HP OpenView Select Audit

For the Windows®, HP-UX®, and Linux® Operating Systems

Software Version: 1.01

Administration Guide

Document Release Date: November 2006
Software Release Date: November 2006

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

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

Trademark Notices

HP OpenView Select Audit includes the following software developed by third parties:

- ANTLR Copyright 2005 Terrence Parr.
- commons-logging from the Apache Software Foundation.
- Install Anywhere, Copyright 2004 Zero G Software, Inc.
- 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.
- OpenAdaptor from the Software Conservancy.
- 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.

Documentation Updates

This manual'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://ovweb.external.hp.com/lpe/doc_serv/

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 OpenView Support web site at:

www.hp.com/managementsoftware/support

HP OpenView 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, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

www.managementsoftware.hp.com/passport-registration.html

Contents

1 Introduction

HP OpenView Select Audit is part of HP's business service 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 login and logout of Select Audit, view reports, monitor dashboards to respond to alerts, run reports, schedule reports, 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:

- 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

Some of the tasks Administrators can perform using the Audit Portal include:

- 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 installed with Select Audit and are available in the `<install_path>/docs` folder where `<install_path>` represents the path where Select Audit is installed.

- *HP OpenView Select Audit 1.01 Administration Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`administration_guide.pdf`).
- *HP OpenView Select Audit 1.01 Installation Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`installation_guide.pdf`).
- *HP OpenView Select Audit 1.01 User's Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`user_guide.pdf`).
- *HP OpenView Select Audit 1.01 Sarbanes-Oxley Model Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`sb_model_guide.pdf`)
- *HP OpenView Select Audit 1.01 Concepts Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`concepts_guide.pdf`)
- *HP OpenView Select Audit 1.01 Report Center User's Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`rpt_center_guide.pdf`)
- *HP OpenView Select Audit 1.01 Report Designer's Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`rpt_design_guide.pdf`)
- *HP OpenView Select Audit 1.01 Report Developer's Guide*, © Copyright 2006 Hewlett-Packard Development Company, L.P. (`rpt_devel_guide.pdf`)

Online help is available with the Audit Portal.

Chapter Summary

This guide includes the chapters listed in Table 1.

➤ See the *HP OpenView Select Audit 1.01 Release Notes* (`relnotes.pdf`) on the Select Audit installation CD for known installation issues at the time of this release.

Table 1 Guide Overview

Chapter	Description
Chapter 2, Getting Started	This chapter describes how to access the Audit Portal and begin using Select Audit.
Chapter 3, Configuring Select Audit	This chapter describes how to configure Select Audit.
Chapter 4, Select Identity Integration	This chapter describes how to integrate Select Identity with Select Audit.
Chapter 5, Select Access Integration	This chapter describes how to integrate Select Access with Select Audit.

Table 1 Guide Overview (cont'd)

Chapter	Description
Chapter 6, Models	This chapter describes how to use models in Select Audit.
Chapter 7, Using Select Audit	This chapter describes how to verify data integrity and how to approve reports using the Audit Portal.
Chapter 8, Using Reports in Select Audit	This chapter describes the features of the reporting tools in Select Audit. Reports are viewed, scheduled and modified using 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.

2 Getting Started

Select Audit is accessed via 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 your configurations.

Select Audit supports the following browsers:

- Internet Explorer 6
- Firefox

This chapter includes the following topics:

- Starting Select Audit on page 13
- Audit Portal Features on page 15
- Setting the Portal Logout Time on page 19

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 enter the following URL:

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

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

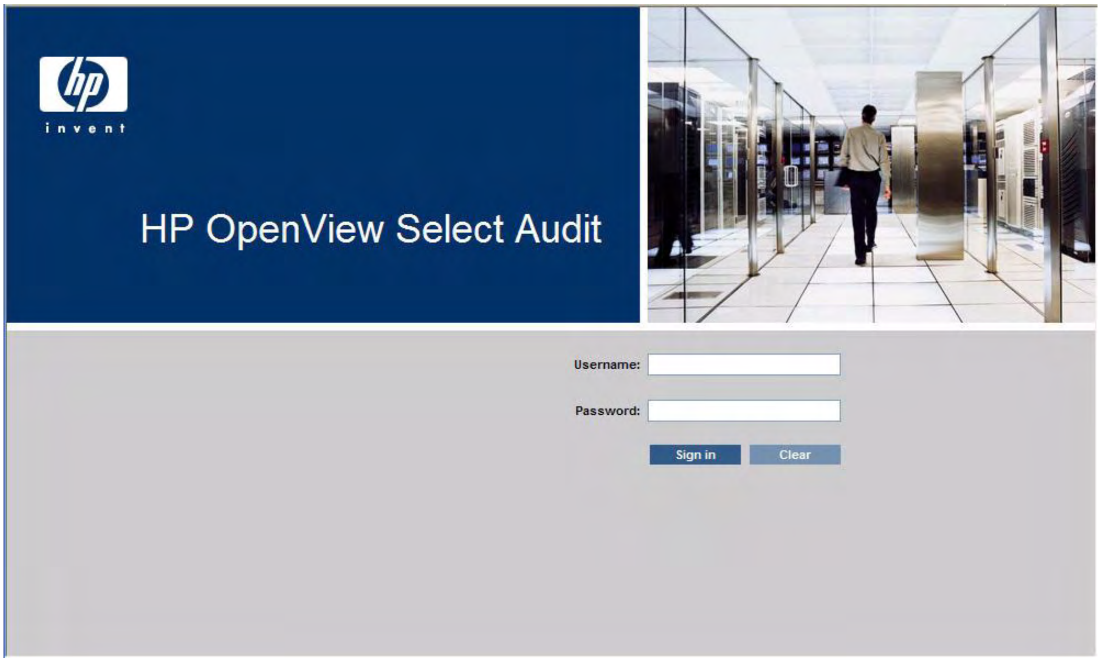
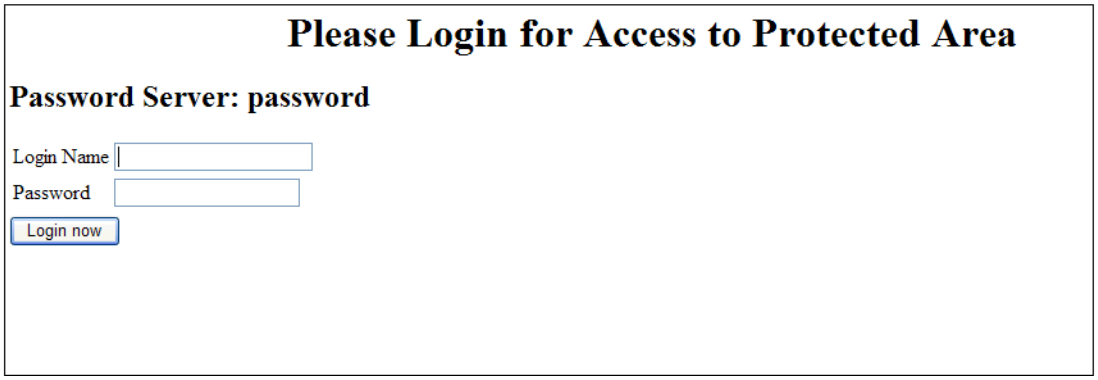


Figure 1 Select Audit Login Page

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

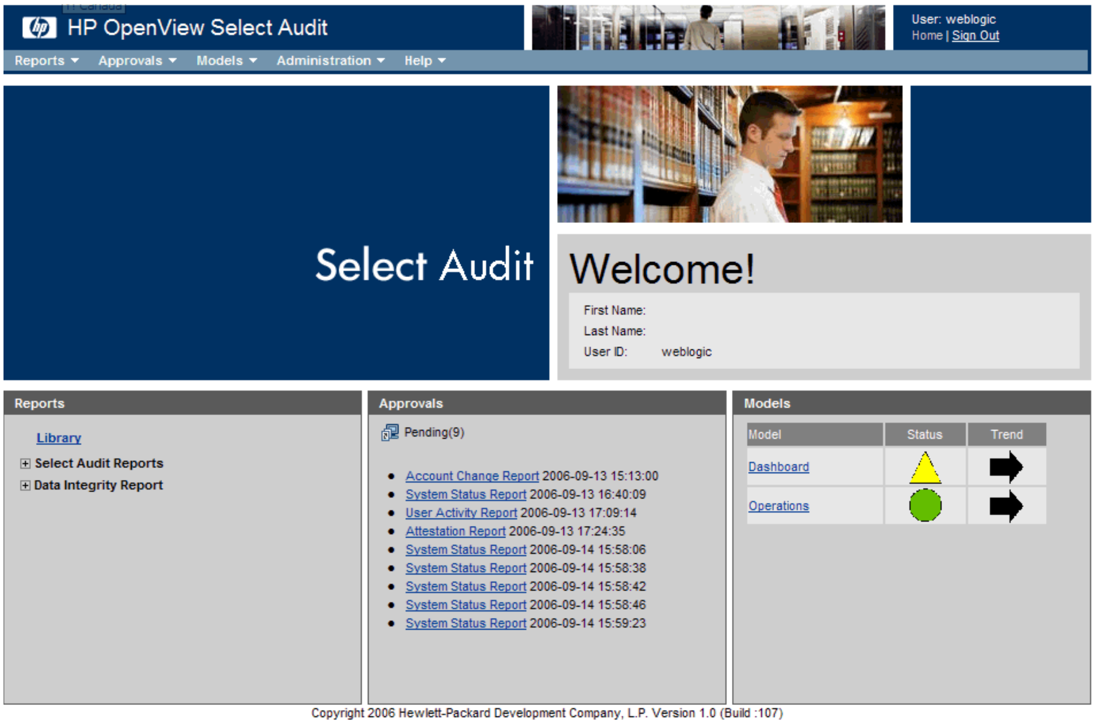


Please Login for Access to Protected Area

Password Server: password

Figure 2 Select Audit/Select Access Integration Login Page

2 Enter your Select Audit username and password in the appropriate fields and click **Sign In**. The **Select Audit Portal** appears.



