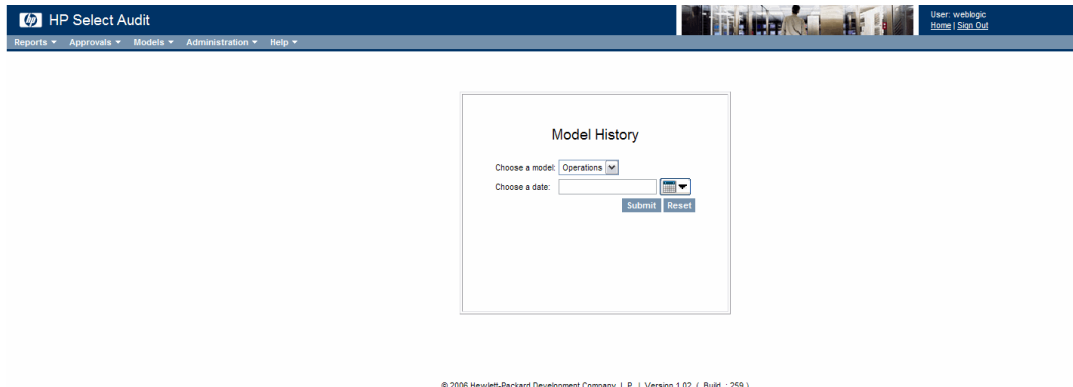
The child nodes are listed under the report metric. You can click the child node name to drill down to reports for those nodes.

The left side of the window lists a hierarchical structure of all reports available for the model.

## Model History

A complete record of model runs organized by date and time is available by selecting **Models** → **Model History** from the menu.


**Figure 7 Model History Screen**



You can select a model from the dropdown list and select a date by clicking the calendar icon, enabling you to view detailed model run results for a given time and date.

## Loading Compliance Models

The Model Loader enables users to load and remove compliance models using the **Model Loader** screen on the **Manage Models** screen, accessed by selecting **Models** → **Manage Models** from the menu.

-  You can run multiple compliance models on the same server.

The model file consists of a zip file (usually named `model.zip`) that includes the properties file `TRDefault`. The loaded model must contain the file `complete.xml`.

Before uploading the model, the Model Loader checks the following:

- The model file is a zip file. The loader checks for a .zip ending and makes sure the file is a real zip file.
- The zip file contains the complete .xml file and that it is a valid xml file. The xml file must contain the root tag <Package> with the attribute name.

The name of the model is retrieved from the name attribute in the <Package> root tag. If there is any error in the loading process, an error message is shown. The model is extracted from its zip format and copied to the Select Audit setup configuration directory. A new directory that is generated as random numbers, for example, <config dir>/models/1027774882/\*, is created in the models directory created by the Audit Server installer.



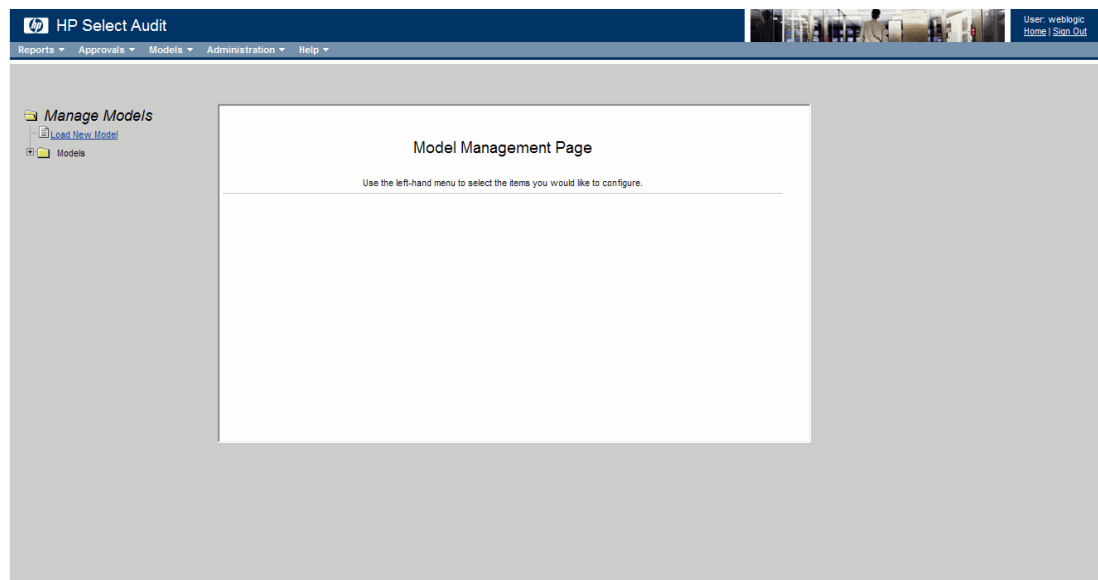
Ensure the user who starts the web server has read/write access for the configuration directory, otherwise an error is generated.

If you attempt to load a model with a name that is already stored in the database, you will be prompted to update the model. If you update the existing model, the Model Loader removes the existing model (both the files and the database entries) and copies the new model in as a new entry.

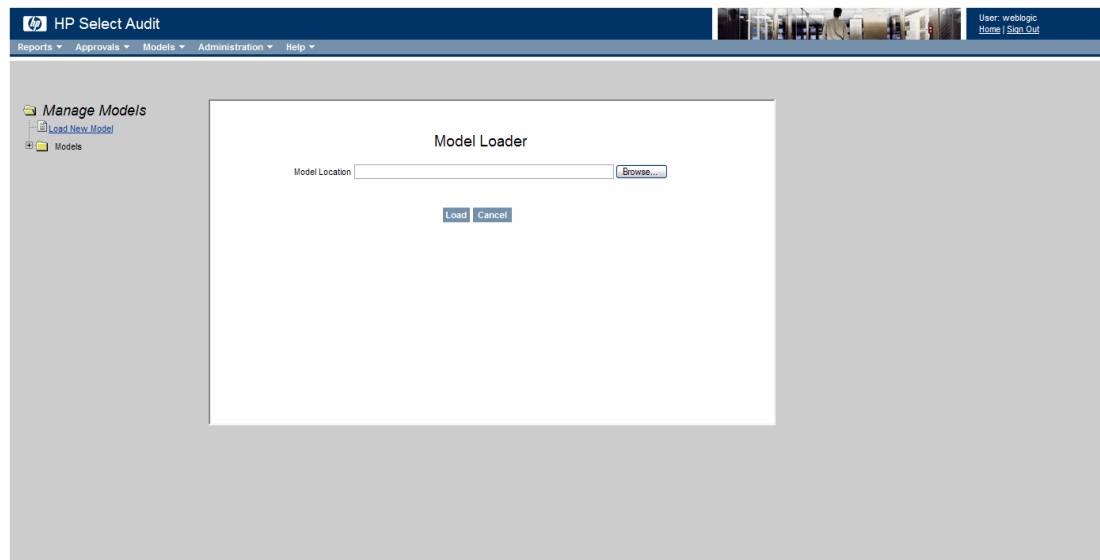
After the model is loaded successfully, the left-hand tree view is refreshed with the newly-loaded model. The previously-generated model reports are not deleted on update.

## To load a compliance model

- 1 Click **Models** → **Manage Models**. The **Model Management** screen opens.



- 2 Click **Load New Model** on the left side of the screen. The **Model Loader** screen opens.



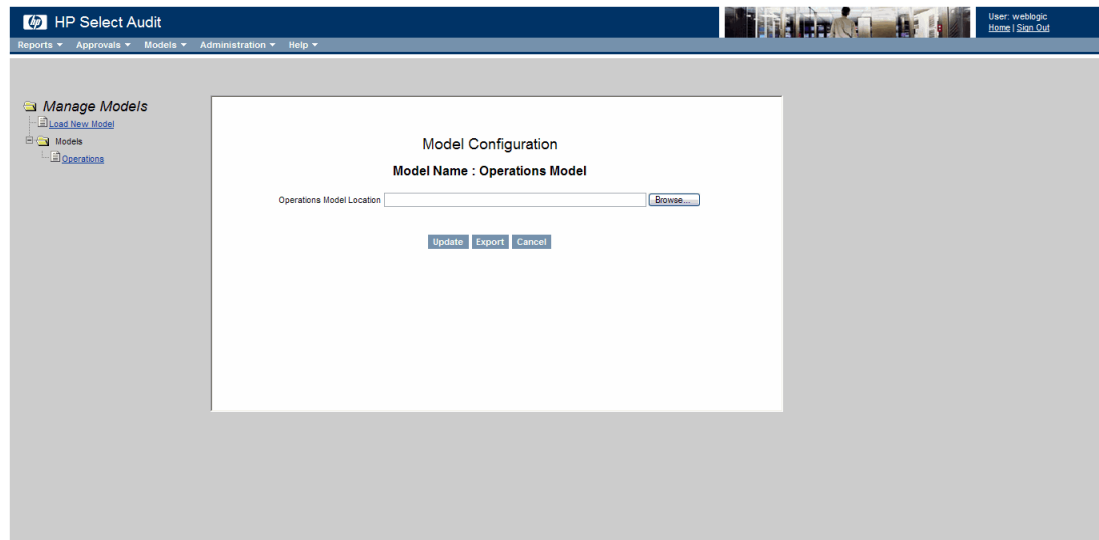
- 3 Click **Browse** and navigate to select the model ZIP file you want to load.
- 4 Click **Load**. The new model is loaded into Select Audit.

## Configuring Models

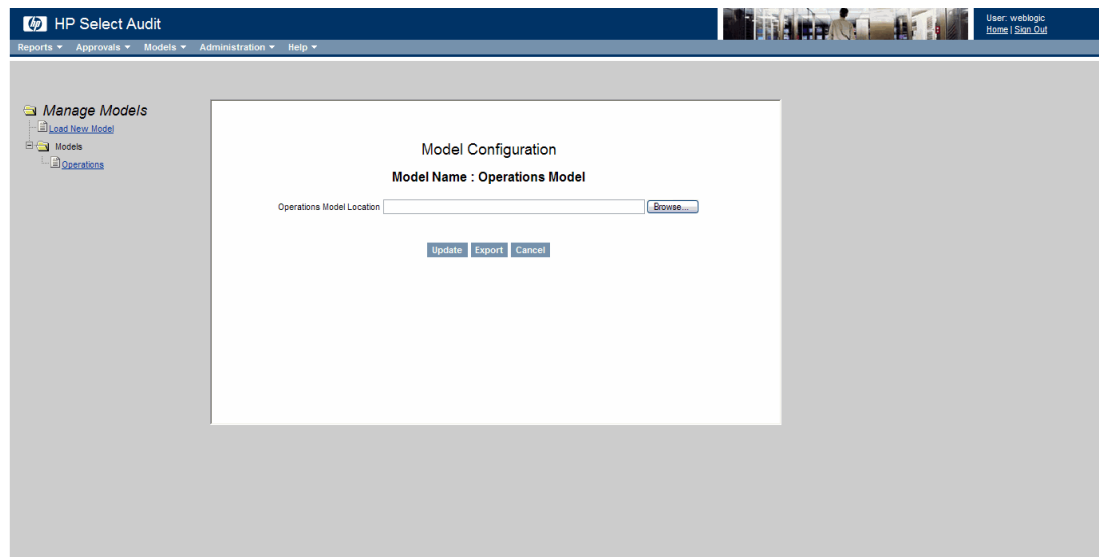
The model configuration screens are used to update, export and models. You can update the Operations model and make any necessary changes using the **Configuration** screen. Using the Compliance model configuration screen, you can export Compliance models to a different location.

### To configure loaded models

- 1 Expand the **Models** folder under Manage Models on the left side of the screen to view the loaded models.
- 2 Click a model name. The configuration screen varies according to the type of model you selected:
  - If you click the Operations Model, the **Operations Model Configuration** screen opens.



- If you click a compliance model name, the corresponding model **Configuration** screen opens.



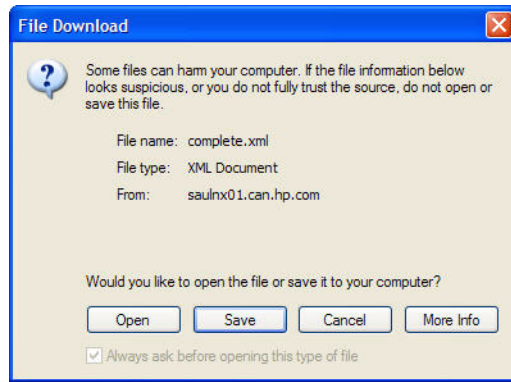
### To update a model

You can update an Operational model by exporting the model, making any desired changes and re-importing the model using the update function.

- 1 On the **Operations Model Configuration** screen, click **Browse** and navigate to select the model zip file you want to update.
- 2 Click **Update**. The updated model is loaded into Select Audit.

### To export a model

- 1 On a **Model Configuration** screen, click **Export Model**. The **File Download** dialog box opens.



The model directory is zipped and the zip file is downloaded to the client browser machine.

- 2 Click **Save**. The **Save As** window opens.
- 3 Browse to the location you which to save the file and click **Save**. The **Download Complete** window opens.
- 4 Click **Close**.

### To delete a model

On a **Model Configuration** screen, click **Delete Model**. The model is deleted from the model directory and all the files in the directory are deleted. The model is no longer available in Select Audit. You can re-load the model if required.



When you delete a model from the Audit Server, the data generated by that model is not deleted.

# 6 Verifying Data

When Select Audit is installed, data integrity protection is initially disabled. You must use the Audit Portal to load the time-stamping key and enable data integrity protection. Once the data integrity protection is enabled, you can verify data integrity and run the Data Integrity report from the Audit Portal.

This chapter describes how to configure and verify data integrity in the Audit Portal. It contains the following sections:

- [Configuring Data Integrity](#) on page 79
- [Verifying Data Integrity](#) on page 82

## Configuring Data Integrity

The Audit Server uses a public/private key pair to generate time-stamps. You must specify the key pair when deploying the Audit Server. Select Audit supports Java, PKCS 11 and 12, and pfx keystores on WebLogic. On WebSphere, only Java keystores are currently supported. Users are responsible for creating and managing the keystore. Select Audit does not provide keystore management.

The old private key can be discarded but the old public key must be kept in the configured keystore in order to verify the old time-stamps. If the public key is not available, data verification will result in integrity errors for anything signed with the private key associated with the unavailable public key.

You configure the signing and keystore properties for data integrity in the Audit Portal.

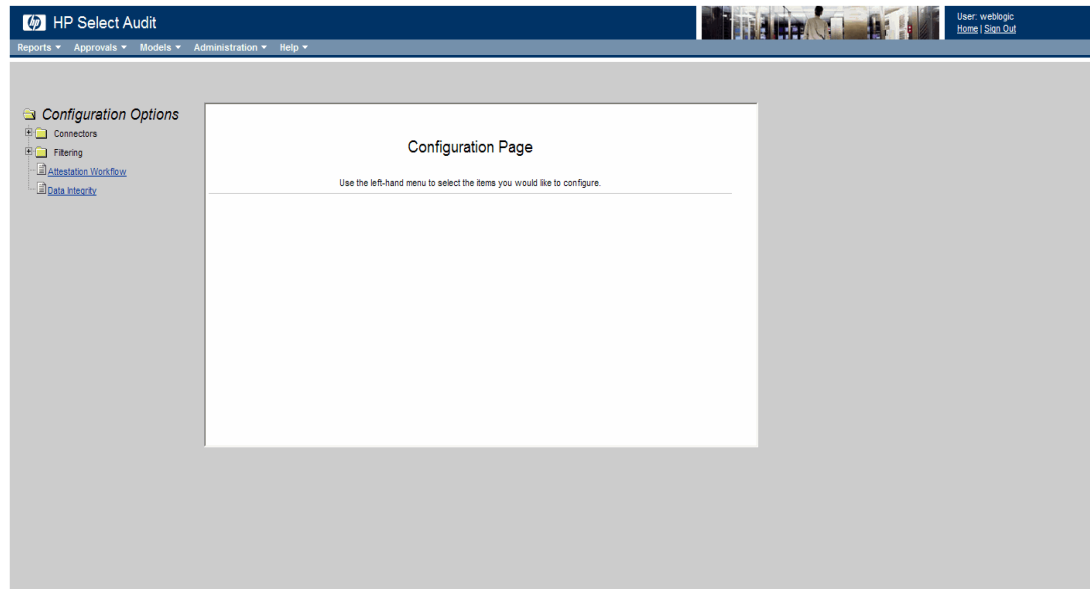
### To configure data integrity for Java and PKCS 12 keystores

The steps in this method work for both Java and PKCS12 keystores.

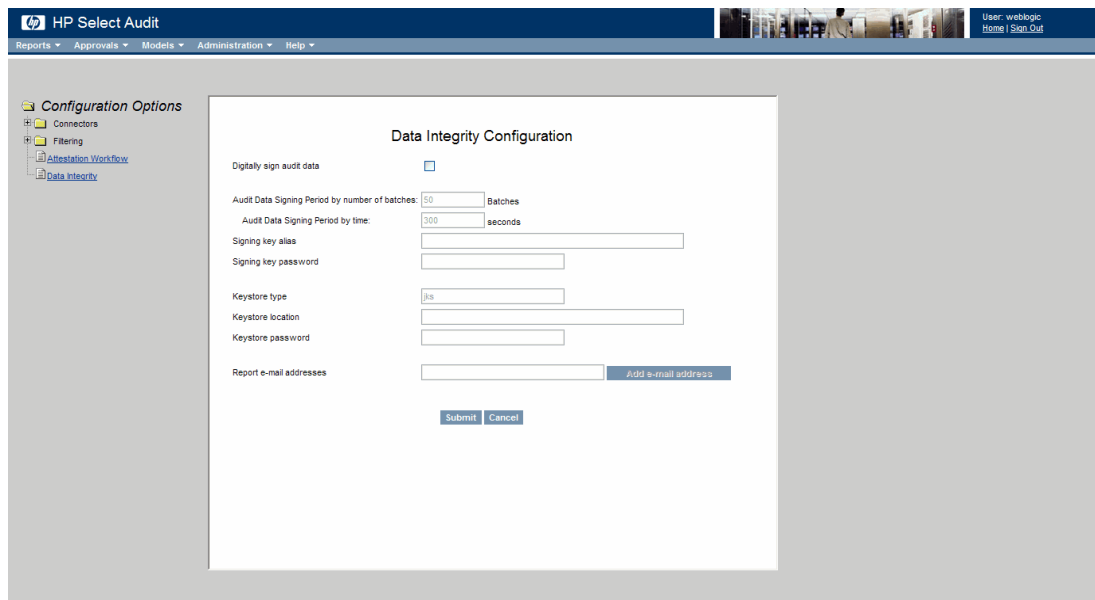


For a cluster installation, the Keystore location has to be accessible to all nodes in the cluster. It should be located on the shared folder, as specified in [Installing in a Clustered Environment on WebLogic](#) on page 20 in the *HP Select Audit 1.02 Installation Guide*.