Welcome!

First Name:
Last Name:
User ID: weblogic

Reports

Library
⊞ Select Audit Reports
⊞ Data Integrity Report

Approvals

Pending(9)

- Account Change Report 2006-09-13 15:13:00
- System Status Report 2006-09-13 16:40:09
- User Activity Report 2006-09-13 17:09:14
- Attestation Report 2006-09-13 17:24:35
- System Status Report 2006-09-14 15:58:06
- System Status Report 2006-09-14 15:58:38
- System Status Report 2006-09-14 15:58:42
- System Status Report 2006-09-14 15:58:46
- System Status Report 2006-09-14 15:59:23

Models

Model	Status	Trend
Dashboard	▲	➡
Operations	●	➡

Copyright 2006 Hewlett-Packard Development Company, L.P. Version 1.0 (Build :107)

Figure 3 Select Audit Portal

From the Audit Portal you can manage audit functions such as running and scheduling reports via 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**.

Figure 4 Audit Portal Toolbar

The menus are described in Table 2.

Table 2 Toolbar

Menu item	Description
Reports	The **Reports** menu has three entries: **Library**, **My Reports** and **Search**. Clicking any of these menu items opens the **Report Center**. The Reports menu items are described below: • Library opens the Report Library in the Report Center. In the Library, you can upload reports to the Report Server. • My Reports opens the My Reports area of the Report Center, which displays 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. • Search opens the Search engine in the Report Center. You can search for reports using any or all of the criteria listed. For detail information about using the Report Center, refer to *HP OpenView Select Audit 1.01 Report Center User's Guide*.
Approvals	The **Approvals** menu is used to view pending approvals assigned to you. See Chapter 7, Using Select Audit for more information about approving reports.
Models	The **Models** menu has three standard submenus: **Overview**, **Operations** and **Manage Models**. It also contains submenus for any loaded compliance models. • Overview opens the high-level view of the currently-loaded models in a new browser window. • Operations opens the **Operations** folder in the Report Center. • Manage Models is used export, load, update and delete models. See Chapter 6, Models for more information about approving reports.
Administration	The **Administration** menu is used to change configuration settings, view schedules for reports, load report packs, and verify the integrity of data. The Administration menu items are described below: • Verify Audit Data Integrity opens the **Data Verification Configuration** screen. In this screen you can specify start and end dates to run data verification. • View Report Schedules opens to the **Schedules** screen, under the **Admin** menu in the Report Center. • Manage Models is used export, load, update and delete models. • Configuration opens the **Configuration** screen. Use this page to change the configuration settings for connectors, data integrity, and the report client.
Help	The **Help** menu is used to access online help for Select Audit. It also contains copyright and version information. Administrators should refer to the **Adminstrator Guide** menu item.

Workspaces

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

Reports workspace

The **Reports** workspace is displayed on the left-hand side of the lower portion of the Audit Portal.

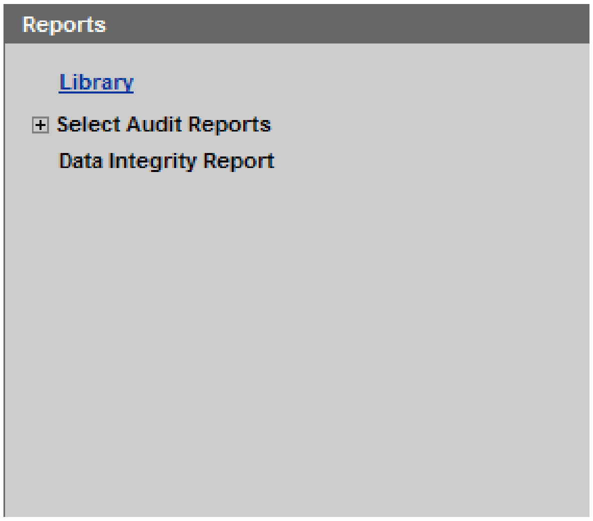


Figure 5 Report Workspace

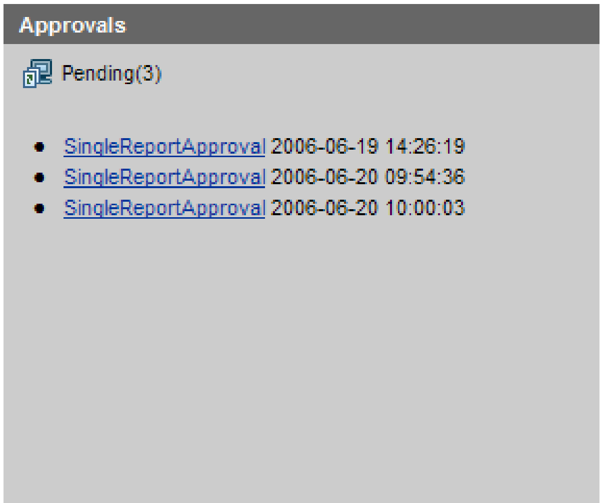
The Reports workspace provides quick access to commonly-used report features:

- **Library** opens the Library in the Report Center.
- **Select Audit Reports** expands to show a list of the most frequently-used Select Audit reports.
- **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.

See Chapter 8, Using Reports in Select Audit for more information about the Report Center.

Approvals workspace

The **Approvals** workspace is displayed in the center of the lower portion of the Audit Portal.



Approvals

Pending(3)

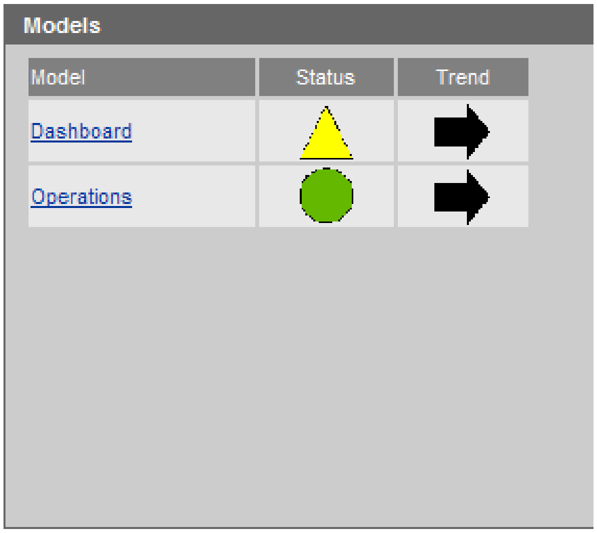
- SingleReportApproval 2006-06-19 14:26:19
- SingleReportApproval 2006-06-20 09:54:36
- SingleReportApproval 2006-06-20 10:00:03

Figure 6 Approvals Workspace

The Approvals workspace 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 82 for more information about approving reports.

Models workspace

The **Models** workspace is displayed on the right-hand side of the lower portion of the Audit Portal.



Models

Model	Status	Trend
Dashboard	▲	➡
Operations	●	➡

Figure 7 Models Workspace

The Models workspace displays a high-level view of the currently-loaded models, showing the status and trend. See Chapter 6, Models for more information about Select Audit models.

Setting the Portal Logout Time

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

1. Open the `auditserver.ear` file and the corresponding Audit Portal `web.war` file in the installation directory.
2. Break out the Audit Portal `web.xml` file.
3. In the WebLogic console, locate the Audit Portal `web.xml` file in the `auditserver.ear` file and the `SelectAuditReporting` applications.
4. Change the `<session-timeout>` element in the `web.xml` file to the desired value, e.g.:

```
<session-config>
   <session-timeout>20</session-timeout>
</session-config>
```

3 Configuring Select Audit

This chapter describes how to configure Select Audit using the Audit Portal. After installing the Audit Server and the Audit Connector, you may optionally configure Select Audit. You can also modify your configuration as necessary. The **Administration** menu is used to change configuration settings.

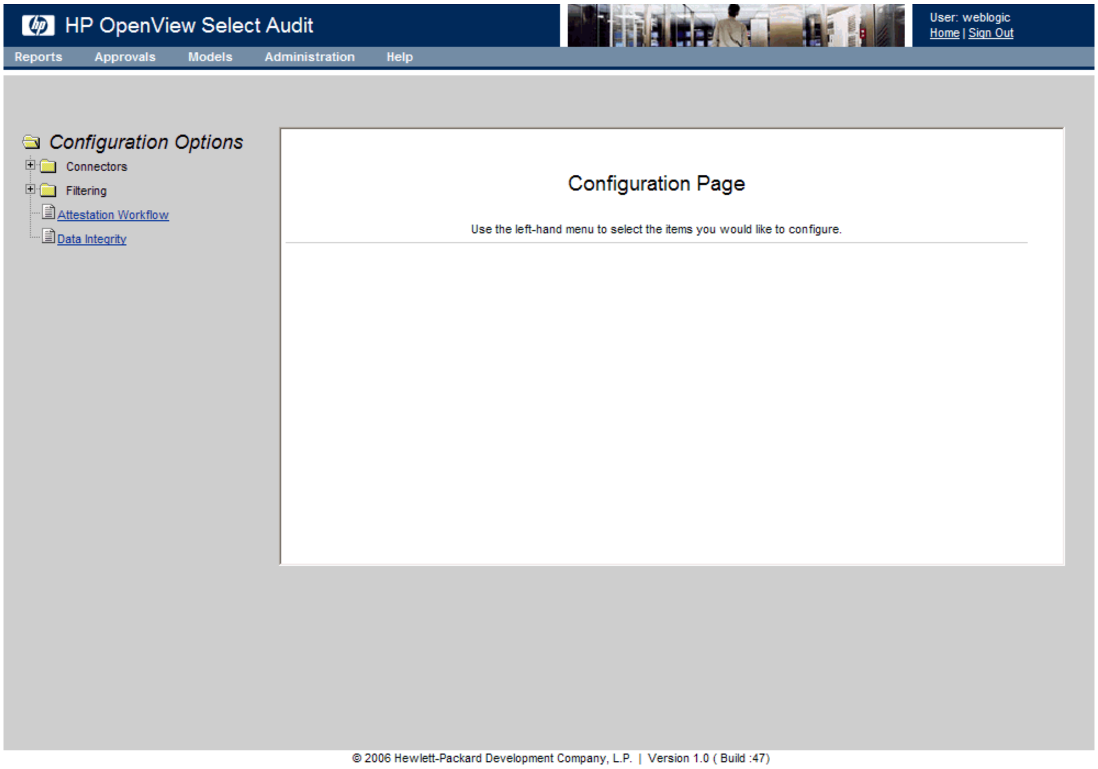
This chapter contains the following topics:

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 OpenView Select Audit 1.01 Installation Guide* for more information. You can configure the connectors to specify when rollovers occur, using the Audit Portal.