- 1 Select **Administration** → **Configuration**. The **Configuration** screen opens.



- 2 Click **Data Integrity**. The **Data Integrity** screen opens.





- 3 Select the **Digitally sign audit data** check box to enable the signing of data and populate the fields with default values.

▶ If this box is not selected, none of the parameters on this screen are used.

- 4 Complete the fields as described in [Table 6](#).

**Table 6 Data Integrity Fields**

Field	Data Entered
Sign audit data every...	Type a value for the batch size or period of time.
Signing key alias	Type the alias for the signing key.
Signing key password	Type the password for the signing key.
Keystore type	Type a keystore type in the <b>Keystore Type</b> field.
Keystore location	Type the path (on the server) of the keystore.
Keystore password	Type the password for the keystore.

- 5 Type the email address of the person who will receive the report in the **Report e-mail addresses** field and click **Add e-mail address**.

▶ When you initially configure Data Integrity, you can type a semicolon separated list of email addresses. The email addresses will be saved when you click **Submit**. After Data Integrity is configured, you can add email addresses using **Add email address** without resaving the other parameters of the Data Integrity configuration.

- 6 Click **Submit**. The message **Successfully submitted** is shown at the bottom of the screen.

### To use .pfx files as keystores

- 1 Download and install Java Cryptopgrphy Extension (JCE) Unlimited Strength Jurisdiction Policy Files 1.4.2 from the Sun web site:

<http://java.sun.com/j2se/1.4.2/download.html>

▶ The high encryption JCE is only required when using pfx keystores. The JCE contains two files: `local_policy.jar` and `US_export_policy.jar`.

- 2 Copy these files into the web server's `JDK/jre/lib/security` directory, where `JDK` is the path to either the web server's Sun or Jrockit JDK configured at installation time, to replace low encryption versions of these files.

▶ You should have backed up the directory previously.

- 3 Ensure that the certificates contain CA certificates.
- 4 Follow [step 1 to 3 in To configure data integrity for Java and PKCS12 keystores](#) on page 79.
- 5 Complete the **Data Integrity** screen as follows:
  - Type `pkcs12` in the **Keystore type** field.
  - Leave the **Signing key alias** and the **Signing key password** fields blank.
  - Type the path to the `.pfx` file the **Keystore location** field.

- Type the email address of the person who will receive the report in the **Report e-mail addresses** field and click **Add e-mail address**.
- 6 Click **Submit**. The message **Successfully submitted** is shown at the bottom of the screen.

## Configuring Select Audit for Keys Stored on Smart Cards and HSMs

Select Audit can digitally sign the audit data using keys stored on smart cards, USB tokens and HSMs. Integration with such devices requires a PKCS#11 provider which makes cryptographic operations of these devices accessible through the JCA/JCE framework.

Please contact your support representative if you want to configure Select Audit for PKCS#11 keystores.

## Verifying Data Integrity


If you are an auditor, you can verify data integrity and the run the Data Integrity report in the Audit Portal.

- 1 Select **Administration** → **Verify Audit Data Integrity**. The **Data Verification** screen opens.

The screenshot shows the HP Select Audit web interface. The top navigation bar includes 'Reports', 'Approvals', 'Models', 'Administration', and 'Help'. The main content area is titled 'Data Verification' and contains the following sections:

- Last Verification Run Status**:
  - Run Start Date:
  - Run End Date:
  - Run Status:
- Run Verification Period**:
  - Start Date: [text input] [calendar icon]
  - End Date: [text input] [calendar icon]
- Buttons: **Verify Now** and **Stop Verification**

This screen is used to specify date parameters for running data verification. The **Last Verification Run Status** section shows the run start and end date, and status of the last run data verification.

- 2 Type a **Start Date** and an **End Date** in the appropriate fields or use the calendars to specify the dates.
  -  You can also specify start and end times in addition to the date by typing the value in the appropriate fields after the date.
- 3 Click **Verify Now**. The message “Verification is successfully executing” is shown at the top of the screen to indicate that data verification is running. If you enter the same values for the start and end dates and times, data verification will not run and an error message will be displayed on the screen.

The **Data Integrity** report is listed in the **Select Audit Reports** folder of the Report Center.



# 7 Workflow Attestation

The Select Audit Workflow Engine sends out alerts about various real-time audit events. It also sends out audit reports for attestation and accepts attestations of those reports. This chapter describes how use the Audit Portal to configure Attestation workflows to specify approvers and schedules for report approvals, and how to approve reports. It contains the following topics:

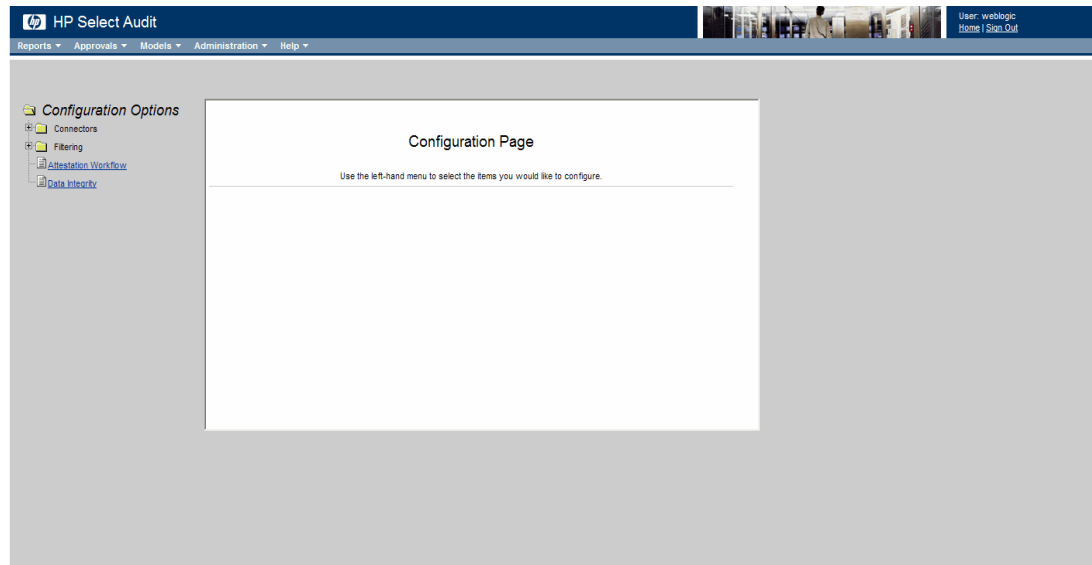
- [Configuring Attestation Workflows](#) on page 85
- [Approving Reports](#) on page 88

## Configuring Attestation Workflows

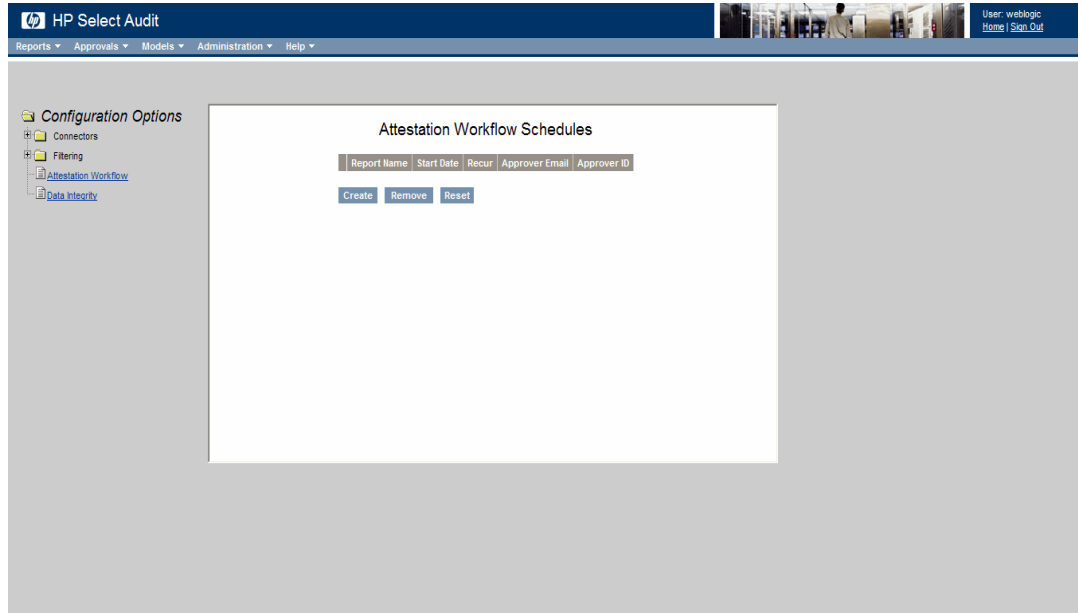
You can configure Attestation workflows in the Audit Portal to specify approvers and schedules for report approvals.

### To configure an Attestation workflow

- 1 Select **Administration** → **Configuration**. The **Configuration** screen opens.

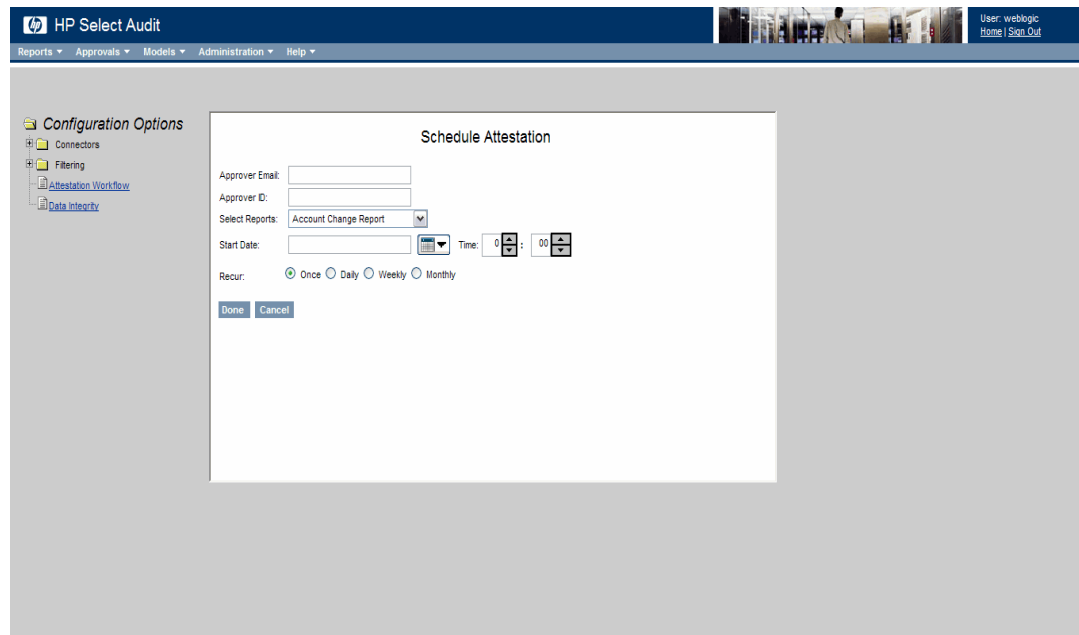


- 2 Click **Attestation Workflow**. The **Attestation Workflow Schedules** screen opens.



The **Attestation Workflow Schedules** screen shows the reports scheduled with an Attestation workflow.

- 3 Click **Create** to add an Attestation workflow schedule. The **Schedule Attestation** screen opens.
  - When setting up a workflow schedule, different users cannot schedule the same Attestation Workflow report for the same time.
  - You cannot modify a schedule. To change a schedule, you must remove the existing schedule and recreate it. Select the check box beside the report name and click **Remove**.



- 4 Type the email address of the person who will approve the report in the **Approver Email** field.

▶ You should setup the email server as described in the *HP Select Audit 1.02 Installation Guide*.

- 5 Type the approver's Select Audit user name in the **Approver ID** field.
- 6 Select the report to be approved from the **Selected Reports** drop-down list.
- 7 Specify a **Start Date** and **Time** for the report.

▶ If you set the Start Date or Time for a period that has already past, the schedule will start immediately.

- 8 Select the **Once**, **Daily**, **Weekly** or **Monthly** radio button to specify the recurrence of the schedule.
- 9 Click **Done**. The new Attestation workflow is shown in the **Schedule List** screen.

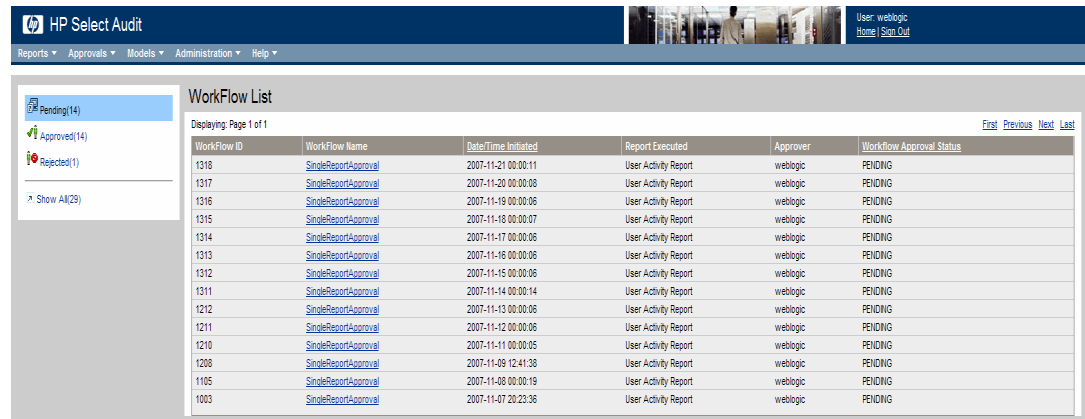
When the report is run, the approver will receive an email alert and see the report in the **My Pending Approvals** screen. See [Approving Reports](#) on page 88 for more information.

# Approving Reports

You can approve reports awaiting your approval, and view reports you have approved or rejected using the **Approvals** menu.

- 1 Click **Approvals** → **My Pending Approvals**. The **Workflow List** screen opens.

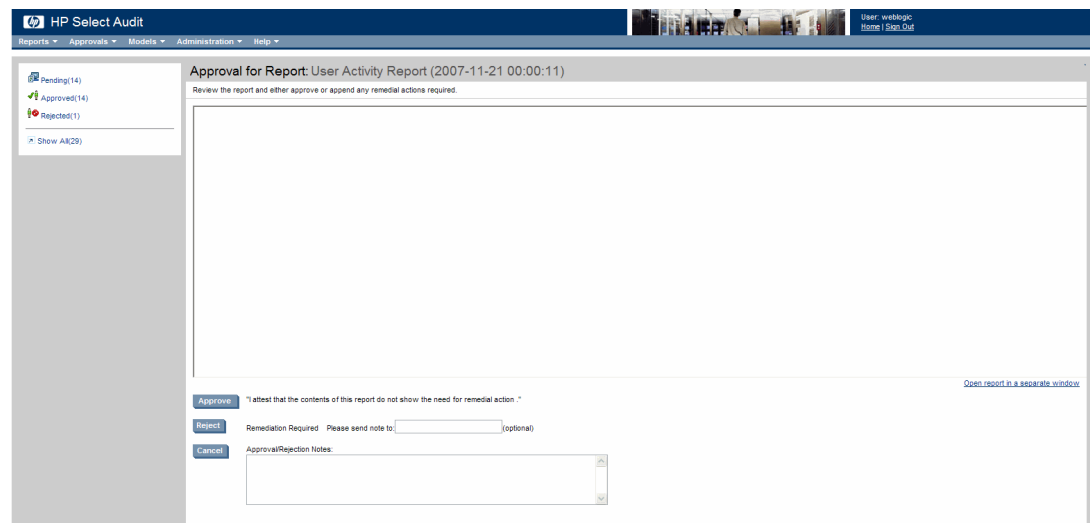
- Click **Approved** or **Rejected** to see a list of approved or rejected reports. Click **Show All** to see all reports with approval requests.
- You can sort the Workflow List by Workflow Approval Status or Time/Date Initiated.



Workflow ID	Workflow Name	Date/Time Initiated	Report Executed	Approver	Workflow Approval Status
1318	SingleReportApproval	2007-11-21 00:00:11	User Activity Report	weblogic	PENDING
1317	SingleReportApproval	2007-11-20 00:00:08	User Activity Report	weblogic	PENDING
1316	SingleReportApproval	2007-11-19 00:00:06	User Activity Report	weblogic	PENDING
1315	SingleReportApproval	2007-11-18 00:00:07	User Activity Report	weblogic	PENDING
1314	SingleReportApproval	2007-11-17 00:00:06	User Activity Report	weblogic	PENDING
1313	SingleReportApproval	2007-11-16 00:00:06	User Activity Report	weblogic	PENDING
1312	SingleReportApproval	2007-11-15 00:00:06	User Activity Report	weblogic	PENDING
1311	SingleReportApproval	2007-11-14 00:00:14	User Activity Report	weblogic	PENDING
1212	SingleReportApproval	2007-11-13 00:00:06	User Activity Report	weblogic	PENDING
1211	SingleReportApproval	2007-11-12 00:00:06	User Activity Report	weblogic	PENDING
1210	SingleReportApproval	2007-11-11 00:00:05	User Activity Report	weblogic	PENDING
1208	SingleReportApproval	2007-11-09 12:41:38	User Activity Report	weblogic	PENDING
1105	SingleReportApproval	2007-11-08 00:00:19	User Activity Report	weblogic	PENDING
1003	SingleReportApproval	2007-11-07 20:23:36	User Activity Report	weblogic	PENDING

- 2 Click the report you wish to approve. The approval page opens in the same browser window.