To configure a connector

1 Select **Administration** → **Configuration**. The **Configuration** screen appears.



Configuration Page

Use the left-hand menu to select the items you would like to configure.

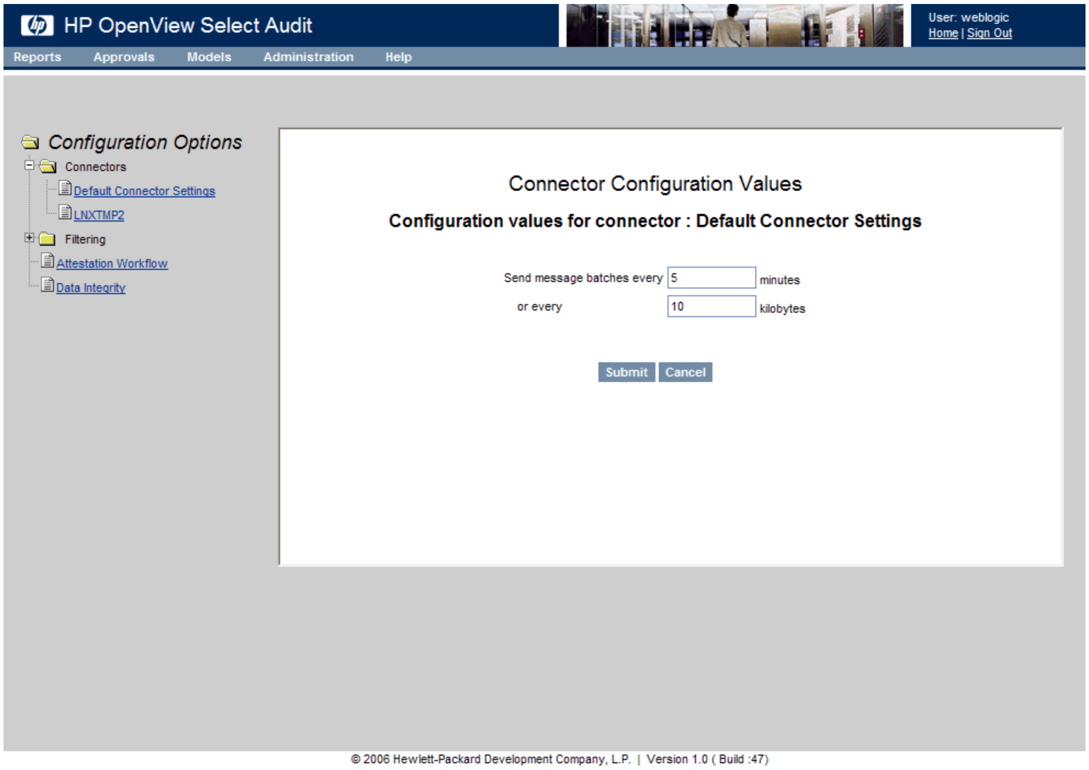
© 2006 Hewlett-Packard Development Company, L.P. | Version 1.0 (Build :47)

Figure 8 Configuration Screen

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 appears.



Connector Configuration Values

Configuration values for connector : Default Connector Settings

Send message batches every 5 minutes

or every 10 kilobytes

© 2006 Hewlett-Packard Development Company, L.P. | Version 1.0 (Build :47)

Figure 9 Connector Configuration Values Screen

4 To specify when rollovers occur, enter a time in the **Send message batches every** field or a batch size in the **or every** field.

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 Change the protection on the directory where Java was installed to `drwxr-xr-x`. (It is installed with protection `drwxrwx---`.) That is, give the owner, `root` full access (`rwx`), the group `root` full access, and every user read access (`rx`).

```
chmod 775 /root/java
```

2 Change the protection on the directory where Select Audit was installed to `drwxr-xr-x`. (It is installed with protection `drwxrwxr--`.)

```
chmod 775 /opt/OV/SelectAudit
```

3 Create a new user saud in /etc/passwd and create a new group saud.

> You might want to create user saud using the shell /bin/. This user must have a password to login.
>
> Set the shell to /bin/nologin so that it's not possible to login to the machine as user saud AND make sure that user saud has a non-empty password. This is to ensure that if that shell ever gets changed (or if some other shell is used instead of /bin/nologin) that a login as user saud can not occur without specifying a password.

4 Change the ownership and group ownership of the log and logfiles directories to user saud and group saud.

```
chown saud /opt/OV/SelectAudit/{log,logfiles}
chgrp saud /opt/OV/SelectAudit/{log,logfiles}
```

5 Change the protection on the log and logfiles directories so that user saud has full access (rwx), group saud has only read (rx) access and everyone else cannot view the contents of these directories.

```
chmod 750 /opt/OV/SelectAudit/{log,logfiles}
```

6 Create the directory /var/run/SelectAudit owned by user saud for the connector pid.

```
mkdir /var/run/SelectAudit
```

7 Change the ownership of /var/run/SelectAudit to user saud and group saud.

```
chown saud /var/run/SelectAudit
chgrp saud /var/run/SelectAudit
```

8 In SAudConn, set the following environment variables:

```
JAVA_HOME=/root/java
CONNECTOR_HOME=/opt/OV/SelectAudit/connector
PATH=$JAVA_HOME/bin:$CONNECTOR_HOME:$PATH
USER=saud
PIDFILE=/var/run/SelectAudit/connector.pid
```

```
export JAVA_HOME CONNECTOR_HOME PATH USER PIDFILE
```

> You have to change the value of PIDFILE from the original PIDFILE=/var/run/connector.pid because only root can write to /var/run and the connector launched by the modified SAudConn script will be running as saud, who can write to /var/run/SelectAudit.

> The variables set in the SAudConn startup script have to be exported as environment variables so that their values are picked up by the shell of the user as which the connector runs.

9 In /opt/OV/SelectAudit, create a file called nohup.sh containing:

```
nohup $JAVA_HOME/bin/java -server -jar connector.jar
connector.props A B > /dev/null 2>&1 & CONNECTORPID="$!"
echo $CONNECTORPID > $PIDFILE
```

10 Edit SAudConn and replace:

```
nohup $JAVA_HOME/bin/java -server -jar connector.jar
connector.props A B > /dev/null 2>&1 & CONNECTORPID="$!"
echo $CONNECTORPID > $PIDFILE
```

with

```
/sbin/runuser $USER -c "sh ./nohup.sh"
```

11 Save the file.

> ➤ If the `saud` user has `shell /bin/nologin`, then use the `runuser -s` option with a specific shell, e.g. `-s /bin/sh` so that the `runuser` command will be forced to use that shell rather than the default.

12 Test the connector. Running `/etc/init.d/SAudConn start` as `root` should start the connector running as user `saud`.

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 OpenView Select Identity* documentation for more information about configuring Select Identity.

During installation, the Audit Server installer performs the following tasks:

- It specifies an authenticator in the WebLogic console.
- It configures a WebLogic directory provider in the Report Center Administration console.
- It creates default users and roles defined in the WebLogic console.

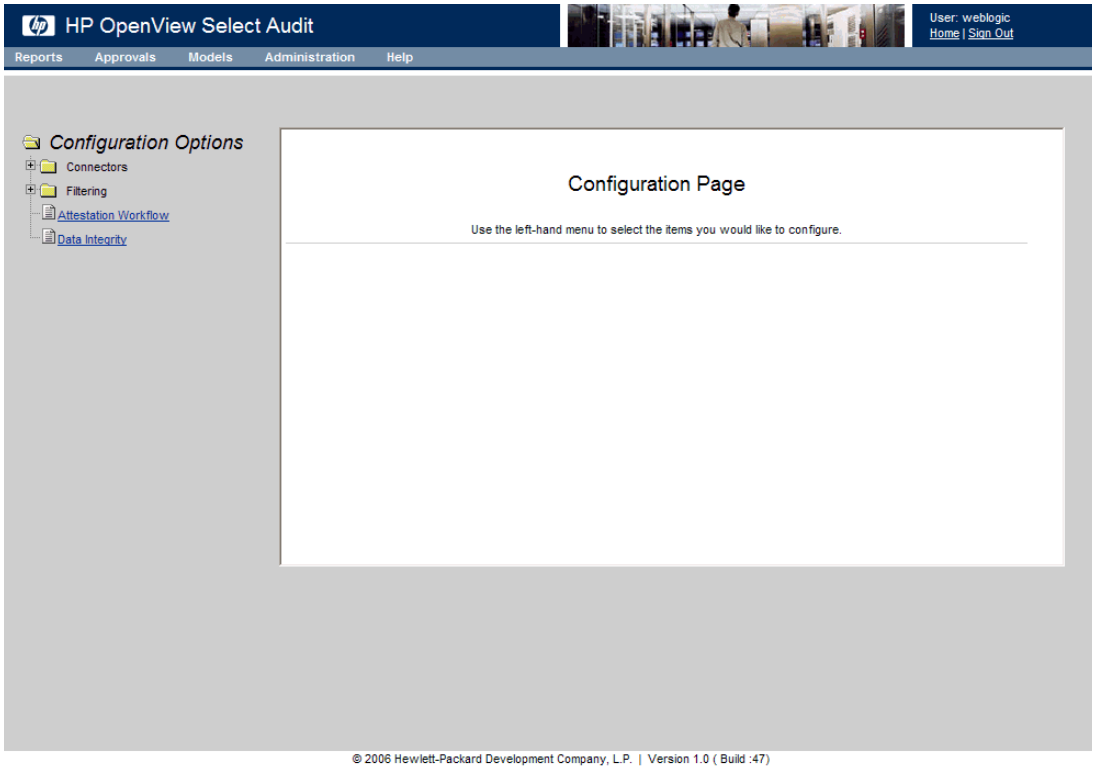
  > ➤ The administrator can use the WebLogic Administration console to add more later.

- It deploys access rules defined in the Report Center.

In the Audit Portal, you must configure the filtering options to enable integration with Select Identity.

To configure Select Identity integration

1 Select **Administration** → **Configuration**. The **Configuration** screen appears.



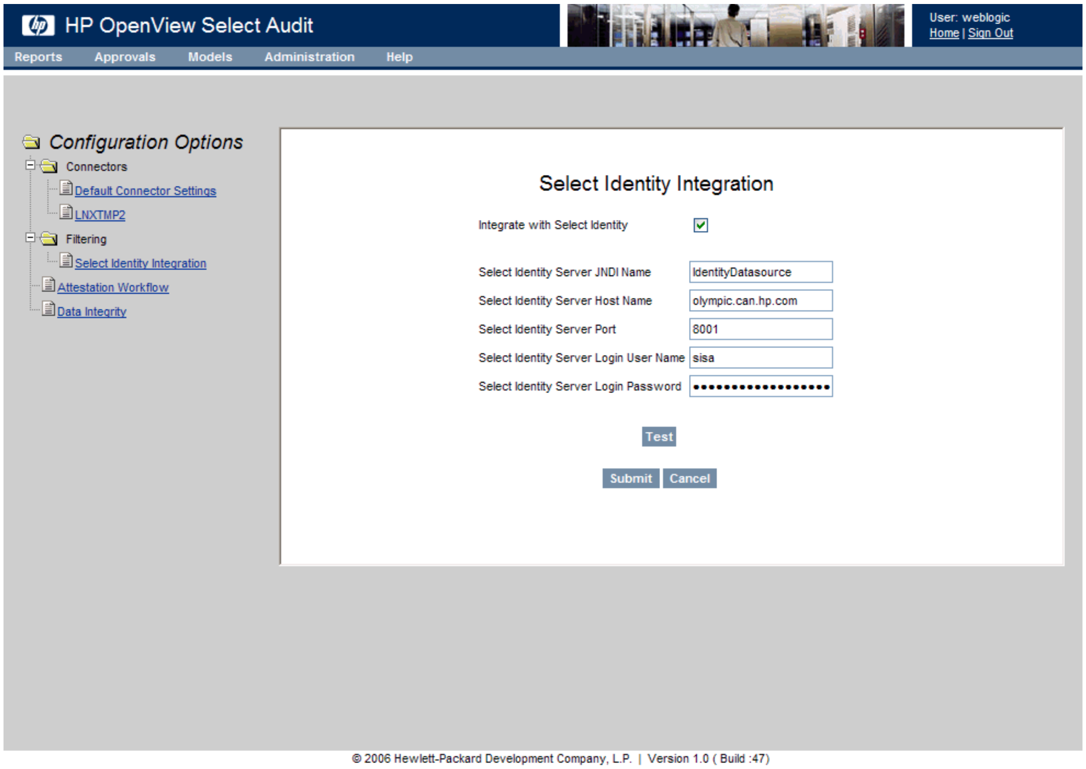
Configuration Page

Use the left-hand menu to select the items you would like to configure.

© 2006 Hewlett-Packard Development Company, L.P. | Version 1.0 (Build :47)

Figure 10 Configuration Screen

2 Click **Filtering**. The **Select Identity Integration** screen appears.



Select Identity Integration

Integrate with Select Identity ☑

Select Identity Server JNDI Name: IdentityDatasource

Select Identity Server Host Name: olympic.can.hp.com

Select Identity Server Port: 8001

Select Identity Server Login User Name: sisa

Select Identity Server Login Password: •••••••••••••••••

© 2006 Hewlett-Packard Development Company, L.P. | Version 1.0 (Build :47)

Figure 11 Select Identity Integration Screen

3. Select the **Integrate with Select Identity** check box to enable the screen fields.
4. Complete the **Select Identity Integration** screen as follows:
   - Enter the server JNDI name in the **Select Identity Server JNDI Name** field.
   - Enter the server host name in the **Select Identity Server Host Name** field.
   - Enter the server port number in the **Select Identity Server Port Name** field.
   - Enter the server login user name in the **Select Identity Server Login User Name** field.
   - Enter the server login password in the **Select Identity Server Login Password** field.
5. Click **Test** to test that the Select Identity Integration setup is valid and that both the SI server and SI database can be contacted by the Audit Server.
6. Click **Submit**. The field entries are validated, the configuration values are committed to the database tables, and the report server is restarted. The message “Changes successfully applied” appears at the top of the Select Identity Integration screen.

➤ Select Identity database information is specified in the Audit Server installer. If you configure the host and port for a different SI installation after you have installed Select Audit, you must create a new JDBC connection pool and data source, or modify the existing ones in the WebLogic console.

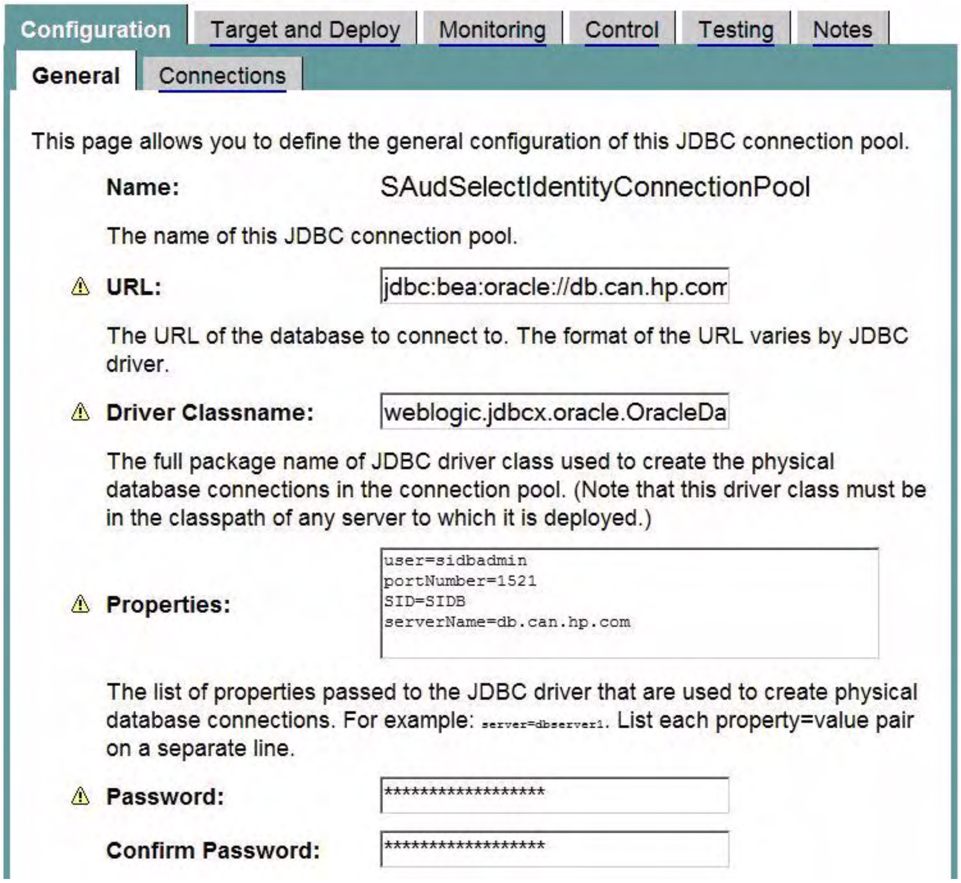
Enabling/Disabling SI Integration After Installation

After you have installed Select Audit you may need to add or modify the Select Identity database information. If you did not enable SI integration during installation, you need to create the database connection and data source pointing to the SI database. If you enabled SI integration in the installer, you may want to modify the database connection pool or data source. These tasks are performed using the WebLogic console.

If you want to turn Select Identity integration off or on, you can do so using the SI Integration screen in the Audit Portal. See To configure Select Identity integration on page 25 for more information.

To create or modify database information in the WebLogic console

1. Login to WebLogic as the administrator.
2. Go to **Services** → **Connection Pools**. The **Connection Pool Definition** screen appears.



This page allows you to define the general configuration of this JDBC connection pool.

Name: SAudSelectIdentityConnectionPool

The name of this JDBC connection pool.

⚠ **URL:** jdbc:bea:oracle://db.can.hp.com

The URL of the database to connect to. The format of the URL varies by JDBC driver.