- You can view the report in a new window by clicking **Open report in separate window** on the report.



- 3 Click **Approve** to approve the report or click **Reject** to send the report back for remedial action.

- You can send a note with the rejection by typing an email address in the **Email note to:** field.



# 8 Using Reports in Select Audit

Reports are viewed, scheduled and modified using the Report Center. This chapter describes how to configure the Report server and the features of the reporting tools in Select Audit. Reports are accessed using the **Reports** menu on the Select Audit toolbar.



You can also access reports using the **Reports** workspace.

For more detailed information about report creation and design, refer to the *HP Select Audit 1.02 Report Center User's Guide*, *HP Select Audit 1.02 Report Designer's Guide* and *HP Select Audit 1.02 Report Developer's Guide*.

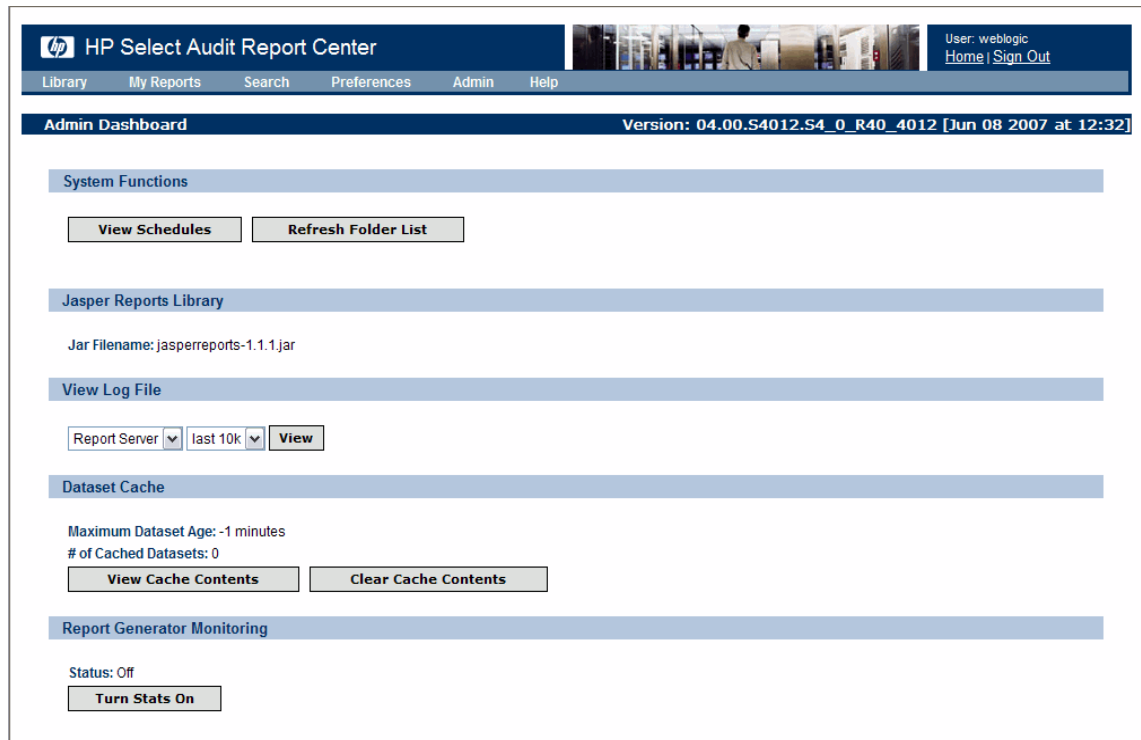
This chapter contains the following topics:

- [Configuring the Report Server](#) on page 89
- [Using the Report Center](#) on page 93
- [Using My Reports](#) on page 95
- [Using the Library](#) on page 95
- [Running the Ad Hoc Wizard](#) on page 105
- [Searching for Reports](#) on page 114
- [Setting Preferences](#) on page 116
- [Editing Report Schedules](#) on page 117

## Configuring the Report Server

You can use the **Admin Dashboard** in the Report Center to configure various aspects of the Report server. Click **Admin** in the Report Center. The **Admin Dashboard** opens.

**Figure 8 Admin Dashboard**



The Admin Dashboard contains five sections:

- System Functions
- Jasper Reports Library
- View Log File
- Dataset Cache
- Report Generator Monitoring

Use these sections to configure the Report server.

## Performing System Functions

You can view all the schedules in the Library and update the Library folder lists in the **System Functions** section of the Admin Dashboard.

## To view schedules

Click **View Schedules**. The **Schedules** screen opens.



ID	Report Name	Recurrence Interval	Owner	Schedule	Status	
1	<a href="#">/Select Audit Reports/Configuration Report</a>	every week	weblogic	Starts: Wed Dec 26 10:17:00 EST 2007 3 run(s) to go	WAITING	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

For each schedule in the Library, the following information is shown:

<b>ID</b>	The report's ID number.
<b>Report Name</b>	The name of the report. If you click the link, a new page opens showing the report's properties.
<b>Recurrence Interval</b>	How often the report automatically produces output.
<b>Owner</b>	User name of the report's owner.
<b>Schedule</b>	The starting and ending timestamps for automatic output generation.
<b>Status</b>	The status of the schedule. Possible values are as follows: <ul style="list-style-type: none"><li>• <b>FIRING</b>: Schedules or tasks that are currently running.</li><li>• <b>PAUSED</b>: Schedules that are paused.</li><li>• <b>RECOVERABLE</b>: Schedules that were running when the system went down.</li><li>• <b>WAITING</b>: Schedules that are waiting to run.</li></ul>

Refer to [Editing Report Schedules](#) on page 117 for information about making changes to report schedules.

## To refresh the folder list

Click **Refresh Folder List** to update the list of folders that is shown in the Library view. This is useful when multiple Report servers share the same Library.

## Jasper Reports Library

This section shows the name of the JAR file for the Library.

## Viewing Log Files

You can view two types of log files using the Admin Dashboard:

- Report server
- SQL

## To view log files

- 1 Select the log that you want to view from the left-most drop-down list.
- 2 Optionally, select the number of characters from the right-most drop-down list. Possible values are:
  - last 10k
  - last 50k
  - all
- 3 Click **View**. The log file opens.

## Viewing the Cache

The datasets created when a user runs reports are temporarily cached in memory. By default, cached datasets are removed from memory if they are unused for 20 minutes. Active datasets are removed after 60 minutes. The Dataset Caching section shows the following information:

- The datasets currently in the cache.
- The time when the dataset was cached.
- The remaining time the dataset will remain in the cache.

By default, dataset caching is enabled for the Report server. It can be disabled for the entire server, for individual queries, or for individual HTTP requests.

- 1 Click **View Cache Contents** to view the cache contents for the Report server. The **Report Server Dataset Cache** screen opens.

Report Server Dataset Cache							
age	time since last used	max age	max unused age	rows	fetch time (ms)	times used	cache key

- 2 Click the browser **Back** button to return to the Admin Dashboard.

## Viewing Report Generator Statistics

You can view statistics for Report Generator performance and memory. The **Admin** screen shows the statistics for all reports run since Report Generator Monitoring was turned on. The **Properties** screen for a report shows the same statistics but only for that report. You can also view the properties of a report to see its statistics.

## How Layout and Content Times are Calculated

The sum of layout and content times is always accurate. This sum represents the time to execute a query, iterate over the result set, and generate the output. However, the breakdown between Layout and Content times may vary depending whether the report was successfully optimized. If optimization is successful, then Content Time is the time to execute the query and Layout Time is the time to iterate the result set and to generate the output. If optimization is unsuccessful, Content Time is the time to execute a query and iterate over the result set and the Layout time is the time to generate output.

Some of the following factors affect whether queries can be optimized:

- Summary calculations in the header
- In-memory sorting
- EJBs and XML datasets
- Stored procedures

### To view report generator statistics

- 1 Click **Turn Stats On** in the **Report Generator Monitoring** section to enable monitoring. A message is shown at the top of the screen confirming that monitoring is enabled.

The **Turn Stats On** button is changed to a **Turn Stats Off** button. In addition, **Report Server Performance Statistics** and **Report Server Memory Statistics** are shown.

**Report Generator Monitoring**

Status: On  
Start Time: Thu Mar 09 12:34:05 EST 2006

**Turn Stats Off**

**Report Generator Performance Statistics**

Report Name	# of Runs	Total Run Time	Avg. Run Time	Avg. Compile Time	Avg. Content Time	Avg. Layout Time
<i>No scopes have been executed.</i>						

**Report Generator Memory Statistics**

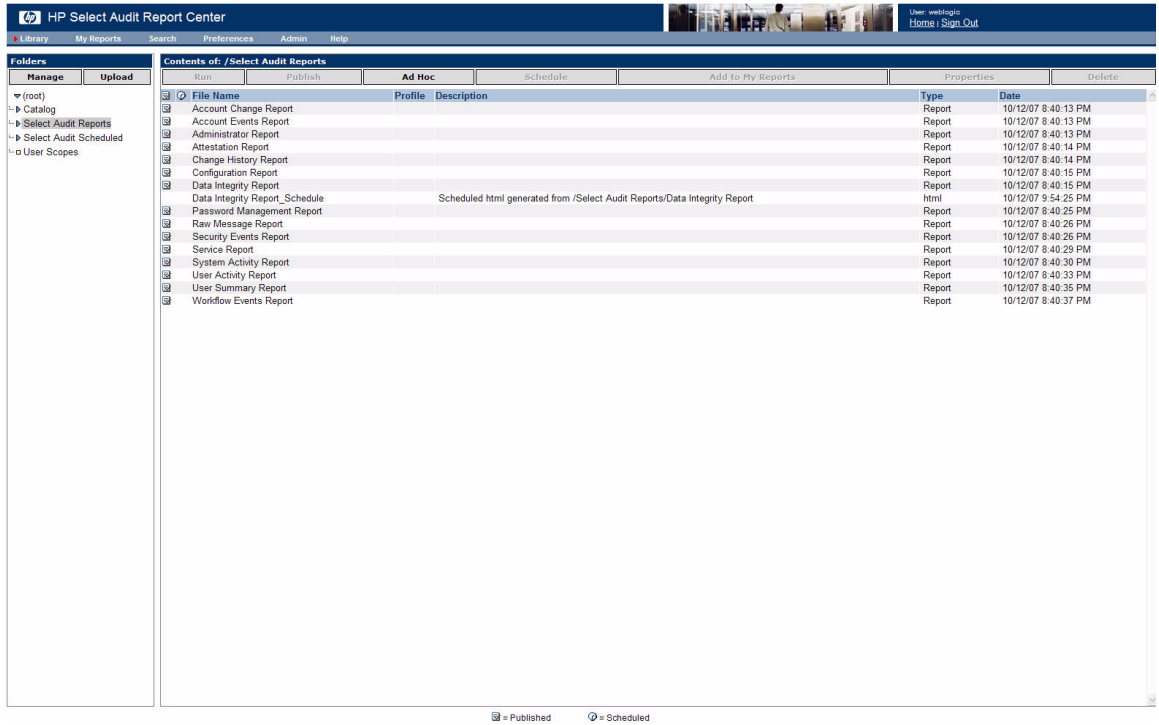
Time (secs)	Memory Used (bytes)	Total Memory (bytes)	Free Memory (bytes)
0	40265128	117776384	77511256
60	40265128	117776384	77511256
120	40265128	117776384	77511256
180	40265128	117776384	77511256
240	40265128	117776384	77511256
300	40265128	117776384	77511256
360	43935088	117776384	73841296

- 2 Click the name in the **Report Name** column to see the properties of any monitored report.
- 3 Click **Turn Stats Off** to disable statistics.

## Using the Report Center

The Report Center is used to view, print, and schedule reports. It is also used to administer the Library. You can use the Report Center to upload files, control security using J2EE (WebLogic) security, schedule reports and monitor performance.

**Figure 9 Report Center**



The Report Center has five main sections, described in [Table 7](#).

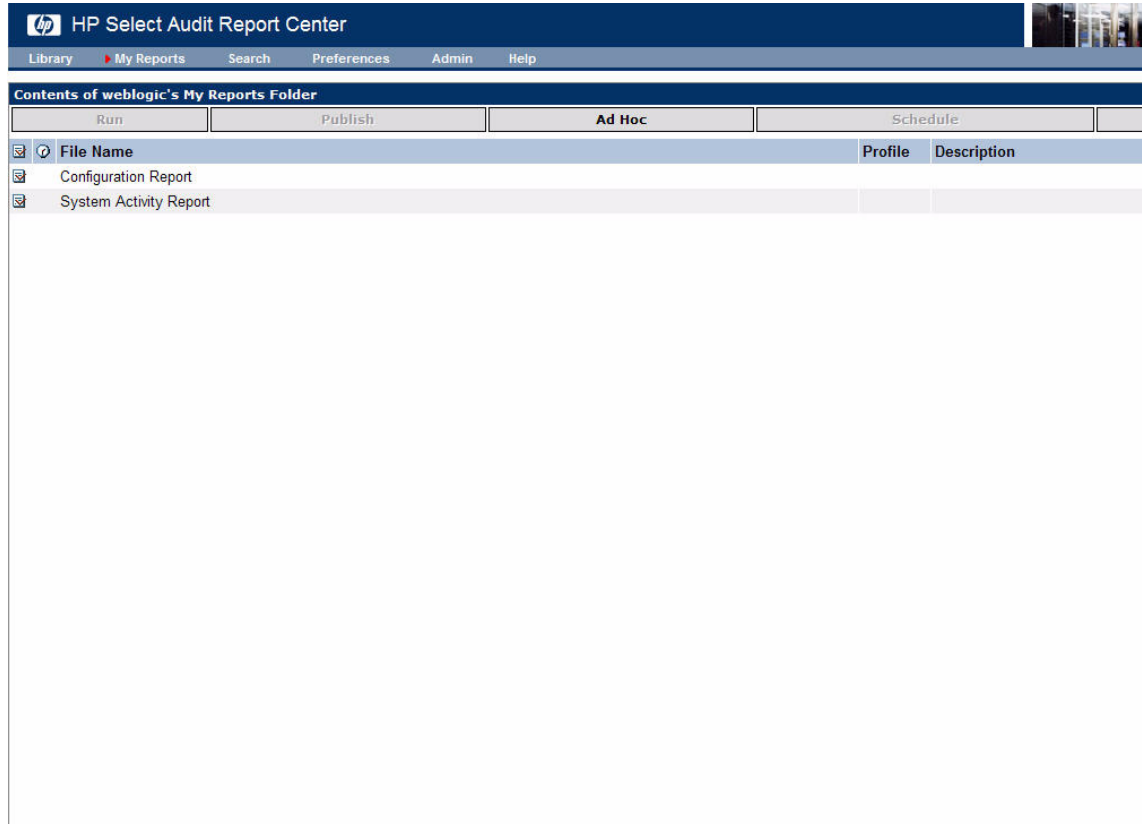
**Table 7 Report Center Sections**

Section	Description
<b>Library</b>	Use the Library to access and arrange the reports on the Report server.
<b>My Reports</b>	My Reports provides a shortcut to frequently-viewed reports.
<b>Search</b>	Use Search to locate files in the Library by name, type or description.
<b>Preferences</b>	Preferences is used to set user preferences, such as your start page.
<b>Admin</b>	Users with administrator privileges can view server logs and report schedules, and monitor system performance.

# Using My Reports

You can save frequently-viewed reports and customized reports in the **My Reports** folder.

**Figure 10 My Reports Folder**



The **My Reports** screen is a single window listing the Library files that you have previously selected using **Add to My Reports**. Refer to [Managing Reports](#) on page 102 and [Running the Ad Hoc Wizard](#) on page 105 for information about using **My Reports**.

# Using the Library

The Library is divided into two panels that are used to manage folders and reports. The left-hand **Folders** panel contains the folders containing reports. The right-hand **Contents of** panel contains the reports contained within the selected folder.

In the Folders panel you can modify the folder settings and upload new files to the Library. Using the **Contents of** panel, you can run, schedule and remove reports, change report properties and create Ad Hoc reports.

The Folders panel has four standard folders: **Catalog**, **Select Audit Reports**, **Select Audit Scheduled**, and **User Scopes**.

## Catalog

The Catalog folder contains the parameter, query, permission and theme files available through the Select Audit Report Designer.

## Select Audit Reports

The Select Audit Reports folder contains 15 predefined Select Audit Reports, as listed in [Table 8](#).

**Table 8 Select Audit Reports**

Report Name	Contents
Account Change Report	All user account change actions (add, delegate, change).
Account Events Report	All account event actions (security violations, admin login errors, expired passwords).
Administrator Report	All administrator actions (configuration changes, authentication changes, password resets).
Attestation Report	Contains all attestation actions (approved, pending, denied).
Change History Report	Administrative audit as complete tasks (the action initiated on this date by this user at this time, approved first by this person at this time, approved next by this person at this time, and the change took affect at this time).
Configuration Report	All configuration change actions (add, change).
Data Integrity Report	A list of tampered records IDs and tampered signature record IDs, with change actions (added, modified, removed).
Password Management Report	All password administration actions (expire, logon).
Raw Message Report	Raw audit messages that aren't normalized through the standard process.
Security Events Report	All security events (security violation, configuration changes).
Service Report	Configuration changes to Select Identity services.
System Activity Report	All system activities (login, logout, changes made).
User Activity Report	All user activities (login, logout, changes made).
User Summary Report	A summary of user activities.
Workflow Events Report	All workflow event messages.

## Select Audit Scheduled

The Select Audit Scheduled Reports folder contains all reports scheduled by the user. For details, see [To run a report](#) on page 102.



## Select Identity-specific Reports

Select Audit provides three Select Identity-specific reports as a separate report bundle, listed in [Table 9](#).

**Table 9** Select Identity-specific Reports

Report Name	Contents
Request Metrics Report	Returns the number of Select Identity requests started, completed, in progress, terminated or rejected for each service. It also displays a total count for each request metric.
Workflow Response Metrics Report	Returns the average approval time for each Select Identity Workflow block and the approver's role.
User Entitlements Report	Returns the Select Identity account information associated with each user, listing the resources that can be accessed and their associated entitlements.