⚠ **Driver Classname:** weblogic.jdbcx.oracle.OracleDa

The full package name of JDBC driver class used to create the physical database connections in the connection pool. (Note that this driver class must be in the classpath of any server to which it is deployed.)

⚠ **Properties:**

```
user=sidbadmin
portNumber=1521
SID=SIDB
serverName=db.can.hp.com
```

The list of properties passed to the JDBC driver that are used to create physical database connections. For example: server=dbserver1. List each property=value pair on a separate line.

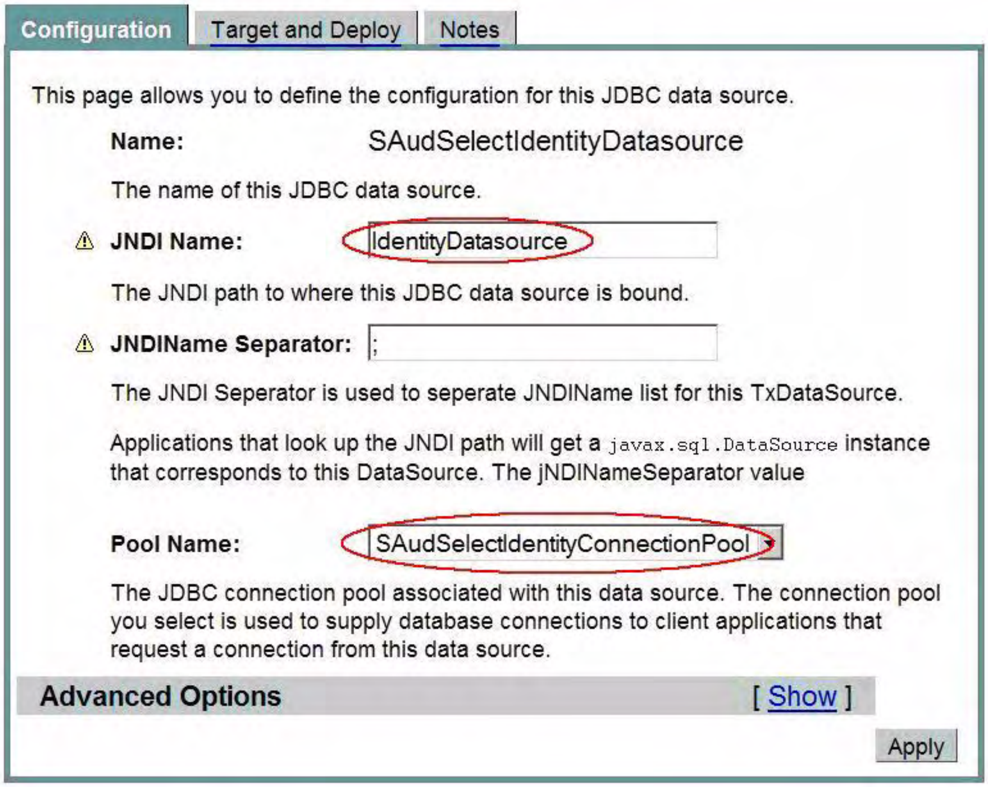
⚠ **Password:** ******************

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

Figure 12 WebLogic Connection Pool Definition Screen

3 Create a pool pointing to the SI database or if SI integration has been turned on, modify the pool that has been created by the installer.

4 Go to **Services** → **Data Sources**. The **Data Source Definition** screen appears.



This page allows you to define the configuration for this JDBC data source.

Name: SAudSelectIdentityDatasource

The name of this JDBC data source.

⚠ **JNDI Name:** IdentityDatasource

The JNDI path to where this JDBC data source is bound.

⚠ **JNDIName Separator:** ;

The JNDI Seperator is used to seperate JNDIName list for this TxDataSource.

Applications that look up the JNDI path will get a `javax.sql.DataSource` instance that corresponds to this DataSource. The jNDINameSeparator value

Pool Name: SAudSelectIdentityConnectionPool

The JDBC connection pool associated with this data source. The connection pool you select is used to supply database connections to client applications that request a connection from this data source.

Figure 13 WebLogic Data Source Definition Screen

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 Login to the Audit Portal as an administrator and follow the steps in To configure Select Identity integration on page 25.

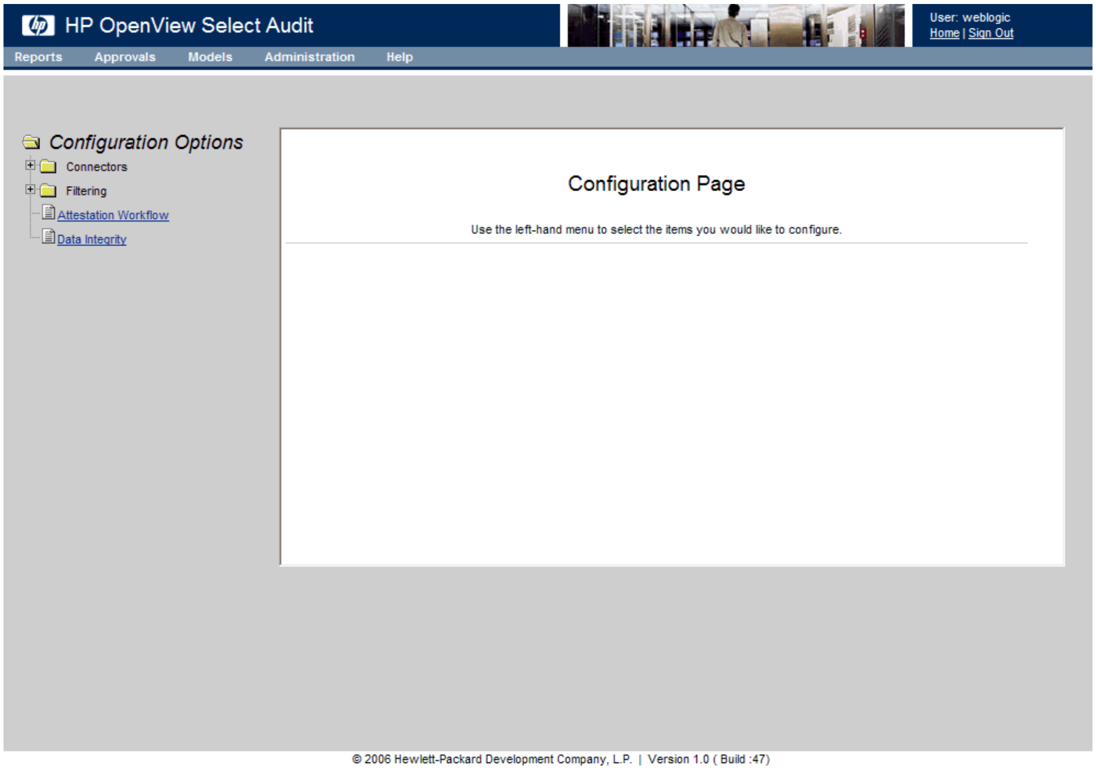
➤ Enter the data source JNDI name you just created in the **Select Identity Server JNDI Name** field.

Configuring Attestation Workflows

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. Workflows are started from the compliance model, based on the state of the model. 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 appears.



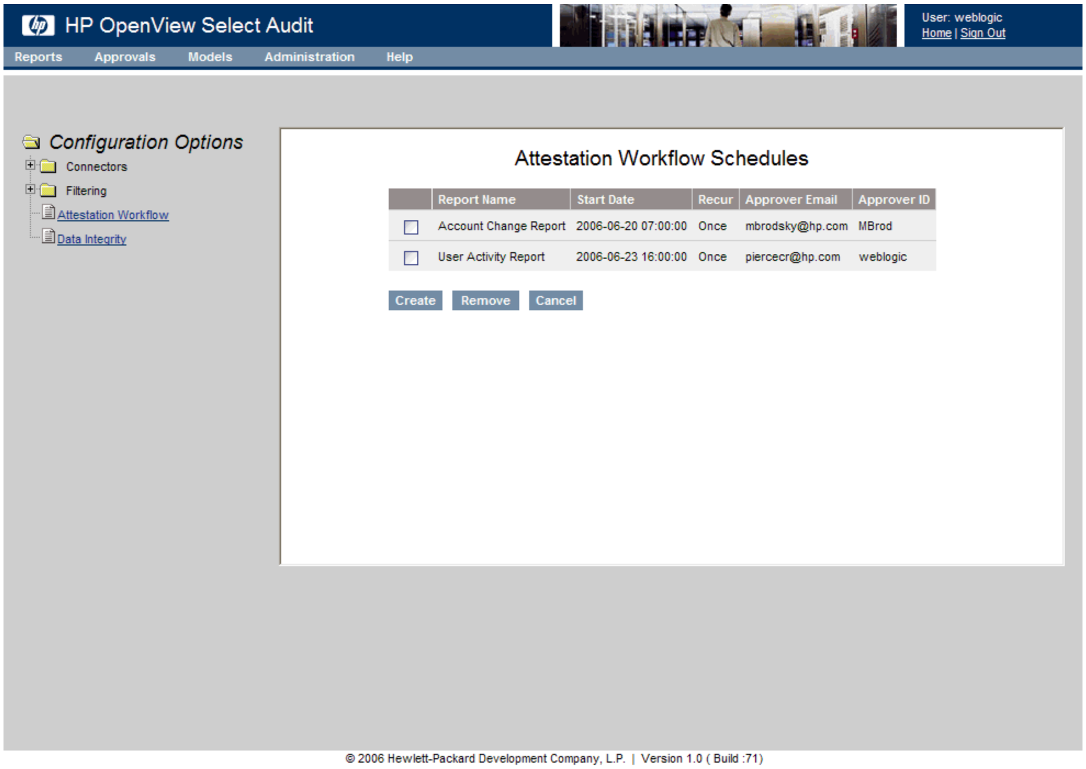
Configuration Page

Use the left-hand menu to select the items you would like to configure.

© 2006 Hewlett-Packard Development Company, L.P. | Version 1.0 (Build :47)

Figure 14 Configuration Screen

2 Click **Attestation Workflow**. The **Attestation Workflow Schedules** screen appears.



Attestation Workflow Schedules

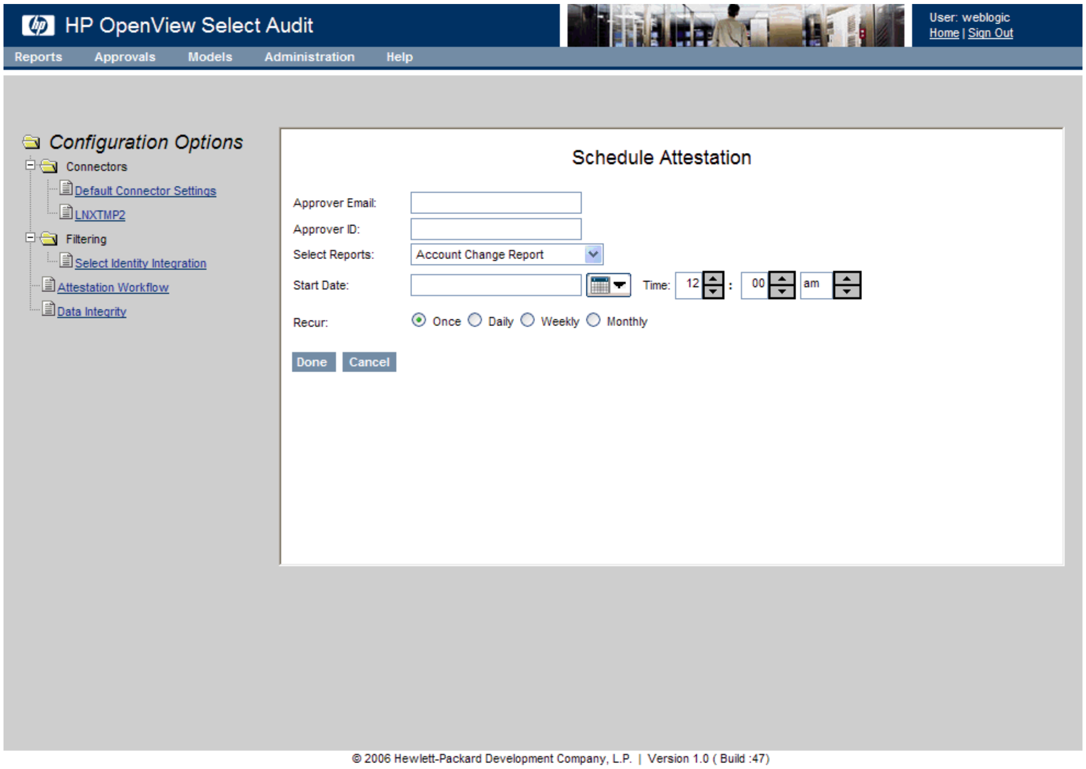
	Report Name	Start Date	Recur	Approver Email	Approver ID
□	Account Change Report	2006-06-20 07:00:00	Once	mbrodsky@hp.com	MBrod
□	User Activity Report	2006-06-23 16:00:00	Once	piercecr@hp.com	weblogic

Figure 15 Attestation Workflow Schedules Screen

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

3 To add an Attestation Workflow schedule, click **Create**. The **Schedule Attestation** screen appears.

➤ 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**.



Schedule Attestation

Approver Email:

Approver ID:

Select Reports: Account Change Report

Start Date: Time: 12 : 00 am

Recur: ● Once ○ Daily ○ Weekly ○ Monthly

© 2006 Hewlett-Packard Development Company, L.P. | Version 1.0 (Build :47)

Figure 16 Schedule Attestation Screen

4 Enter 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 Step 23 in Chapter 3 of the *HP OpenView Select Audit 1.01 Installation Guide*.

5 Enter the approver's Select Audit username 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 appears 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 82 for more information.

Configuring Data Integrity

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.

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. Users are responsible for creating and managing the keystore. Select Audit does not provide keystore management.

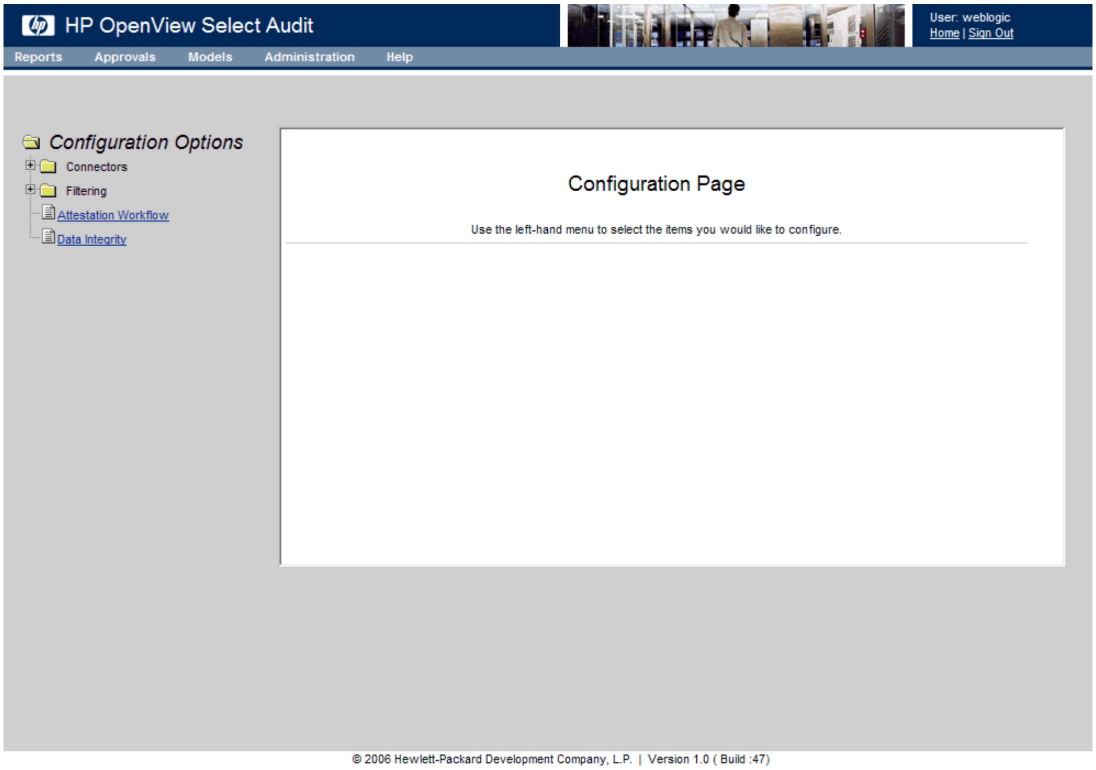
The old private key can be discarded but the old public key must be kept in the configured keystore in order to verify the old time-stamps. If the public key is not available, data verification will result in integrity errors for anything signed with the private key associated with the unavailable public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

1 Select **Administration** → **Configuration**. The **Configuration** screen appears.



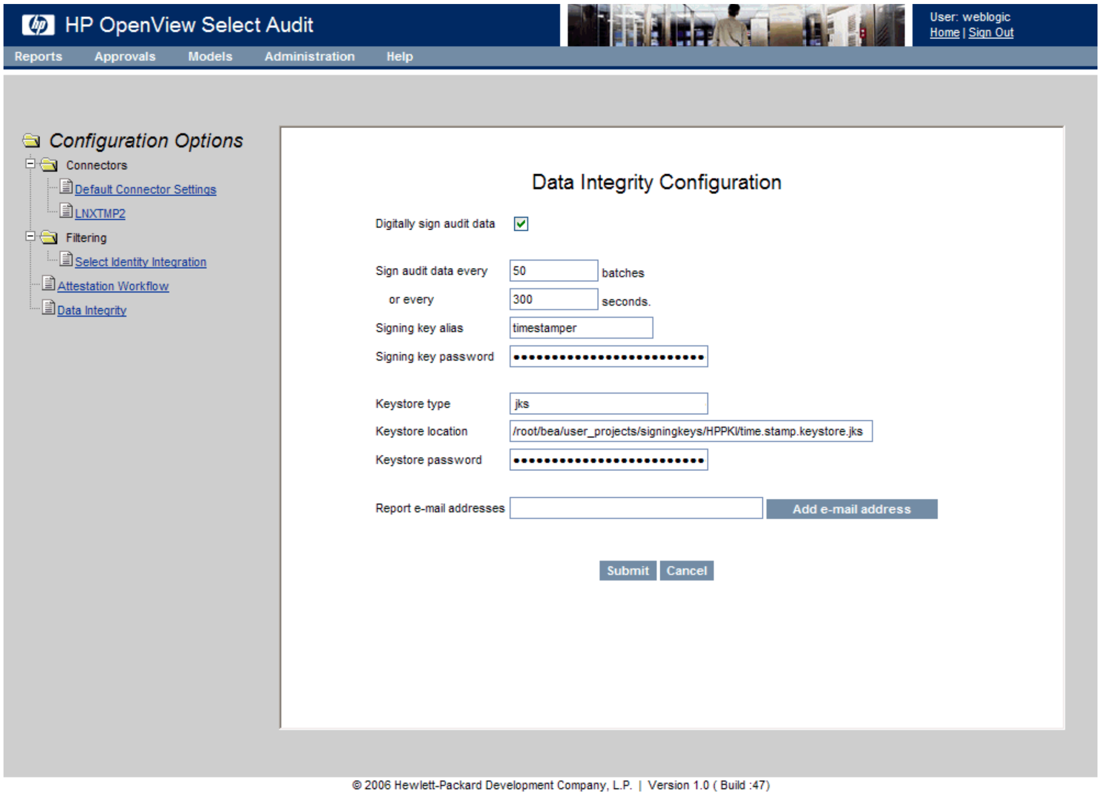
Configuration Page

Use the left-hand menu to select the items you would like to configure.