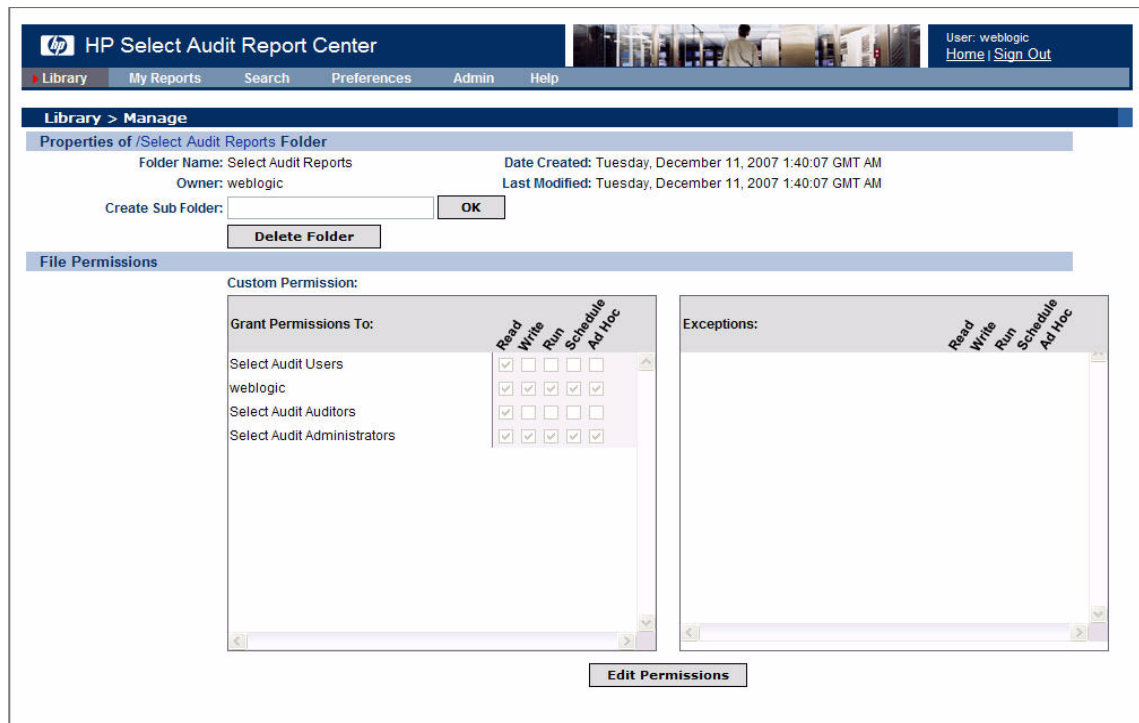
## User Scopes

User Scopes is the home directory for all users in the Library. When you create reports, they are saved to this folder by default.

## Managing Folders

Click **Manage** to open the **Library > Manage** screen. In this screen, you can create sub-folders, delete folders and edit file permissions.

**Figure 11 Library > Manage Screen**



### To create a sub-folder

- 1 Type a folder name in the **Create Sub Folder** field on the **Library > Manage** screen.
- 2 Click **OK**. The new folder is shown in the Library Folder list.

### To delete a folder

- 1 In the Library, select the folder you want to delete and click **Manage**. The **Library > Manage** screen opens.
- 2 Confirm that the name of the folder you want to delete is shown in the **Folder Name** field in the **Properties** section of the screen.
- 3 Click **Delete Folder**. A prompt opens asking you to confirm the deletion of the folder.
- 4 Click **OK**. The folder name is no longer shown in the **Properties** section of the **Library > Manage** screen and or the Library Folder list.

## To change folder permissions

- 1 Click **Edit Permissions** on the **Library > Manage** screen. The **Edit Permissions** screen opens.

HP Select Audit Report Center

User: weblogic  
Home | Sign Out

Library > Properties > Edit Permission

Permissions for: Select Audit Reports

Grant Permissions To:	Read	Write	Run	Schedule	Ad Hoc
Select All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select Audit Users	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
weblogic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Select Audit Auditors	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select Audit Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Exceptions:	Read	Write	Run	Schedule	Ad Hoc
Select All	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add Groups... Add Users... Delete Submit Cancel

Copyright © 2002-2006 JasperSoft Corporation. All rights reserved.

The Edit Permissions screen has two sections: **Grant Permissions To** and **Exceptions**.

Permissions can be set to grant or exclude access to folders in the same manner in each section. Permissions can be set universally, by group or by user.

- 2 To set permissions or exceptions, select the corresponding check boxes. You can set the following folder permissions:

**Read** Users/group members can read the RDL file.

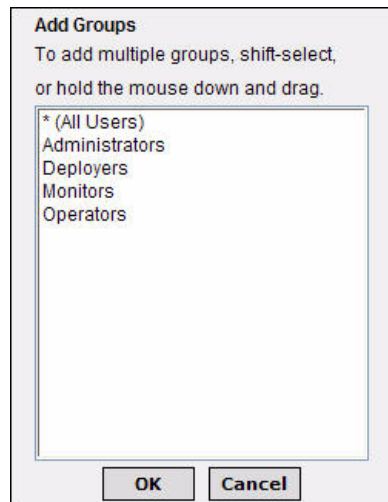
**Write** Users/group members can edit the RDL file.

**Run** Users/group members can run a report.

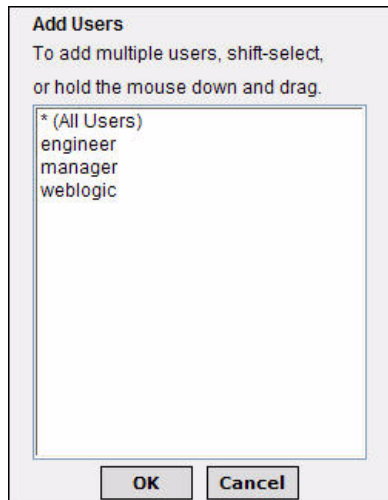
**Schedule** Users/group members can schedule a report.

**Ad Hoc** Users/group members can create a new report using the current report as the starting point.

- 3 Click **Submit**. The **Library > Manage** screen opens, showing the updated folder permissions.
- 4 Click **Add Groups...** to add groups. The **Add Groups** dialog box opens.



- 5 Select the groups you want to add and click **OK**. The new groups are shown in the **Grant Permissions To** or the **Exceptions** list.
- 6 Click **Add Users...** to add users. The **Add Users** dialog box opens.



- 7 Select the users you want to add and click **OK**. The new users are shown in the **Grant Permissions To** or the **Exceptions** list.
- 8 To delete a group or user, select the group or user and click **Delete**. The group or user is removed from the **Grant Permissions To** or the **Exceptions** list.

## Uploading Files

- 1 In the Library, select the folder that you want to upload a file to.
- 2 Click **Upload**. The **Upload** screen opens.

Library > Upload

Upload New File

Destination: /User Scopes

Name:

Description:

File type: Report

Source File:  Browse...

Publish on upload

Upload File Cancel

- 3 Type the name of the file in the **Name** field.
- 4 Optionally, type a description in the **Description** field.
- 5 Select a file type from the **File Type** drop-down list.
- 6 Type a path or click **Browse** to specify the location of the source file in the **Source File** field.
- 7 Select the **Publish on upload** check box to publish the report when you upload the file.
- 8 Click **Upload File**. The report is shown in the **Contents of** panel of the Report Center.

## Managing Reports

You manage reports in the **Contents of** panel. Select the folder containing the report and select the report in the right-hand panel.

**Figure 12 Contents Of Panel**

Contents of: /Select Audit Reports						
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	File Name	Profile	Description	Type	Date	
<input checked="" type="checkbox"/>	Account Change Report			Report	06/19/2006 14:16:21	
<input checked="" type="checkbox"/>	Account Change Report - saved result			Saved Results	06/23/2006 11:42:24	
<input checked="" type="checkbox"/>	Account Change Report_1150746471528			html	06/19/2006 15:47:57	
<input checked="" type="checkbox"/>	Account Change Report_1150811672614			html	06/20/2006 09:54:34	
<input checked="" type="checkbox"/>	Account Change Report_1151079180664			html	06/23/2006 12:13:02	
<input checked="" type="checkbox"/>	Account Change Report_1151096583604			html	06/23/2006 17:03:05	
<input checked="" type="checkbox"/>	Account Events Report			Report	06/19/2006 14:16:23	
<input checked="" type="checkbox"/>	Administrator Report			Report	06/19/2006 14:16:25	
<input checked="" type="checkbox"/>	Administrator Report_1150812000794			html	06/20/2006 10:00:02	
<input checked="" type="checkbox"/>	Administrator Report_1150898400704			html	06/21/2006 10:00:02	
<input checked="" type="checkbox"/>	Attestation Report			Report	06/19/2006 14:16:26	
<input checked="" type="checkbox"/>	Change History Report			Report	06/19/2006 14:16:28	
<input checked="" type="checkbox"/>	Configuration Report			Report	06/19/2006 14:16:30	
<input checked="" type="checkbox"/>	Data Integrity Report			Report	06/19/2006 14:16:31	

The buttons at the top of the **Contents of** panel are described in [Table 10](#).

**Table 10 Report Buttons**

Button	Description
<b>Run</b>	Generates the report from the file.
<b>Publish</b>	Publishes the report. If the report has already been published, this button is grayed out.
<b>Ad Hoc</b>	Creates a new report using the Ad Hoc Wizard. Refer to <a href="#">Running the Ad Hoc Wizard</a> on page 105 for more information about using the Ad Hoc Wizard.
<b>Schedule</b>	Used to create and manage a schedule for automatically generating reports.
<b>Add To My Reports</b>	Adds the file to a list of frequently-used files.
<b>Properties</b>	Used to view file properties and performance statistics, and modify scheduling and permissions.
<b>Delete</b>	Deletes the report file from the Library.


### To run a report


Select a report and click **Run**. The report opens in a new window.


- ▶ You can also run a report by hovering the mouse over the **Run** button and selecting the output format you want.

## To publish a report

- 1 Select an unpublished report and click **Publish**.

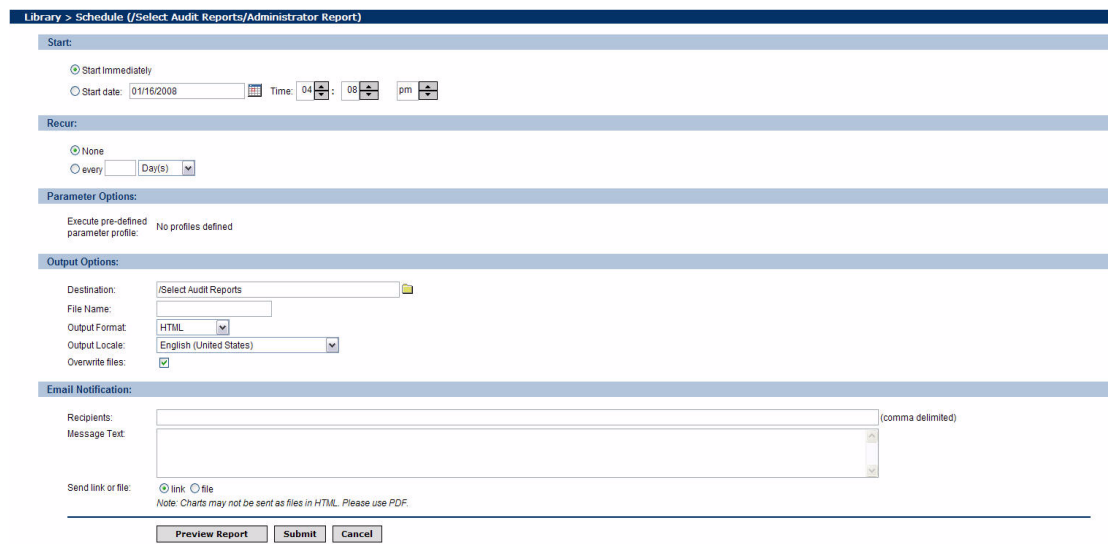
▶ Unpublished reports do not have the  icon beside the report name in the **Contents of** panel.

The published icon  is shown beside the report.

- 2 To unpublish a report, select the report and then click **Properties**. The **Properties** screen opens.
- 3 Click **Unpublish** in the Publish section. The status changes to unpublished and the  icon is no longer shown beside the report name in the **Contents of** panel.

## To schedule report execution

- 1 Select a report and click **Schedule**. The **Library > Schedule** screen opens.



You can schedule a report, specify the output destination and format, and send email alerts to specified recipients.


- 2 Enter information for the following sections:


**Start** Schedule a report to start immediately, or specify a date and time.

**Recur** Select the frequency. Possible values are Minutes, Hours, Weeks, Days and Months.

**Parameter Options** Displays predefined parameter profiles.

- Start** Schedule a report to start immediately, or specify a date and time.
- End** Specify a date and time or number of occurrences.  
**Note:** This options is only active if you specify values for Recur.
- Output Options**
- Specify a destination folder.
  - Choose a file name.
  - Select an output format: HTML, XML, PDF, CSV or Excel.
  - Select and output locale.
  - Select the **Overwrite files** check box if you want new scheduled output to override the old.
- Email Notifications** Type one or more email addresses to receive email alerts, and specify whether to send the output as a link or as an attached file.

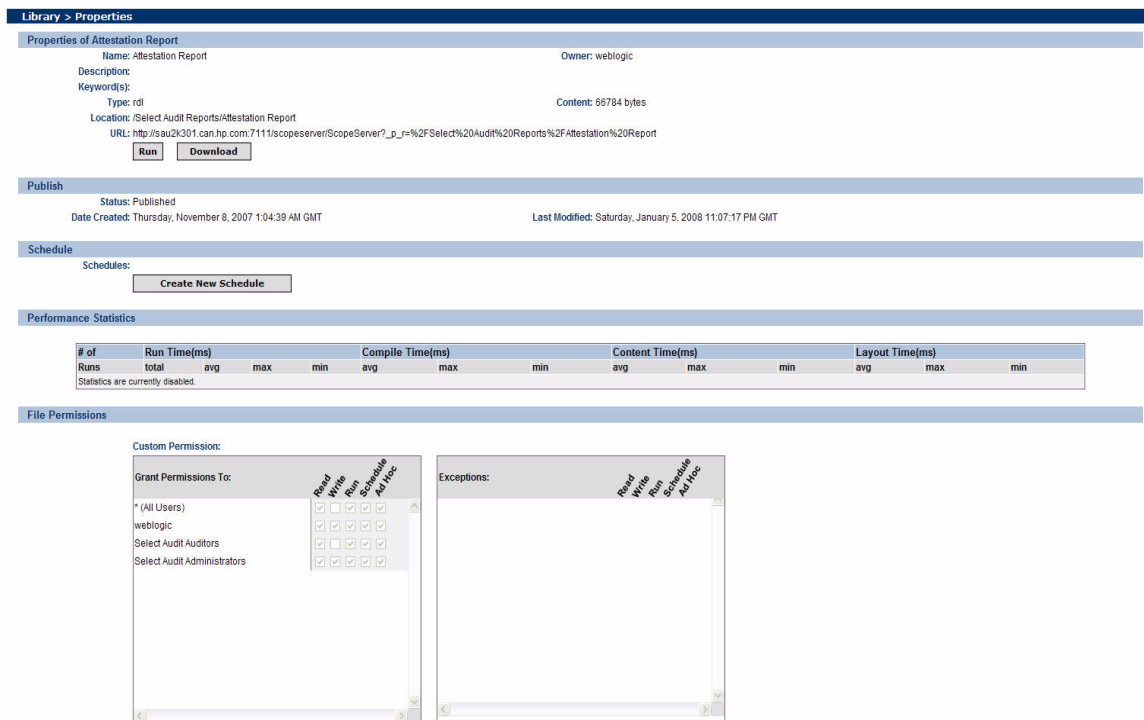
3 Click **Submit**. The  icon is shown beside the report name in the **Contents of** panel to indicate a schedule is set for the report.

 You can view the schedule by clicking **View Schedules** on the **Admin Dashboard**.

## To check report properties

Select a report and click **Properties**. The **Library > Properties** screen opens.

**Figure 13 Library > Properties Screen**



**Library > Properties**

**Properties of Attestation Report**

Name: Attestation Report Owner: weblogic  
 Description:  
 Keyword(s):  
 Type: rdl Content: 65784 bytes  
 Location: /Select Audit Reports/Attestation Report  
 URL: http://sau2k301.can.hp.com:7111/scopeserver/ScopeServer?p\_=%2FSelect%20Audit%20Reports%2FAttestation%20Report  
 Run Download

**Publish**

Status: Published  
 Date Created: Thursday, November 8, 2007 1:04:39 AM GMT  
 Last Modified: Saturday, January 5, 2008 11:07:17 PM GMT

**Schedule**

Schedules:  
 Create New Schedule

**Performance Statistics**

# of Runs	Run Time(ms)			Compile Time(ms)			Content Time(ms)			Layout Time(ms)		
	total	avg	max	min	avg	max	min	avg	max	min	avg	max
Statistics are currently disabled.												

**File Permissions**

Custom Permission:

Grant Permissions To:

	Read	Write	Run	Schedule	Full Proc
*(All Users)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
weblogic	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select Audit Auditors	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Select Audit Administrators	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Exceptions:

	Read	Write	Run	Schedule	Full Proc
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>



The **Properties** screen enables you to run and download reports. The sections of the screen are described in [Table 11](#).

**Table 11 Properties Screen Sections**

Section	Description
<b>Properties &lt;report name&gt;</b>	Lists the selected report's properties. It contains the following buttons: <ul style="list-style-type: none"><li>• <b>Run</b> runs the report.</li><li>• <b>Download</b> opens a dialog box to download the file to a different location.</li></ul>
<b>Publish</b>	Indicates the Status and Date Published. To unpublish report, click <b>Unpublish</b> .
<b>Schedule</b>	Allows you to create a new schedule for the report.
<b>Performance Statistics</b>	Lists the following statistics: <ul style="list-style-type: none"><li>• The number of report runs.</li><li>• The time taken to run.</li><li>• The time taken to compile.</li><li>• The time taken to build content.</li><li>• The time taken to create layout.</li></ul> You turn on Performance Statistics using the Admin Dashboard. See <a href="#">Configuring the Report Server</a> on page 89 for more information.
<b>File Permissions</b>	Shows the existing file permissions. Click <b>Edit Permissions</b> to change the file permissions.