© 2006 Hewlett-Packard Development Company, L.P. | Version 1.0 (Build :47)

Figure 17 Configuration Screen

2 Click **Data Integrity**. The **Data Integrity** screen appears.



Data Integrity Configuration

Digitally sign audit data ☑

Sign audit data every 50 batches

or every 300 seconds.

Signing key alias timestamper

Signing key password ••••••••••••••••••••••••

Keystore type jks

Keystore location /root/bea/user_projects/signingkeys/HPPKI/time.stamp.keystore.jks

Keystore password ••••••••••••••••••••••••

Report e-mail addresses

Add e-mail address
Submit
Cancel
© 2006 Hewlett-Packard Development Company, L.P. | Version 1.0 (Build :47)

Figure 18 Data Integrity Screen

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 3.

Table 3Data Integrity Fields

Field	Data Entered
Sign audit data every...	Enter a value for the batch size or period of time.
Signing key alias	Enter the alias for the signing key.
Signing key password	Enter the password for the signing key.
Keystore type	Enter a type in the **Keystore Type** field.
Keystore location	Enter the path of the keystore.
Keystore password	Enter the password for the keystore.

5 Enter 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 enter 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** appears 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 WebLogic server's `JDK/jre/lib/security` directory, where JDK is the path to either the WebLogic 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 Steps 1 to 3 in To configure data integrity for Java and PKCS12 keystores on page 33.

5 Complete the **Data Integrity** screen as follows:

- Select `pkcs12` from the **Keystore type** drop-down list.
- Leave the **Signing key alias** and the **Signing key password** fields blank.
- Enter the path to the `.pfx` file the **Keystore location** field.
- Enter 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** appears at the bottom of the screen.

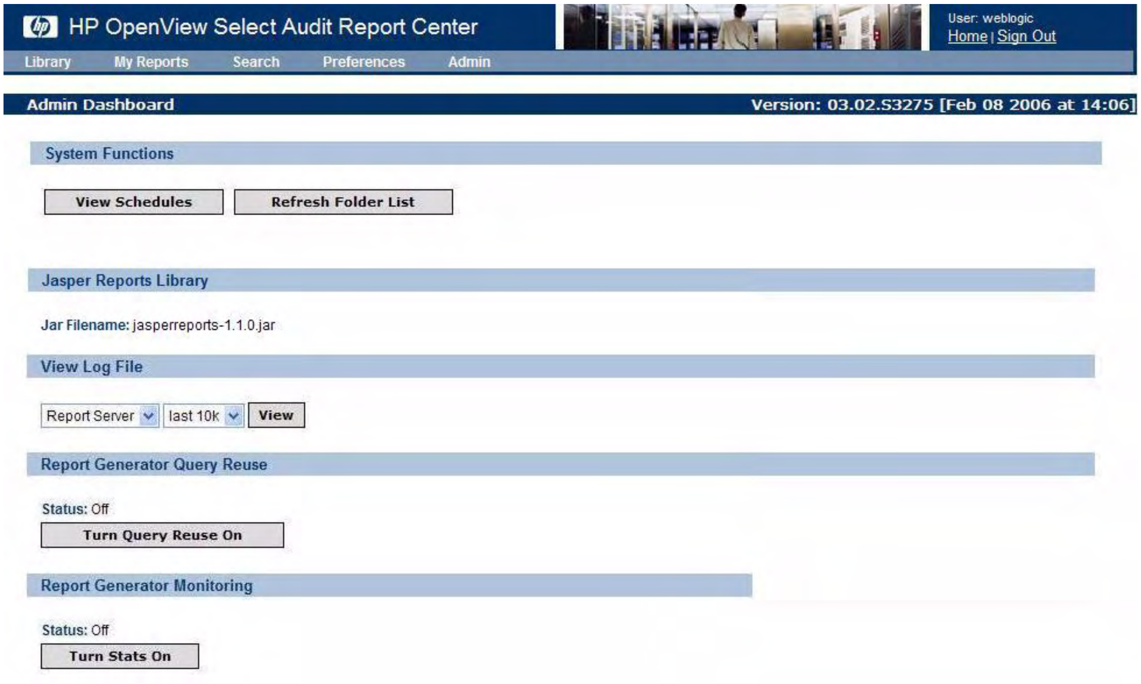
Configuring Select Audit for Keys Stored on Smart Cards and HSMs

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 via the JCA/JCE framework.

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

Configuring the Report Server

You can use the **Admin Dashboard** in the Report Center to configure various aspects of the Report Server. To open the Admin Dashboard, click **Admin** in the Report Center. The **Admin Dashboard** opens.



Version: 03.02.S3275 [Feb 08 2006 at 14:06]

Jar Filename: jasperreports-1.1.0.jar

Status: Off

Status: Off

Figure 19 Admin Dashboard

The Admin Dashboard contains five sections:

- System Functions
- Jasper Reports Library
- View Log File
- Report Generator Query Reuse
- Report Generator Monitoring

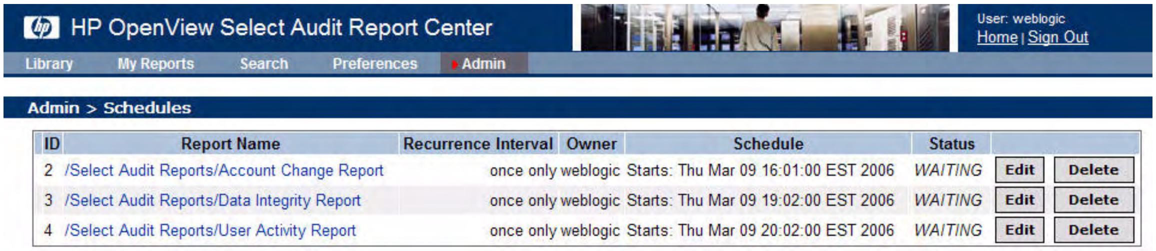
Use these sections to configure the Report Server.

Performing System Functions

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

To view schedules

Click **View Schedules**. The **Schedules** screen appears.



ID	Report Name	Recurrence Interval	Owner	Schedule	Status		
2	/Select Audit Reports/Account Change Report	once only	weblogic	Starts: Thu Mar 09 16:01:00 EST 2006	*WAITING*	Edit	Delete
3	/Select Audit Reports/Data Integrity Report	once only	weblogic	Starts: Thu Mar 09 19:02:00 EST 2006	*WAITING*	Edit	Delete
4	/Select Audit Reports/User Activity Report	once only	weblogic	Starts: Thu Mar 09 20:02:00 EST 2006	*WAITING*	Edit	Delete

Figure 20 Schedules Screen

For each schedule in the Library, the following information appears:

ID The report's ID number.

Report Name The name of the report. If you click the link, a new page appears displaying the report's properties.

Recurrence How often the report automatically produces output.

Interval When a recurrence is specified, the period between recurrences.

Owner User name of the report's owner.

Schedule The starting and ending timestamps for automatic output generation.

Status The status of the schedule. Possible values are:

- **FIRING**: schedules or tasks that are currently firing
- **PAUSED**: schedules that are paused
- **RECOVERABLE**: schedules that were firing when the system went down
- **WAITING**: schedules that are waiting to fire

Refer to Editing Report Schedules on page 112 for information about making changes to report schedules.

To refresh the folder list

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

Jasper Reports Library

This section displays the name of the `jar` file for the Library.

Viewing Log Files

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

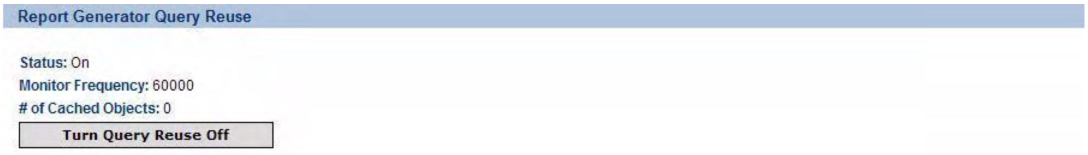
- Report Server
- SQL

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 is displayed.

Enabling Caching

1. To enable caching for the Report Server, click **Turn Query Reuse On**. A message appears at the top of the screen confirming that the caching is enabled.



Report Generator Query Reuse

Status: On
Monitor Frequency: 60000
# of Cached Objects: 0

Figure 21 Report Generator Query Reuse

The following is displayed in the **Report Generator Query Reuse** section:

- the query reuse status
- the monitor frequency
- the number of cached objects

The **Turn Query Reuse Off** button is displayed. A thread monitors the caches and clears objects as they expire.

2. To turn query reuse off, click **Turn Query Reuse Off**. A message appears at the top of the screen confirming that the caching is disabled.

➤ Changes you make to query reuse configuration in the Report Center only last for the remainder of the session. To make persistent changes, change the **query reuse monitoring frequency** property.