## Running the Ad Hoc Wizard

You can create and modify report layouts using the **Ad Hoc** Wizard. The Ad Hoc Wizard is a browser-based tool that lets you design layouts for your own reports. Any report in the Library with Ad Hoc permission can be used to launch the Ad Hoc Wizard.

The Ad Hoc Wizard leads you through a series of steps to create the desired layout. You can move back and forth between steps or jump directly to the desired step. You can save the report or preview it in its current state at any point in the wizard.

The Ad Hoc Wizard is used to fashion tabular or graphic layouts using the information that the developer puts in a report. If the report contains parameters, the report developer can use the Report Center to make the Ad Hoc Wizard use different labels or parameter mappings for the report.

For more information on configuring the Ad Hoc Wizard, see the *HP Select Audit 1.02 Report Center User's Guide*.

## Changing the Date Format for Ad Hoc Reports

The default date format for reports created using the Ad Hoc Wizard is `mm/dd/yyyy` (U.S. format). You can change the date format to the international standard sortable date format `yyyy/mm/dd` (`yyyy-mm-dd`).

The `defaultscope.xml` file in the `scopeserver/WEB-INF/conf` directory contains all the default settings for Ad Hoc reports. The property that controls the date format is `dateFormat` and the value is empty by default. This means that the date will be shown in the Java default date format. For the syntax of the property's value, please refer to the Java documentation for class `java.text.SimpleDateFormat`.

### To change the date format

- 1 In the `scopeserver/WEB-INF/conf` directory, open the `defaultscope.xml` file.
- 2 Find the following line in `defaultscope.xml`.

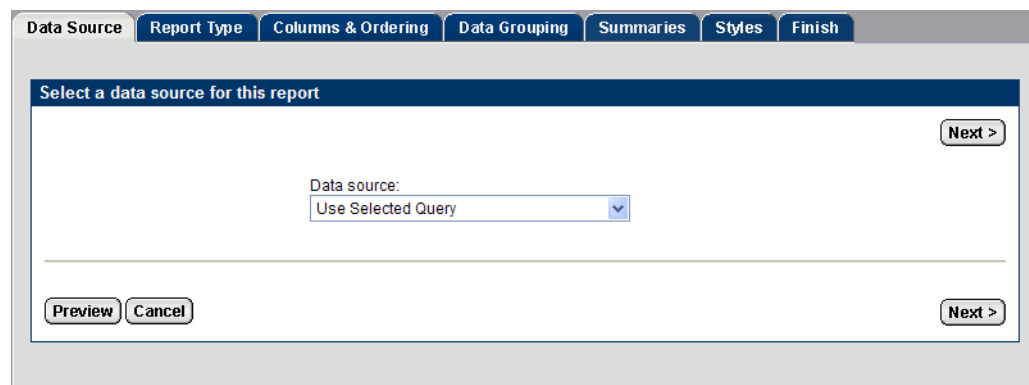
```
<Property name="dateFormat"></Property>
```
- 3 Set the required format in this line. For example, to make the date appear in a standard format, use the following line:

```
<Property name="dateFormat">yyyy-MM-dd HH:mm:ss Z</Property>
```

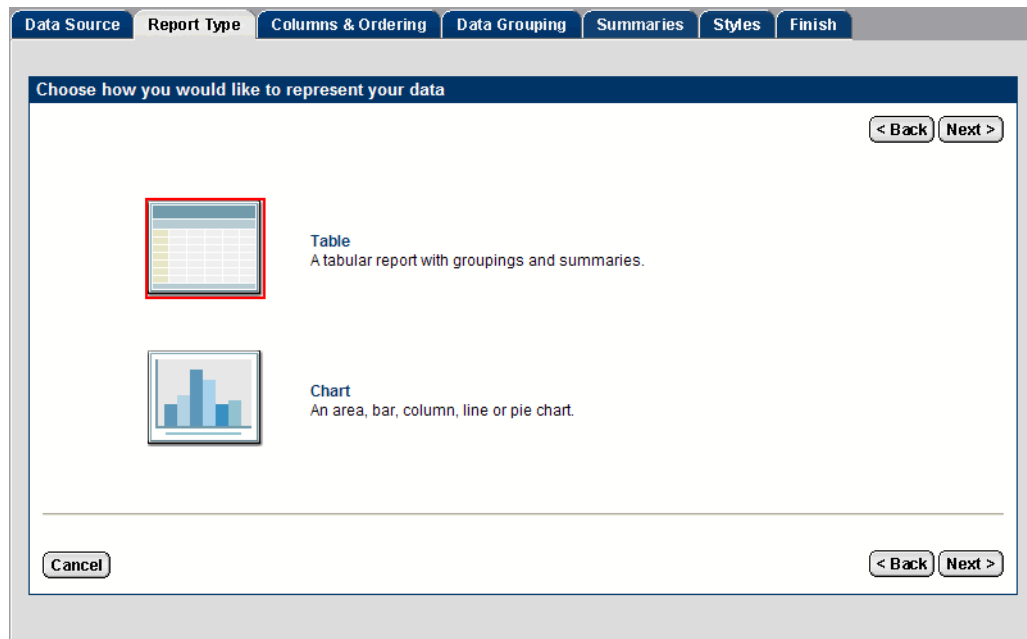
This will render the date and time as `2006-06-25 16:30:47 -0400`.
- 4 Restart the Report server after modifying the `defaultscope.xml` file.

## Creating a Tabular Report

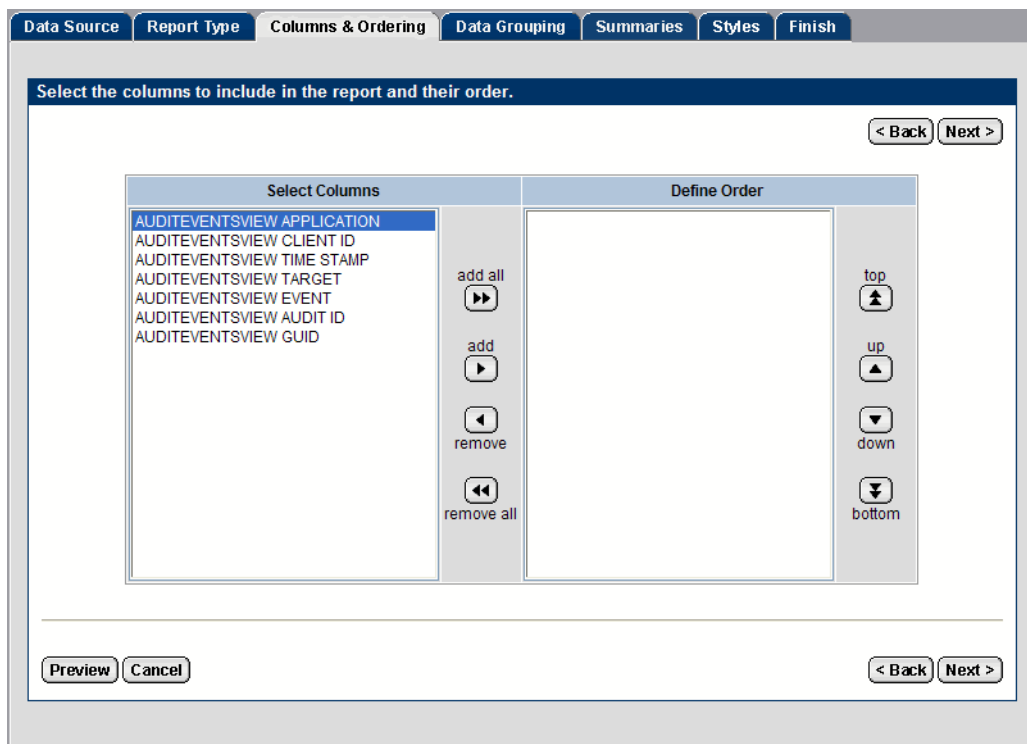
- 1 Select the report in the Library or My Reports view and then click **Ad Hoc**. The Ad Hoc Wizard opens showing the **Data Source** tab.



- 2 Select data for the report from the **Data source** drop-down list:
  - Select **Use selected report** to use the first data block from an existing report. You must select a report before you launch the Ad Hoc Wizard.
  - Select a query name from the Catalog. All queries that reside under **Catalog > Queries** are available for selection. This option does not require you do a prior selection of an existing report.
- 3 Click **Next**. The **Report Type** screen opens.



- 4 Select **Table** and click **Next**. The **Columns and Ordering** screen opens.



- 5 Select the columns you want to include in the report and use the **Up** and **Down** arrows to define the order of the columns.
- 6 Click **Next**. The **Data Grouping** screen opens.

Select each level of data grouping.

Group by (optional):

then by (optional):

then by (optional):

Preview Cancel < Back Next >

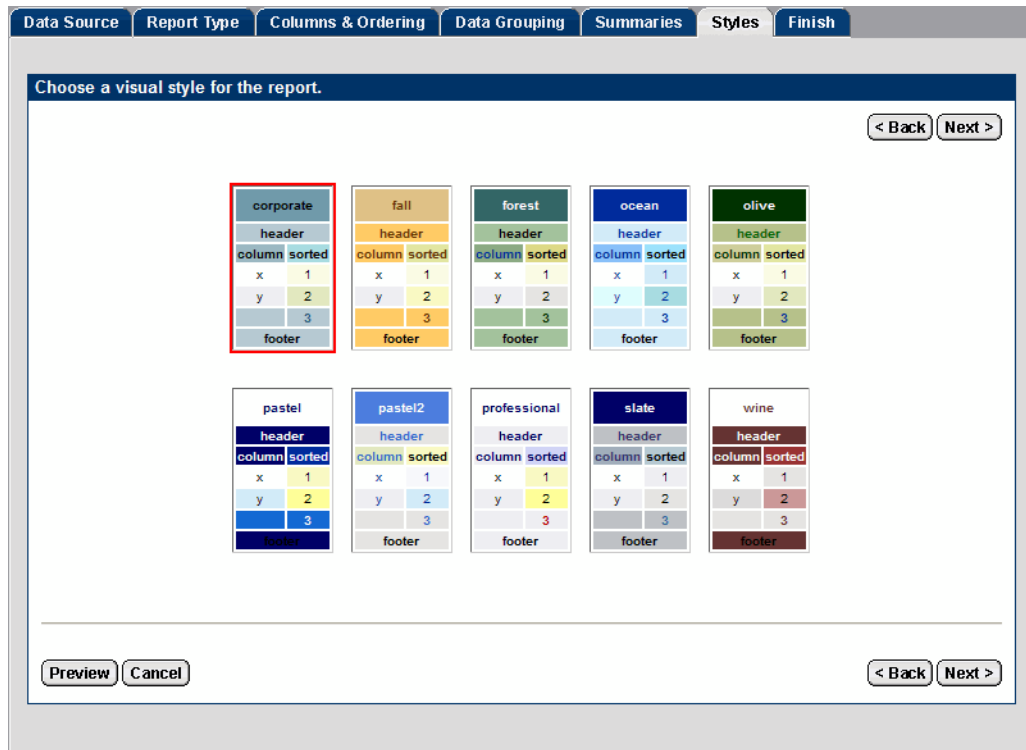
- Optionally, select how you would like the report data grouped and click **Next**. The **Summaries** screen opens.

Apply aggregate functions to columns. (optional)

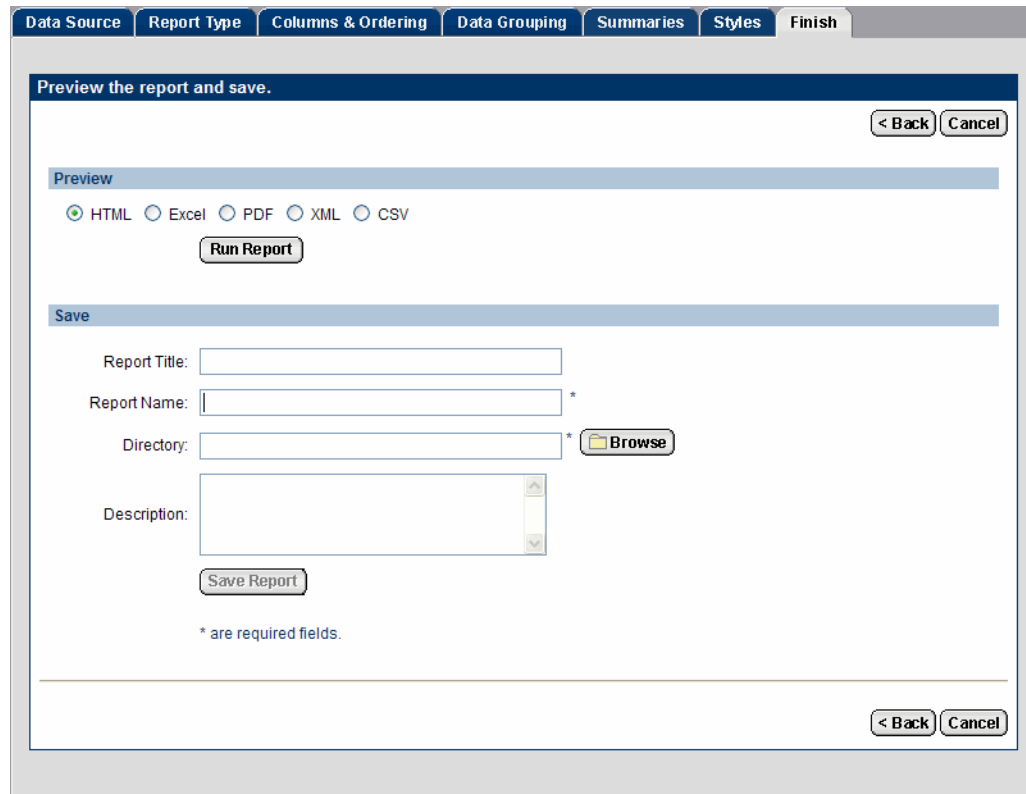
Column	Column Mask	Aggregate Function
AUDITEVENTSVIEW_CLIENT_ID		
AUDITEVENTSVIEW_TIME_STAMP		
AUDITEVENTSVIEW_APPLICATION		

Preview Cancel < Back Next >

- Optionally, select an aggregate function for the column and click **Next**. The **Styles** screen opens.



- 9 Select a style for the report and click **Next**. The **Finish** screen opens.

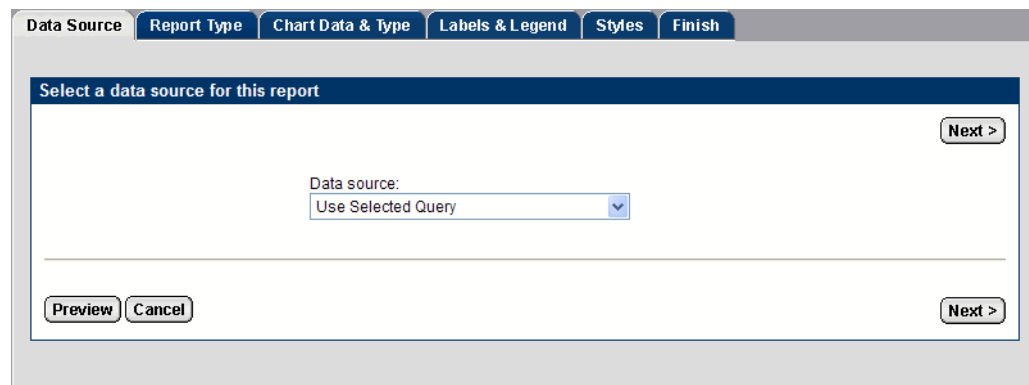


- 10 Select a report format and click **Run Report** to preview the report.

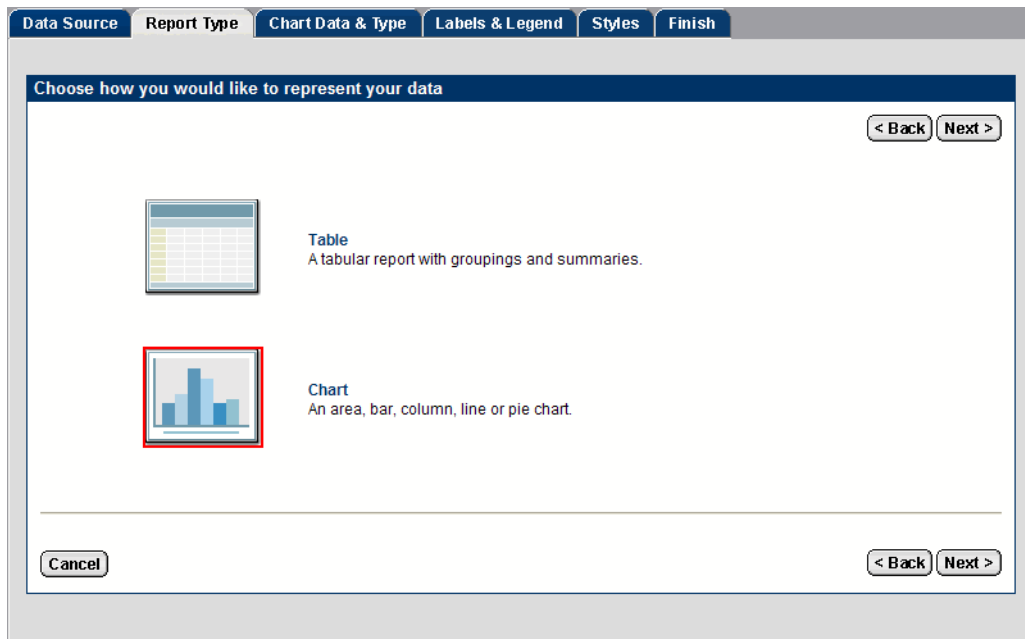
- 11 Type a **Report Title**, **Report Name**, **Directory** and **Description** for the report in the corresponding fields.
  - ▶ Report names cannot include a combination of blank spaces and the “+” character. The Report server will not recognize this combination.
  - ▶ Click **Browse** to select the directory where you want to save the report.
- 12 Click **Save Report**. The Ad Hoc Wizard opens a confirmation message when the report has been saved.
- 13 Click **Close**. The Ad Hoc Wizard closes and the new report is listed in the directory you saved it to.

## Creating a Chart

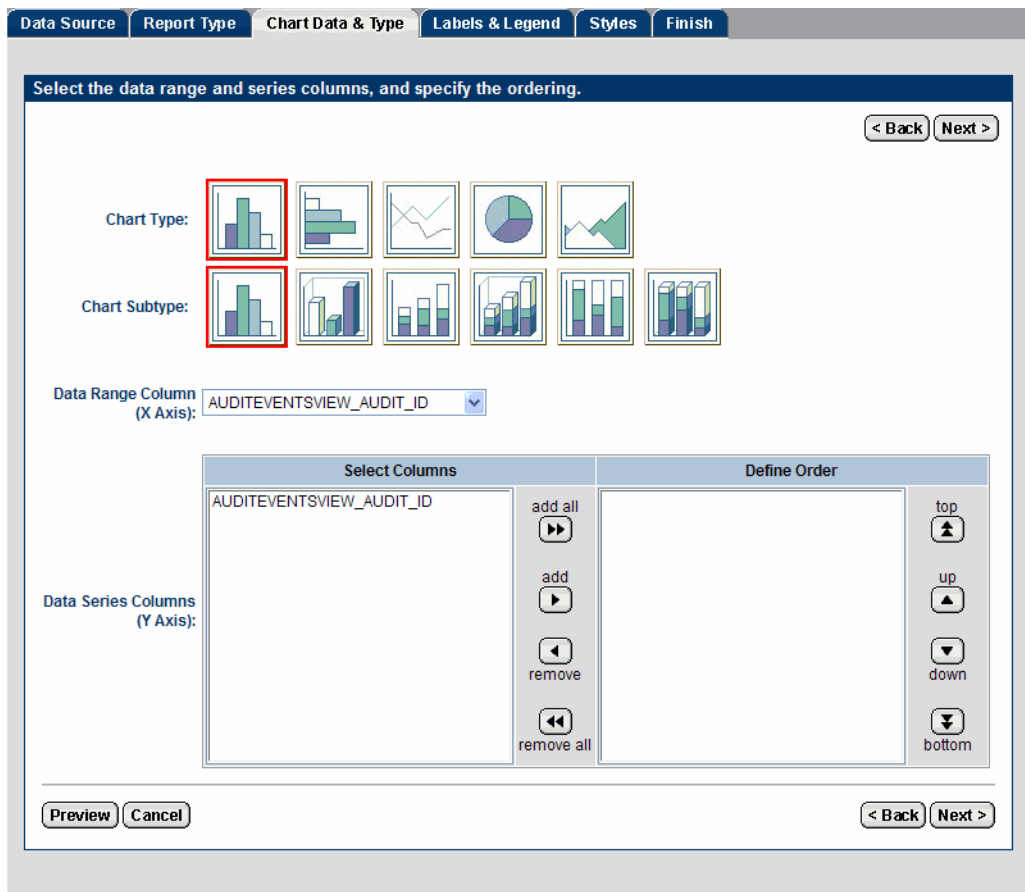
- 1 Select the report in the Library or My Reports view and then click **Ad Hoc**. The Ad Hoc Wizard opens showing the **Data Source** tab.



- 2 Select data for the report from the **Data source** drop-down list:
  - Select **Use selected report** to use the first data block from an existing report. You must select a report before you launch the Ad Hoc Wizard.
  - Select a query name from the Catalog. All queries that reside under **Catalog > Queries** are available for selection. This option does not require you to the prior selection of an existing report.
- 3 Click **Next**. The **Report Type** screen opens.

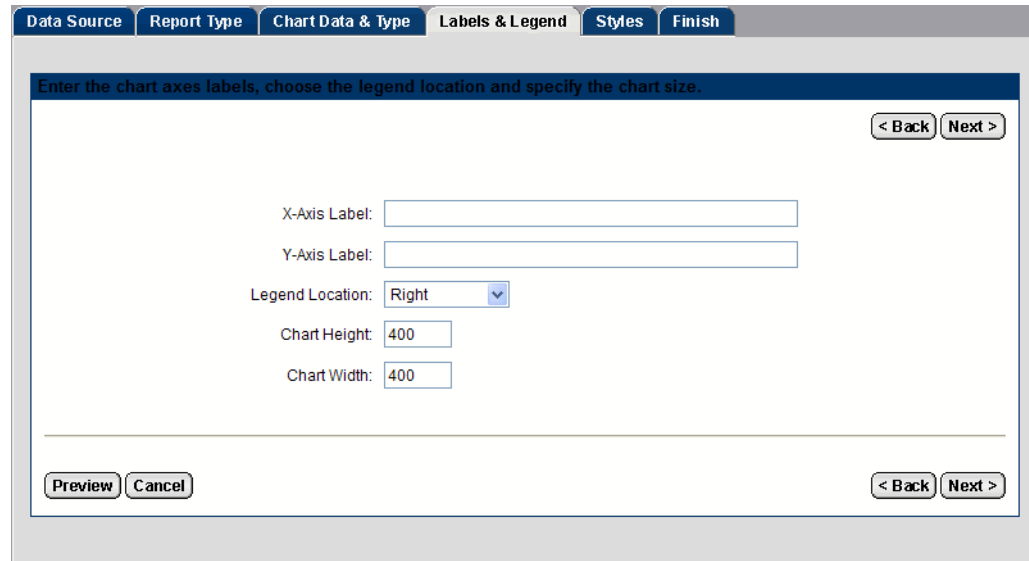


- 4 Select **Chart** and click **Next**. The **Chart Data & Type** screen opens.



- 5 Select the following:
  - **Chart Type** and **Subtype**
  - **Data Range Column**
  - **Data Series Columns**

▶ Use the **Up** and **Down** arrows to define the order of the columns.
- 6 Click **Next**. The **Labels & Legend** screen opens.



Enter the chart axes labels, choose the legend location and specify the chart size.

< Back Next >

X-Axis Label:

Y-Axis Label:

Legend Location: Right

Chart Height:

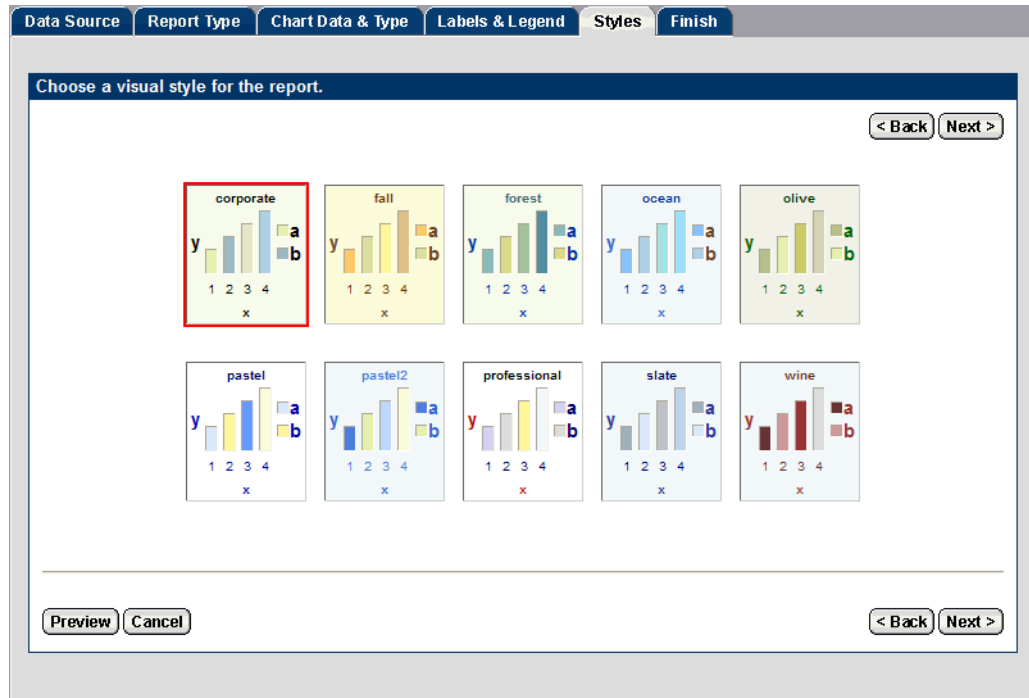
Chart Width:

Preview Cancel

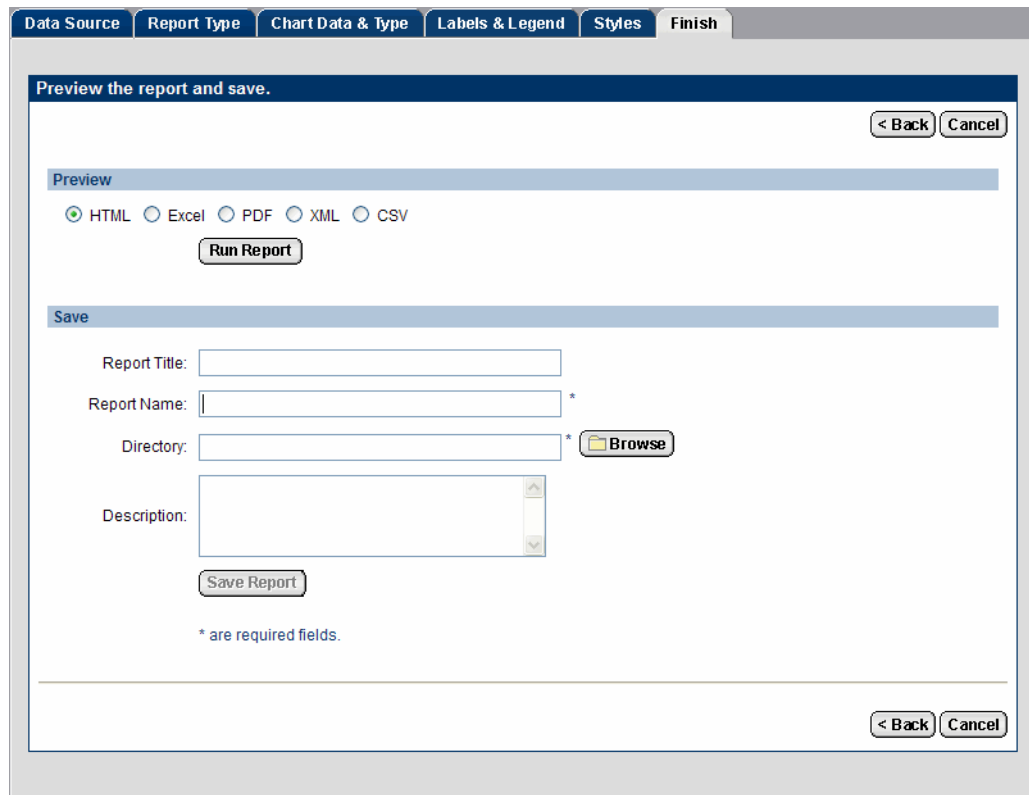
< Back Next >

- 7 Do the following:
  - Type an **X Axis Label**.
  - Type a **Y Axis Label**.
  - Select a location for the legend from the **Legend Location** drop-down list.
  - Type the **Chart Height**.
  - Type the **Chart Width**.
- 8 Click **Next**. The **Styles** screen opens.





- 9 Select a style for the chart and click **Next**. The **Finish** screen opens.



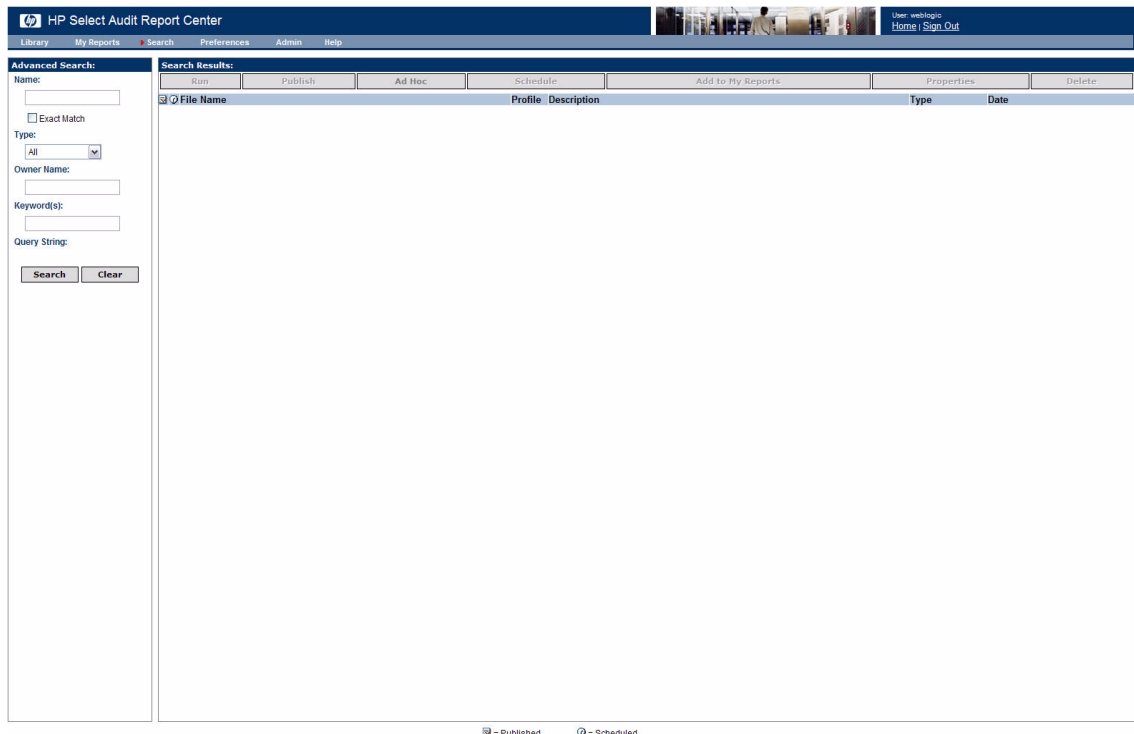
- 10 Select a format and click **Run Report** to preview the chart.

- 11 Type a **Report Title**, **Report Name**, **Directory** and **Description** for the chart in the corresponding fields.
  - Report names cannot include a combination of blank spaces and the “+” character. The Report server will not recognize this combination.
  - Click **Browse** to select the directory where you want to save the chart.
- 12 Click **Save Report**. The Ad Hoc Wizard shows a confirmation message when the chart has been saved.
- 13 Click **Close**. The Ad Hoc Wizard closes and the new chart is listed in the directory you saved it to.

## Searching for Reports

The **Search** screen helps you find a report or other Library file without browsing through the Library hierarchy.

**Figure 14 Search Screen**



Like the Library screen, the Search screen, has two panels. The **Advanced Search** panel contains the fields that define your search criteria and the **Search Results** panel contains any matching Library files.

If you enter values in multiple fields in the **Advanced Search** pane, all fields must match the file’s metadata for the search to succeed. Once you have filled in all the fields, click **Search** to begin the search. To clear the fields, click **Clear**.

## To search for a report

- 1 Click **Search**. The **Search** screen opens.
- 2 In the **Advanced Search** panel, complete any of the fields as follows:

<b>Name</b>	Type the name of the report that you are searching for.
<b>Type</b>	Select whether you are looking for report files ( <b>Report</b> ), already-run scheduled static output ( <b>Output</b> ), interactive views of static data ( <b>Saved Results</b> ), or all files ( <b>all</b> ).
<b>Owner Name</b>	Type the name of the file's owner.
<b>Keyword(s)</b>	Type any number of keywords associated with the report that you are looking for.
<b>Query String</b>	Type a string to filter the returned reports.

- 3 Click **Search**. Any matching reports are shown in the **Search Results** panel.

For more information about searching for reports, refer to the *HP Select Audit 1.02 Report Center User's Guide*.

## To search for data in a report

You can search within a given report for specific data.

- 1 Click **Reports** → **Library**.
- 2 Double-click the report you want to search. The report opens in a new browser window.

### User Activity Report

Please select a profile:

Application Types:

Actions:

Start Time (e.g. 2005-01-01 00:00:00):

End Time (e.g. 2005-12-31 23:59:59):

User:

Target:

User Activities				
Time	User	Action	Target	Application
October 11, 2006 5:08:28 PM GMT-04:00	<anonymous>	<a href="#">Workflow Report Approval</a>	Account Change Report	Select Audit Workflow
October 11, 2006 5:06:33 PM GMT-04:00	<anonymous>	<a href="#">Workflow Report Approval</a>	Account Change Report	Select Audit Workflow
October 11, 2006 2:13:13 PM GMT-04:00	weblogic	<a href="#">Workflow Report Approval</a>	System Status Report	Select Audit Workflow
October 11, 2006 2:12:13 PM GMT-04:00	weblogic	<a href="#">Workflow Report Approval</a>	System Status Report	Select Audit Workflow
October 11, 2006 2:11:13 PM GMT-04:00	weblogic	<a href="#">Workflow Report Approval</a>	System Status Report	Select Audit Workflow
October 11, 2006 2:10:17 PM GMT-04:00	weblogic	<a href="#">Workflow Report Approval</a>	System Status Report	Select Audit Workflow
October 11, 2006 1:59:15 PM GMT-04:00	<anonymous>	<a href="#">Workflow Report Approval</a>	Data Integrity Report	Select Audit Workflow
October 11, 2006 1:57:20 PM GMT-04:00	<anonymous>	<a href="#">Workflow Report Approval</a>	Data Integrity Report	Select Audit Workflow

- 3 Type the search criteria and click **Search**. The results are shown in the **Report** window.

## User Activity Report

Please select a profile:

Application Types:

Actions:

Start Time (e.g. 2005-01-01 00:00:00):

End Time (e.g. 2005-12-31 23:59:59):

User:

Target:

User Activities				
Time	User	Action	Target	Application
October 10, 2006 1:14:04 AM GMT-04:00	admin;16.157.55.9	<a href="#">Partner delete</a>	alvafish - SP	http://ivory.chn.hp.com:8000/tfs
October 10, 2006 1:07:49 AM GMT-04:00	admin;16.157.55.9	<a href="#">Partner add</a>	alvafish - SP	http://ivory.chn.hp.com:8000/tfs
October 10, 2006 1:06:45 AM GMT-04:00	admin;16.157.55.9	<a href="#">Admin Logged in</a>		http://ivory.chn.hp.com:8000/tfs
October 9, 2006 11:24:24 PM GMT-04:00	admin;16.157.55.9	<a href="#">Admin Logged in</a>		http://ivory.chn.hp.com:8000/tfs
October 9, 2006 11:24:18 PM GMT-04:00	admin;16.157.55.9	<a href="#">Admin Login Error</a>		http://ivory.chn.hp.com:8000/tfs

You can specify an exact value or use wild cards when searching on text field. Two wildcards can be used for searching, “%” and “\_”. “%” represents 0 to an unlimited number of characters. “\_” represents a single character. The wildcards can be placed anywhere in the search text, and can be used multiple times. For example: %User%, s\_User%, S%User, %User, User%.

## User Activity Report

Please select a profile:

Application Types:

Actions:

Start Time (e.g. 2005-01-01 00:00:00):

End Time (e.g. 2005-12-31 23:59:59):

User:

Target:

User Activities				
Time	User	Action	Target	Application
October 10, 2006 1:14:04 AM GMT-04:00	admin;16.157.55.9	<a href="#">Partner delete</a>	alvafish - SP	http://ivory.chn.hp.com:8000/tfs
October 10, 2006 1:07:49 AM GMT-04:00	admin;16.157.55.9	<a href="#">Partner add</a>	alvafish - SP	http://ivory.chn.hp.com:8000/tfs
October 10, 2006 1:06:45 AM GMT-04:00	admin;16.157.55.9	<a href="#">Admin Logged in</a>		http://ivory.chn.hp.com:8000/tfs
October 9, 2006 11:24:24 PM GMT-04:00	admin;16.157.55.9	<a href="#">Admin Logged in</a>		http://ivory.chn.hp.com:8000/tfs
October 9, 2006 11:24:18 PM GMT-04:00	admin;16.157.55.9	<a href="#">Admin Login Error</a>		http://ivory.chn.hp.com:8000/tfs

## Setting Preferences

You use the **Preferences** screen to set or change your home directory in the Library or your start page (the view that will be shown when you launch the Report Center).



Library is the default start page.

- 1 Click **Preferences**. The **Preferences** screen opens.



- 2 Type the directory path in the **Home Directory** field.
- 3 Select a page from the **Start Page** drop-down list and click **Set**.
- 4 Log out of the Audit Portal and log in again to see the new view.

## Editing Report Schedules

You can edit report schedules and properties using the **View Report Schedules** menu item.

- 1 Select **Administration** → **View Report Schedules**. The **Schedules** screen in the Report Center opens.



- 2 To edit the report's properties:
  - a Click the **Report Name**. You can make any changes to the report properties from this screen.
  - b Click the Browser **Back** button to return to the **Schedules** screen.
- 3 To change the report schedule:
  - a Click **Edit**. The **Schedule** screen opens.
  - b Make the changes and click **Submit** to return to the **Schedules** screen.
- 4 To remove a schedule:
  - a Click **Delete**. A confirmation box opens.
  - b Click **Yes** to remove the schedule.



# A Select Identity/Select Audit Data Filtering

This appendix contains a table listing how Select Identity report type permissions are mapped in Select Audit.

**Table 12 Select Identity Event Filtering**

Report Type Assigned in SI	Events Viewable in Select Audit		
	Audit Event Name	Application	Component Event Name
Audit User	Sent Login request	Select Federation	SF Protocol Sent Login Request
Audit User	Sent Logout request	Select Federation	SF Protocol Sent Logout Request
Audit User	Received Login request	Select Federation	SF Protocol Received Login Request
Audit User	Received Login request	Select Federation	SF Protocol Received Logout Request
Audit User	Received Logout request	Select Federation	SF API Received logout request
Audit User	Logged In	Select Access	Login
Audit User	Logged In	Select Identity	SI login
Audit User	Logged In	Select Federation	SF Internal Logged In
Audit User	Logged Out	Select Access	Logout
Audit User	Logged Out	Select Identity	SI logout
Audit User	Logged Out	Select Federation	SF Internal Logged Out
Audit User	Login Error	Select Access	Login error
Audit User	Login Error	Select Federation	SF Internal Login Error
Audit User	Admin Logged In	Select Access	Admin Login
Audit User	Admin Logged In	Select Access	Delegate Admin Login
Audit User	Admin Logged In	Select Federation	SF Admin Logged In
Audit User	Admin Logged Out	Select Access	Admin Logout
Audit User	Admin Logged Out	Select Access	Delegate Admin Logout
Audit User	Admin Logged Out	Select Federation	SF Admin Logged Out
Audit User	Admin Login Error	Select Access	Admin Login error

**Table 12 Select Identity Event Filtering (cont'd)**

Report Type Assigned in SI	Events Viewable in Select Audit		
	Audit Event Name	Application	Component Event Name
Audit User	Admin Login Error	Select Access	Delegate Admin Login error
Audit User	Admin Login Error	Select Federation	SF Admin Login Error
Audit User	Credential expire	Select Access	Credential expire
Audit User	User Authenticated	Select Federation	SF Internal User Authenticated
Audit User	User Authentication Error	Select Federation	SF Internal User Authentication Error
Audit User	Access Allow	Select Access	Allow
Audit User	Access Deny	Select Access	Deny
Audit User	Reset Password	Select Identity	SI Reset Password
Audit User	Change Password	Select Identity	SI Change Password
Audit User	Change Password	Select Federation	SF AdminAdm Password Changed
Audit User	Error Changing Password	Select Federation	SF AdminAdm Error Changing Password
Audit User	Forget Password	Select Identity	SI Forget Password
Audit User	Expire Password Notification	Select Identity	SI Expire Password Notification
Audit User	Expire Password	Select Identity	SI Expire Password
Audit User	Hint Setup	Select Identity	SI Hint Setup
Audit User	Password Policy change	Select Access	passwordPolicyChange
Audit User	Password Reset Config Change	Select Access	password Reset Config Change
Audit User	User Add	Select Access	UserAdd
Audit User	User Add	Select Identity	SI Add NewUser
Audit User	User Delete	Select Access	UserDelete
Audit User	User Change	Select Access	UserChange
Audit User	User Change	Select Identity	SI Modify user
Audit User	Terminate User	Select Identity	SI Terminate User
Audit User	Modify Profile	Select Identity	SI Modify Profile
Audit User	Manage User Expiration	Select Identity	SI Manage User Expiration



**Table 12 Select Identity Event Filtering (cont'd)**

Report Type Assigned in SI	Events Viewable in Select Audit		
	Audit Event Name	Application	Component Event Name
Audit User	Move User	Select Identity	SI Move User
Audit User	disable before terminate	Select Identity	SI disable before terminate
Audit User	Added Admin	Select Federation	SF AdminAdm Added Admin
Audit User	Deleted Admin	Select Federation	SF AdminAdm Deleted Admin
Audit User	User Consented	Select Federation	SF User Consented
Audit User	Copy User	Select Identity	SI Copy User
Audit User	User Source Add	Select Access	userSourceAdd
Audit User	User Source Delete	Select Access	userSourceDelete
Audit User	User Source Change	Select Access	userSourceChange
Audit User	Security Violation	Select Identity	SI Security Violation
Audit User	Group Add	Select Access	GroupAdd
Audit User	Group Delete	Select Access	GroupDelete
Audit User	Group Change	Select Access	GroupChange
Audit User	User Role Add	Select Access	UserRoleAdd
Audit User	User Role Delete	Select Access	UserRoleDelete
Audit User	User Role Change	Select Access	UserRoleChange
Audit User	Admin Role Add	Select Identity	SI Admin role create
Audit User	Admin Role Delete	Select Identity	SI Admin role delete
Audit User	Admin Role Change	Select Identity	SI Admin role modify
Audit User	User role delegation Activate	Select Identity	SI User Role Delegation Activate
Audit User	User role delegation Deactivate	Select Identity	SI User Role Delegation Deactivate
Audit User	Folder Add	Select Access	FolderAdd
Audit User	Folder Delete	Select Access	FolderDelete
Audit User	Folder Change	Select Access	FolderChange
Audit User	Authn Add	Select Access	authnAdd
Audit User	Authn Delete	Select Access	authnDelete
Audit User	Authn Change	Select Access	authnChange

**Table 12 Select Identity Event Filtering (cont'd)**

Report Type Assigned in SI	Events Viewable in Select Audit		
	Audit Event Name	Application	Component Event Name
Audit User	Delegate delegated	Select Access	delegate delegate
Audit User	Delegate undelegate	Select Access	delegate undelegate
Audit User	Delegate inherit	Select Access	delegate inherit
Audit User	Delegate Change	Select Access	delegateChange
Audit User	WorkflowConfigChange	Select Access	WorkflowConfigChange
Audit User	WorkflowChangeRequest submitted	Select Access	WorkflowChangeRequest submitted
Audit User	WorkflowChangeRequest approved	Select Access	WorkflowChangeRequest approved
Audit User	WorkflowChangeRequest rejected	Select Access	WorkflowChangeRequest rejected
Audit User	WorkflowChangeRequest reverted	Select Access	WorkflowChangeRequest reverted
Audit User			
Audit User	Workflow create	Select Identity	SI workflow create
Audit User	Workflow delete	Select Identity	SI workflow delete
Audit User	Workflow modify	Select Identity	SI workflow modify
Audit User	Workflow view	Select Identity	SI workflow view
Audit User	Workflow copy	Select Identity	SI workflow copy
Audit User	Workflow import	Select Identity	SI workflow import
Audit User	Workflow export	Select Identity	SI workflow export
Audit User	Enable Service Membership	Select Identity	SI Enable Service Membership
Audit User	Disable Service Membership	Select Identity	SI Disable Service Membership
Audit User	Enable All Services	Select Identity	SI Enable All Services
Audit User	View resource attribute	Select Identity	SI View resource attribute
Audit User	View attribute	Select Identity	SI View attribute
Audit User	activeAttributes	Select Access	activeAttributes
Audit User	User Federated	Select Federation	SF Internal User Federated

**Table 12 Select Identity Event Filtering (cont'd)**

Report Type Assigned in SI	Events Viewable in Select Audit		
	Audit Event Name	Application	Component Event Name
Audit User	User Federation Error	Select Federation	SF Internal User Federation Error
Audit User	View Service Membership	Select Identity	SI View Service Membership
Audit User	Ignore Add	Select Identity	SI Ignore Add
Audit User	Ignore Modify	Select Identity	SI Ignore Modify
Audit User	Ignore Delete	Select Identity	SI Ignore Delete
Audit Service	WorkflowConfigChange	Select Access	WorkflowConfigChange
Audit Service	WorkflowChangeRequest submitted	Select Access	WorkflowChangeRequest submitted
Audit Service	WorkflowChangeRequest approved	Select Access	WorkflowChangeRequest approved
Audit Service	WorkflowChangeRequest rejected	Select Access	WorkflowChangeRequest rejected
Audit Service	WorkflowChangeRequest reverted	Select Access	WorkflowChangeRequest reverted
Audit Service			
Audit Service	Workflow create	Select Identity	SI workflow create
Audit Service	Workflow delete	Select Identity	SI workflow delete
Audit Service	Workflow modify	Select Identity	SI workflow modify
Audit Service	Workflow view	Select Identity	SI workflow view
Audit Service	Workflow copy	Select Identity	SI workflow copy
Audit Service	Workflow import	Select Identity	SI workflow import
Audit Service	Workflow export	Select Identity	SI workflow export
Audit Service	Add Service	Select Identity	SI Add Service
Audit Service	Create service	Select Identity	SI Create service
Audit Service	Delete service	Select Identity	SI Delete service
Audit Service	Modify service	Select Identity	SI Modify service
Audit Service	Copy service	Select Identity	SI Copy service
Audit Service	Set service attribute values	Select Identity	SI Set service attribute values

**Table 12 Select Identity Event Filtering (cont'd)**

Report Type Assigned in SI	Events Viewable in Select Audit		
	Audit Event Name	Application	Component Event Name
Audit Service	Set service attribute properties	Select Identity	SI Set service attribute properties
Audit Service	Create service view	Select Identity	SI Create service view
Audit Service	Delete service view	Select Identity	SI Delete service view
Audit Service	Modify service view	Select Identity	SI Modify service view
Audit Service	Create service role	Select Identity	SI Create service role
Audit Service	Delete service role	Select Identity	SI Delete service role
Audit Service	Create service context	Select Identity	SI Create service context
Audit Service	Delete service context	Select Identity	SI Delete service context
Audit Service	Modify service context	Select Identity	SI Modify service context
Audit Service	Import service	Select Identity	SI Import service
Audit Service	Modify service role	Select Identity	SI Modify service role
Audit Service	Svc Change Recon Modify User	Select Identity	SI Svc Change Recon Modify User
Audit Service	Svc Change Recon Add resource	Select Identity	SI Svc Change Recon Add resource
Audit Service	Svc Change Recon Delete resource	Select Identity	SI Svc Change Recon Delete resource
Audit Service	Service Export	Select Identity	SI Service Export
Audit Service	Create attribute	Select Identity	SI Create attribute
Audit Service	Delete attribute	Select Identity	SI Delete attribute
Audit Service	Modify attribute	Select Identity	SI Modify attribute
Audit Service	View attribute	Select Identity	SI View attribute
Audit Service	Copy attribute	Select Identity	SI Copy attribute
Audit Service	Attribute import	Select Identity	SI attribute export
Audit User Creation	User Add	Select Access	UserAdd
Audit User Creation	User Add	Select Identity	SI Add NewUser
Audit User Creation	Move User	Select Identity	SI Move User
Audit User Creation	Added Admin	Select Federation	SF AdminAdm Added Admin
Audit User Creation	Copy User	Select Identity	SI Copy User

**Table 12 Select Identity Event Filtering (cont'd)**

Report Type Assigned in SI	Events Viewable in Select Audit		
	Audit Event Name	Application	Component Event Name
Audit User Creation	User Source Add	Select Access	userSourceAdd
Audit User Creation	Group Add	Select Access	GroupAdd
Audit User Creation	User Role Add	Select Access	UserRoleAdd
Audit User Creation	Admin Role Add	Select Identity	SI Admin role create
Audit User Creation	Folder Add	Select Access	FolderAdd
Audit User Creation	Authn Add	Select Access	authnAdd
Audit User Creation	WorkflowConfigChange	Select Access	WorkflowConfigChange
Audit User Creation	WorkflowChangeRequest submitted	Select Access	WorkflowChangeRequest submitted
Audit User Creation	WorkflowChangeRequest approved	Select Access	WorkflowChangeRequest approved
Audit User Creation	WorkflowChangeRequest rejected	Select Access	WorkflowChangeRequest rejected
Audit User Creation	WorkflowChangeRequest reverted	Select Access	WorkflowChangeRequest reverted
Audit User Creation			
Audit User Creation	Workflow create	Select Identity	SI workflow create
Audit User Creation	Workflow delete	Select Identity	SI workflow delete
Audit User Creation	Workflow modify	Select Identity	SI workflow modify
Audit User Creation	Workflow view	Select Identity	SI workflow view
Audit User Creation	Workflow copy	Select Identity	SI workflow copy
Audit User Creation	Workflow import	Select Identity	SI workflow import
Audit User Creation	Workflow export	Select Identity	SI workflow export
Audit User Creation	Enable Service Membership	Select Identity	SI Enable Service Membership
Audit User Creation	Enable All Services	Select Identity	SI Enable All Services
Audit User Deletion	User Delete	Select Access	UserDelete
Audit User Deletion	Move User	Select Identity	SI Move User
Audit User Deletion	Deleted Admin	Select Federation	SF AdminAdm Deleted Admin
Audit User Deletion	User Source Delete	Select Access	userSourceDelete

**Table 12 Select Identity Event Filtering (cont'd)**

Report Type Assigned in SI	Events Viewable in Select Audit		
	Audit Event Name	Application	Component Event Name
Audit User Deletion	Group Delete	Select Access	GroupDelete
Audit User Deletion	User Role Delete	Select Access	UserRoleDelete
Audit User Deletion	Admin Role Delete	Select Identity	SI Admin role delete
Audit User Deletion	Folder Delete	Select Access	FolderDelete
Audit User Deletion	Authn Delete	Select Access	authnDelete
Audit User Deletion	WorkflowConfigChange	Select Access	WorkflowConfigChange
Audit User Deletion	WorkflowChangeRequest submitted	Select Access	WorkflowChangeRequest submitted
Audit User Deletion	WorkflowChangeRequest approved	Select Access	WorkflowChangeRequest approved
Audit User Deletion	WorkflowChangeRequest rejected	Select Access	WorkflowChangeRequest rejected
Audit User Deletion	WorkflowChangeRequest reverted	Select Access	WorkflowChangeRequest reverted
Audit User Deletion			
Audit User Deletion	Workflow create	Select Identity	SI workflow create
Audit User Deletion	Workflow delete	Select Identity	SI workflow delete
Audit User Deletion	Workflow modify	Select Identity	SI workflow modify
Audit User Deletion	Workflow view	Select Identity	SI workflow view
Audit User Deletion	Workflow copy	Select Identity	SI workflow copy
Audit User Deletion	Workflow import	Select Identity	SI workflow import
Audit User Deletion	Workflow export	Select Identity	SI workflow export
Audit User Deletion	Disable Service Membership	Select Identity	SI Disable Service Membership
Audit User Termination	Terminate User	Select Identity	SI Terminate User
Audit User Termination	disable before terminate	Select Identity	SI disable before terminate
Audit User Termination	WorkflowConfigChange	Select Access	WorkflowConfigChange

**Table 12 Select Identity Event Filtering (cont'd)**

<b>Report Type Assigned in SI</b>	<b>Events Viewable in Select Audit</b>		
	<b>Audit Event Name</b>	<b>Application</b>	<b>Component Event Name</b>
Audit User Termination	WorkflowChangeRequest submitted	Select Access	WorkflowChangeRequest submitted
Audit User Termination	WorkflowChangeRequest approved	Select Access	WorkflowChangeRequest approved
Audit User Termination	WorkflowChangeRequest rejected	Select Access	WorkflowChangeRequest rejected
Audit User Termination	WorkflowChangeRequest reverted	Select Access	WorkflowChangeRequest reverted
Audit User Termination	Workflow create	Select Identity	SI workflow create
Audit User Termination	Workflow delete	Select Identity	SI workflow delete
Audit User Termination	Workflow modify	Select Identity	SI workflow modify
Audit User Termination	Workflow view	Select Identity	SI workflow view
Audit User Termination	Workflow copy	Select Identity	SI workflow copy
Audit User Termination	Workflow import	Select Identity	SI workflow import
Audit User Termination	Workflow export	Select Identity	SI workflow export
Audit User Password	Reset Password	Select Identity	SI Reset Password
Audit User Password	Change Password	Select Identity	SI Change Password
Audit User Password	Change Password	Select Federation	SF AdminAdm Password Changed
Audit User Password	Error Changing Password	Select Federation	SF AdminAdm Error Changing Password
Audit User Password	Forget Password	Select Identity	SI Forget Password
Audit User Password	Expire Password Notification	Select Identity	SI Expire Password Notification

**Table 12 Select Identity Event Filtering (cont'd)**

<b>Report Type Assigned in SI</b>	<b>Events Viewable in Select Audit</b>		
	<b>Audit Event Name</b>	<b>Application</b>	<b>Component Event Name</b>
Audit User Password	Expire Password	Select Identity	SI Expire Password
Audit User Password	Password Policy change	Select Access	passwordPolicyChange
Audit User Password	Password Reset Config Change	Select Access	password Reset Config Change
Audit User Password	WorkflowConfigChange	Select Access	WorkflowConfigChange
Audit User Password	WorkflowChangeRequest submitted	Select Access	WorkflowChangeRequest submitted
Audit User Password	WorkflowChangeRequest approved	Select Access	WorkflowChangeRequest approved
Audit User Password	WorkflowChangeRequest rejected	Select Access	WorkflowChangeRequest rejected
Audit User Password	WorkflowChangeRequest reverted	Select Access	WorkflowChangeRequest reverted
Audit User Password	Workflow create	Select Identity	SI workflow create
Audit User Password	Workflow delete	Select Identity	SI workflow delete
Audit User Password	Workflow modify	Select Identity	SI workflow modify
Audit User Password	Workflow view	Select Identity	SI workflow view
Audit User Password	Workflow copy	Select Identity	SI workflow copy
Audit User Password	Workflow import	Select Identity	SI workflow import
Audit User Password	Workflow export	Select Identity	SI workflow export
Audit User Hint	Hint Setup	Select Identity	SI Hint Setup
Audit User Login	Sent Login request	Select Federation	SF Protocol Sent Login Request
Audit User Login	Sent Logout request	Select Federation	SF Protocol Sent Logout Request



**Table 12 Select Identity Event Filtering (cont'd)**

Report Type Assigned in SI	Events Viewable in Select Audit		
	Audit Event Name	Application	Component Event Name
Audit User Login	Received Login request	Select Federation	SF Protocol Received Login Request
Audit User Login	Received Login request	Select Federation	SF Protocol Received Logout Request
Audit User Login	Received Logout request	Select Federation	SF API Received logout request
Audit User Login	Logged In	Select Access	Login
Audit User Login	Logged In	Select Identity	SI login
Audit User Login	Logged In	Select Federation	SF Internal Logged In
Audit User Login	Logged Out	Select Access	Logout
Audit User Login	Logged Out	Select Identity	SI logout
Audit User Login	Logged Out	Select Federation	SF Internal Logged Out
Audit User Login	Login Error	Select Access	Login error
Audit User Login	Login Error	Select Federation	SF Internal Login Error
Audit User Login	Admin Logged In	Select Access	Admin Login
Audit User Login	Admin Logged In	Select Access	Delegate Admin Login
Audit User Login	Admin Logged In	Select Federation	SF Admin Logged In
Audit User Login	Admin Logged Out	Select Access	Admin Logout
Audit User Login	Admin Logged Out	Select Access	Delegate Admin Logout
Audit User Login	Admin Logged Out	Select Federation	SF Admin Logged Out
Audit User Login	Admin Login Error	Select Access	Admin Login error
Audit User Login	Admin Login Error	Select Access	Delegate Admin Login error
Audit User Login	Admin Login Error	Select Federation	SF Admin Login Error
Audit User Login	Credential expire	Select Access	Credential expire
Audit User Login	Reset Password	Select Identity	SI Reset Password
Audit User Login	Password Reset Config Change	Select Access	password Reset Config Change
Audit User Login	WorkflowConfigChange	Select Access	WorkflowConfigChange
Audit User Login	WorkflowChangeRequest submitted	Select Access	WorkflowChangeRequest submitted

**Table 12 Select Identity Event Filtering (cont'd)**

Report Type Assigned in SI	Events Viewable in Select Audit		
	Audit Event Name	Application	Component Event Name
Audit User Login	WorkflowChangeRequest approved	Select Access	WorkflowChangeRequest approved
Audit User Login	WorkflowChangeRequest rejected	Select Access	WorkflowChangeRequest rejected
Audit User Login	WorkflowChangeRequest reverted	Select Access	WorkflowChangeRequest reverted
Audit User Login	Workflow create	Select Identity	SI workflow create
Audit User Login	Workflow delete	Select Identity	SI workflow delete
Audit User Login	Workflow modify	Select Identity	SI workflow modify
Audit User Login	Workflow view	Select Identity	SI workflow view
Audit User Login	Workflow copy	Select Identity	SI workflow copy
Audit User Login	Workflow import	Select Identity	SI workflow import
Audit User Login	Workflow export	Select Identity	SI workflow export
Admin Configuration	WorkflowConfigChange	Select Access	WorkflowConfigChange
Admin Configuration	WorkflowChangeRequest submitted	Select Access	WorkflowChangeRequest submitted
Admin Configuration	WorkflowChangeRequest approved	Select Access	WorkflowChangeRequest approved
Admin Configuration	WorkflowChangeRequest rejected	Select Access	WorkflowChangeRequest rejected
Admin Configuration	WorkflowChangeRequest reverted	Select Access	WorkflowChangeRequest reverted
Admin Configuration	Workflow create	Select Identity	SI workflow create
Admin Configuration	Workflow delete	Select Identity	SI workflow delete
Admin Configuration	Workflow modify	Select Identity	SI workflow modify
Admin Configuration	Workflow view	Select Identity	SI workflow view

**Table 12 Select Identity Event Filtering (cont'd)**

<b>Report Type Assigned in SI</b>	<b>Events Viewable in Select Audit</b>		
	<b>Audit Event Name</b>	<b>Application</b>	<b>Component Event Name</b>
Admin Configuration	Workflow copy	Select Identity	SI workflow copy
Admin Configuration	Workflow import	Select Identity	SI workflow import
Admin Configuration	Workflow export	Select Identity	SI workflow export
Admin Configuration	Logging Config Change	Select Access	loggingConfigChange
Admin Configuration	Report Config	Select Audit	Select Audit Report Config



## B Operations Model Thresholds

This appendix describes the Operations model and lists the default thresholds for indicating the status of the model. The Operations model measures the health of the Audit Server itself, and the various processes managed by the Audit Server. There are two main categories:

- The processing of message batches.
- The handling of notification workflows.

The model is organized as a tree, with the basic metrics at the bottom rolling up into summary nodes above. The status of a summary node is the “lowest” status of all the input nodes. The trend is calculated relative to the previous status of the summary node (whatever the previous lowest input was). All measurements cover activity during the last day.

The high-level structure has Operational Status at the top and three nodes below:

- Batch Count Status
- Batch Delay Status
- Audit Workflow Status

### Batch Count Status

These measurements show the current state of the message batch processor within the Audit Server.

**Table 13 Batch Count Status Thresholds**

Node	Description	Red	Yellow	Green
Batches Normalizing	The number of batches being normalized at the moment the model analysis ran.	8 – 10	3 – 7	0 – 2
Batches Done	The number of batches successfully processed during the last day.	N/A	0 – 4	5 or more
Batches Pending	The number of batches received, but not yet begun processing.	16 – 20	4 – 15	0 – 3
Batches Error	The number of batches that could not be successfully normalized during the last day.	2 or more	1	0
Batches Unknown	The number of batches in an unknown state (indicates an internal error in the Audit Server).	2 or more	1	0

## Batch Delay Status

These measurements look at the amount of time the Audit Server is taking to process batches.

**Table 14 Batch Delay Status Thresholds**

Node	Description	Red	Yellow	Green
Batches Normalizing 1 Minute	The number of batches being normalized at the moment the model analysis ran that have been normalizing for at least one minute. Indicates that the Audit Server is taking an unusually long time to normalize these message batches.	2 or more	1	0
Batches Delayed 5 Minutes	The number of batches currently being normalized that waited more than five minutes from the time they were received to the time they began being normalized.	1 or more	N/A	0
Batches Pending 5 Minutes	The number of batches received more than five minutes ago but not yet begun processing.	2 or more	1	0
Batches Processed Over 10 Minutes	The number of batches that completed processing in the last day that took more than ten minutes from when they were received to when processing completed (or processing was determined to have failed).	No thresholds applied		

## Audit Workflow Status

These measurements look at current counts, processing delays and user interaction delays in the Audit Approval workflows.

**Table 15 Audit Workflow Status Thresholds**

Node	Description	Red	Yellow	Green
Audit Workflow Pending	The number of reports currently waiting for approval.	8 or more	3 – 7	0 – 2
Audit Workflow Notify Fail	The number of reports currently waiting for approval for which there was an error sending out the email notification.	1 or more	N/A	0
Audit Workflow Completed	The number of notification/alert workflows that completed in the last day where no user approval was required.	No thresholds applied		
Audit Workflow Approved	The number of reports approved by users during the last day.	No thresholds applied		

**Table 15 Audit Workflow Status Thresholds (cont'd)**

<b>Node</b>	<b>Description</b>	<b>Red</b>	<b>Yellow</b>	<b>Green</b>
Audit Workflow Rejected	The number of reports rejected (disapproved) by users during the last day.	2 or more	1	0
Audit Workflow Pending 7 Days	The number of workflows that have been waiting at least seven days for a user to respond and approve/reject the report.	8 or more	3 – 7	0 – 2
Audit Workflow Pending 14 Days	Approvals that have been waiting over 14 days for a user to respond.	2 or more	1	0
Audit Workflow Stuck	Workflows stuck in an internal processing state. Indicates an internal error in the Audit Server approvals subsystem.	1 or more	N/A	0
Audit Workflow Errors	The number of approval processes that terminated because of a processing error.	1 or more	N/A	0





# Index

## A

- access control
  - levels, 35
  - Report Level, 35
  - reports, 35
  - Row Level, 36
- Ad Hoc Wizard, 105 to 114
  - charts, 110
  - date format, 106
  - designing reports for, 105
  - overview, 105
  - tabular reports, 106
- Admin Dashboard
  - cache, 92
  - components, 90
  - described, 89
  - Library JAR file, 91
  - log files, viewing, 91
  - report statistics, 92
  - system functions, 90
- Administration menu, 18
- administration report schedules, 117
- administrator password
  - globally configuring, 30
  - tool, 30
  - using, 30
- administrator password tool
  - running, 30
  - structure, 30
- appenders, setting for logging, 26
- applications
  - correlating users, 23
  - enabling/disabling correlation, 24
- approvals
  - menu, 17
  - workspace, 19
- Attestation workflow, configuring, 85
- Auditors, 33
- Audit Portal
  - Administration menu, 18
  - Approvals menu, 17
  - Approvals workspace, 19

- configuration, 21, 40, 85, 89
- data integrity configuration, 79
- features, 17
- Help menu, 18
- Loader screen, 74
- Model Configuration screen, 76
- models, 71
- Models menu, 17
- Models workspace, 19
- report schedules, 117
- Reports menu, 17
- Reports workspace, 18
- setting logout time, WebLogic, 20
- setting logout time, WebSphere, 21
- toolbar, 17

## C

- charts, 110
- child nodes, model, 74
- compliance models
  - Audit Portal, loading, 74
  - configuring, 77
  - described, 72
  - loading, 74
  - model file, 74
- configuration
  - administrator password, 30
  - Attestation workflows, 85
  - Audit Portal screen, 76
  - compliance model, 77
  - connectors, 21
  - connectors, manual, 23
  - correlating users, 23
  - data integrity, 79
  - log4j, 26
  - mail sessions, 25
  - Operations model, 76
  - Report server, 89
  - Select Identity, 40
  - Select Identity database, 44, 48
- connectors
  - configuring, 21
  - Linux configuration, 23
  - manually configuring, 23

- correlating users
  - described, 23
  - MSSQL, disabling, 25
  - MSSQL, enabling, 25
  - Oracle, disabling, 24
  - Oracle, enabling, 24

## D

- data integrity
  - .pfx files, 81
  - configuring, 79
  - HSMs, 82
  - Java, 79
  - PKCS12, 79
  - smart cards, 82
  - verification, 82

## F

- filtering
  - Select Identity, described, 40
  - Select Identity reports, 40, 119
- folders
  - managing, 97
  - permissions, 99

## G

- guide, contents of, 12

## H

- HSMs, configuring keystores, 82

## I

- integrations
  - Select Access, 51, 61
  - Select Identity, 33, 40

## K

- keystores
  - .pfx files, 81
  - HSMs, 82
  - PKCS12, 79
  - smart cards, 82

## L

- Library
  - Catalog folder, 96
  - described, 95
  - files, uploading, 101
  - folder management, 97
  - reports, 102

- report toolbar, 102
- Select Audit Reports folder, 96
- User Scopes folder, 97

- log4j
  - appenders, setting, 26
  - configuring, 26
  - enabling, 26
  - properties file, 26

- log4j.properties, 26

- logging
  - configuring, 26
  - enabling, 26
  - setting appenders, 26

## M

- mail sessions, configuring, 25

- models

- analysis tree, 72
- child node reports, 74
- compliance, 72
- Configuration screen, 76
- configuring, 76, 77
- deleting, 78
- exporting, 77
- history, 74
- loading, 74
- menu, 17
- model file, 74
- Model Loader screen, 74
- Operations, 72
- overview, 71
- status, 73
- trend, 74
- updating, 77
- workspace, 19

- MSSQL

- correlating users, disabling, 25
- correlating users, enabling, 25

- My Reports, 95

## O

- online help, 18

- Operations model
  - configuring, 76
  - described, 72
  - thresholds, 133
  - updating, 77

- Oracle

- correlating users, disabling, 24
- correlating users, enabling, 24

## P

- permission data
  - described, 34
  - storing and refreshing, 35
- permission policies
  - described, 34
  - report type, 34
  - Select Identity, 34
  - services and contexts, 34
  - user management, 34
- permissions
  - folders, 99
  - Select Identity, 33
- portal
  - Administration menu, 18
  - Approvals menu, 17
  - Approvals workspace, 19
  - features, 17
  - Help menu, 18
  - models, 71
  - Models menu, 17
  - Models workspace, 19
  - report schedules, 117
  - Reports menu, 17
  - Reports workspace, 18
  - setting logout time for WebLogic, 20
  - setting logout time for WebSphere, 21
  - toolbar, 17
- preferences, setting, 116
- publishing reports, 103

## R

- report access
  - Select Access, 69
  - Select Identity, 37
- Report Center
  - Ad Hoc Wizard, 105
  - cache, 92
  - Catalog folder, 96
  - components, 94
  - files, uploading, 101
  - folder permissions, 99
  - folders, 97
  - Library, 95
  - log files, viewing, 91
  - My Reports, 95
  - preferences, 116
  - reports, 102
  - reports, searching for, 114
  - reports, searching within, 115
  - report statistics, 92
  - Select Audit Reports folder, 96

- system functions, 90
- User Scopes folder, 97
- using, 93

- Report Level control, 35
- report permission mapping, Select Identity, 33
- reports
  - access control, 35
  - Ad Hoc, date format, 106
  - Ad Hoc Wizard, 105
  - approving, 88
  - charts, 110
  - managing, 102
  - mappings, 33
  - menu, 17
  - overview, 89
  - properties, 104
  - publishing, 103
  - Report Center, 93
  - running, 102
  - schedules, 103
  - schedules, editing, 117
  - searching, 114
  - searching within, 115
  - Select Identity-specific, 97
  - tabular, 106
  - toolbar, 102
- report statistics
  - layout and content times, 92
  - viewing, 92
- Reports workspace, 18
- roles, Select Audit, 39
- Row Level control, 36

## S

- schedules
  - editing, 117
  - reports, 103
  - viewing, 90
- Select Access
  - integration, 51, 61
  - report access, 69
- Select Audit
  - access control levels, 35
  - activities, 11
  - Ad Hoc Wizard, 105
  - Administration menu, 18
  - Approvals menu, 17
  - Approvals workspace, 19
  - Attestation workflows, configuration, 85
  - Audit Portal, 17
  - configuration, 21, 40, 85, 89
  - connector configuration, 21

- data integrity configuration, 79
- data integrity verification, 82
- Help menu, 18
- models, 71
- models, configuring, 76
- models, deleting, 78
- models, exporting, 77
- models, loading, 74
- Models menu, 17
- Models workspace, 19
- My Reports, 95
- report access control, 35
- report approval, 88
- Report Center, 93
- Report Level control, 35
- reports, 89
- reports, searching for, 114
- reports, searching within, 115
- report schedules, 117
- Reports menu, 17
- Reports workspace, 18
- roles, 39
- Row Level control, 36
- Select Identity configuration, 40
- Select Identity database information, 44, 48
- Select Identity integration, 40
- Select Identity
  - configuring, 40
  - database information, 44, 48
  - filtering, 40, 119
  - filtering described, 40
  - integration, 33
  - integration and J2EE, 39
  - permission data, 34
  - permission data, storing, 35
  - permission mapping, 33
  - permission policies, 34
  - permissions, 33
  - report access, 37
  - report type permissions, 34
  - services and contexts permissions, 34
  - user management permissions, 34
- Select Identity-specific reports, 97
- smart cards, configuring keystores, 82
- status
  - model, 73
- system functions
  - cache, 92
  - log files, 91
  - report statistics, 92
  - schedules, 90

## T

- thresholds, Operations model, 133
- toolbar
  - Administration menu, 18
  - Approvals menu, 17
  - Audit Portal, 17
  - Help menu, 18
  - Models menu, 17
  - reports, 102
  - Reports menu, 17
- trend, model, 74

## W

- WebLogic
  - Select Access integration, 51
  - Select Identity database information, 44
  - setting portal logout time, 20
- WebSphere
  - Select Access integration, 61
  - Select Identity database information, 48
  - setting portal logout time, 21
- wizards, Ad Hoc, 105
- workflows, Attestation, configuring, 85
- workspace
  - Approvals, 19
  - Models, 19
  - Report, 18