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

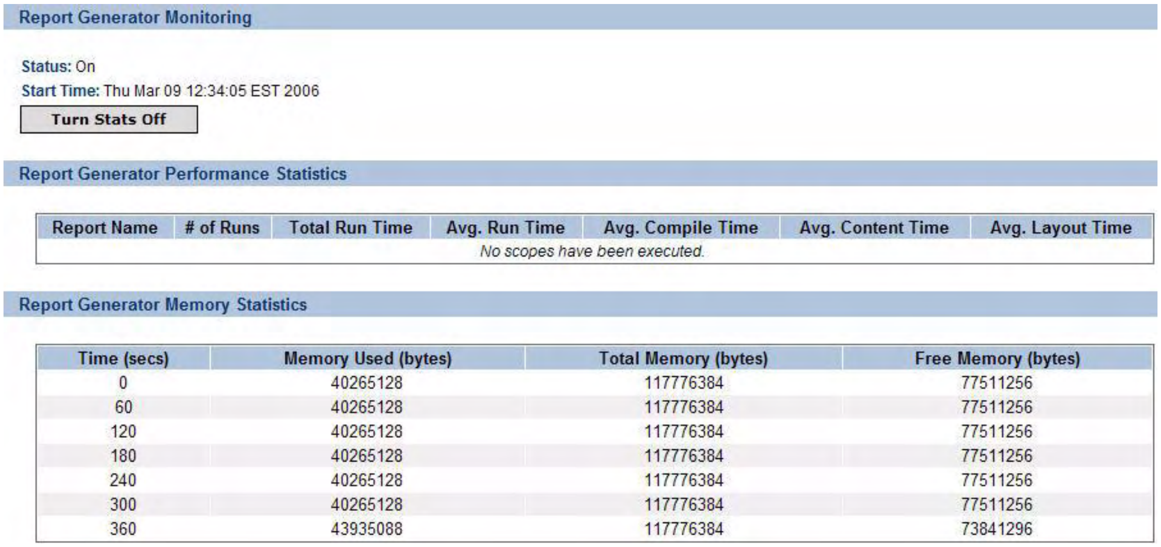
The sum of layout and content times is always accurate. This sum represents the time to execute a query, iterate over the result set, and generate the output. However, the breakdown between Layout and Content times may vary depending whether the report was successfully optimized. If optimization is successful,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

- summary calculations in the header
- in-memory sorting
- EJBs and XML datasets
- stored procedures

To view report generator statistics

1 In the **Report Generator Monitoring** section, click **Turn Stats On** to enable monitoring. A message appears 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 displayed.



Report Generator Monitoring

Status: On

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

Report Generator Performance Statistics

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

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

Figure 22 Report Generator Statistics

2 To see the properties of any monitored report, click the name in the **Report Name** column.

3 To disable statistics, click **Turn Stats Off**.

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 displayed in the audit reports. The table `GlobalUsers` 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 `jdoe` in Select Identity and `dn=jdoe` in Select Access, the mapping in the `GlobalUsers` table will be:

GUID	APPID	USERNAME
john doe	SelectIdentity	jdoe
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 display the application-specific user ID that is read from the FACT tables and stored at the time the message was normalized. Refer to *HP OpenView Select Audit 1.01 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.

By default, the user correlation feature is disabled.

To enable user correlation

Use the following steps to enable user correlation:

1. Populate the table `GlobalUsers`.

   Make sure the exact values of the `USERNAME` are inserted into the table, with no right to left spaces. Spaces will prevent finding the user name in the table.

2. Open up a SQLPlus session.
3. Connect to the database instance that houses the audit data.
   a. Copy the `UserCorrelation.sql` script located in the `.../<SelectAudit_installation_folder>/setup/db/scripts/config/` folder to your `C:` drive.
   b. Run the script as seen in the Sample SQLPlus session below.

Sample SQLPlus session

```
SQL > connect saud/*********@audit_abc.com
Connected.
SQL > @c:\usercorrelation.sql
Turn user correlation feature on or off >on
User Correlation Enabled.
```

To disable user correlation

Use the following steps to disable user correlation:

1. Open up a SQLPlus session.
2. Connect to the database instance that houses the audit data.
   a. Copy the UserCorrelation.sql script located in the .../<SelectAudit_installation_folder>/setup/db/scripts/config/ folder to your C: drive.
   b. Run the script as seen in the Sample SQLPlus session below.

Sample SQLPlus session

```
SQL > connect saud/*********@audit_abc.com
Connected.

SQL > @c:\usercorrelation.sql
Turn user correlation feature on or off >off
User Correlation Disabled.
```

Configuring a Mail Session in WebLogic

The Audit Server installer uses the default return address select-audit-workflow@localhost on the **Report Notification** screen. If you leave the default address in the **Return Email Address (From)** field, an exception will be thrown by the SMTP server when it tries to send a message that has in the default value in the **From** field. You must change the address to a valid email address using the WebLogic console after installation.

To configure a mail session

1. Open the WebLogic console.
2. Click Services/Mail in the left console pane.
3. Click **Configure a new Mail Session**.
4. Enter the JNDI and properties for the mail session.
5. Click **Apply**.

Configuring Log4j

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

If you have an existing log4j.properties or log4j.xml file in use, merge the two files together and add the new file to the WebLogic classpath. You may specify only one log4j configuration file per JVM.

Enabling logging

The default setting for all loggers is ERROR, 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 WebLogic instance should be restarted for the changes to take effect.

log4j.properties file

The log4j.properties file is shown below:

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


# Root Logger
log4j.rootCategory=OFF, MAIN, CONSOLE


# HP App Log Level - Select Audit log messages
log4j.logger.com.hp.ov=ERROR


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


# Workflow Manager Logger - Workflow Log Messages
log4j.logger.com.hp.ov.selectaudit.workflow.manager=ERROR, 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.FOPRednderer=ERROR
log4j.logger.org.apache.struts=ERROR

# 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



############## APPENDERS ###################

# CONSOLE appender writes to a console
log4j.appender.CONSOLE=org.apache.log4j.ConsoleAppender
log4j.appender.CONSOLE.layout=org.apache.log4j.PatternLayout

# MAIN appender writes all output to a file [sa.log]
log4j.appender.MAIN=org.apache.log4j.RollingFileAppender
log4j.appender.MAIN.File=$LOG_DIR$/sa.log
log4j.appender.MAIN.MaxFileSize=2000KB
log4j.appender.MAIN.MaxBackupIndex=10
log4j.appender.MAIN.layout=org.apache.log4j.PatternLayout
log4j.appender.MAIN.layout.ConversionPattern=%d{dd-MMM@HH:mm:ss,SSS} %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=$LOG_DIR$/wf.log
log4j.appender.WORKFLOW.MaxFileSize=2000KB
log4j.appender.WORKFLOW.MaxBackupIndex=10
log4j.appender.WORKFLOW.layout=org.apache.log4j.PatternLayout
log4j.appender.WORKFLOW.layout.ConversionPat-
tern=%d{dd-MMM@HH:mm:ss,SSS} %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=$USER_INSTALL_DIR$/dist/reporting/
ReportServer/WEB-INF/logs/ScopeServerLog.txt
```

```
log4j.appender.SERVER-FILE.MaxFileSize=10MB
log4j.appender.SERVER-FILE.MaxBackupIndex=10
log4j.appender.SERVER-FILE.layout=org.apache.log4j.PatternLayout
log4j.appender.STOPPER.layout.ConversionPattern=%d{ISO8601} [%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=$USER_INSTALL_DIR$/dist/reporting/ReportS-
erver/WEB-INF/logs/AuditRdlExecutionLog.txt
log4j.appender.SQL-FILE.MaxFileSize=10MB
log4j.appender.SQL-FILE.MaxBackupIndex=10
log4j.appender.SQL-FILE.layout=org.apache.log4j.PatternLayout
log4j.appender.SQL-FILE.layout.ConversionPattern="%d{ISO8601} [%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=$USER_INSTALL_DIR$/dist/reporting/
ReportServer/WEB-INF/logs/PerformanceLog.txt
log4j.appender.PERFORMANCE-FILE.MaxFileSize=10MB
log4j.appender.PERFORMANCE-FILE.MaxBackupIndex=10
log4j.appender.PERFORMANCE-FILE.layout=org.apache.log4j.PatternLayout
log4j.appender.PERFORMANCE-FILE.layout.ConversionPattern=%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

If the Select Audit Administrator password (for example, “weblogic”) is changed in a WebLogic Console 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)

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

Running the Administrator Password Tool

Use the following steps to the Administrator password.

1. Make sure your jdk1.4 is “visible” by typing `java` in the command line. If Java is not found, add the jdk1.4 `bin` directory to the system `PATH`.
2. Check the Java version:

   ```
   java -version
   ```

   The version should be either 1.4.2_08_b03 or the JVM installed with the Audit Connector. The Administrator Password tool may not work properly if the Java version is not one of these versions.
3. Run the `adminpwd` shell (batch) script.

   ➤ The full path to this directory is a mandatory parameter for both the Windows and UNIX `adminpwd` shell scripts (`/root/bea/weblogic81/server/lib`).

   If you do not enter the full path, the following line will be displayed:

   - On Windows:

     ```
     Usage:

     For Audit Server: adminpwd -s BEA_HOME\weblogic81\server\lib
     [-d]

     For Connector   : adminpwd -c [-d]
     ```

   - On UNIX:

     ```
     Usage:

     For Audit Server: adminpwd.sh -s BEA_HOME/weblogic81/server/
     lib [-d]

     For Connector   : adminpwd.sh -c [-d]
     ```

   Use the `-d` option to display the debug information.

- On Windows:

a. Run `adminpwd -s c:\bea\weblogic81\server\lib` to change the Audit Server password files.

b. Run `adminpwd -c` to change the Audit Connector password file.

➤ Assume that `BEA_HOME` is `c:\bea`.

- On UNIX:

a Run `./adminpwd.sh -s /root/bea/weblogic81/server/lib` to change the Audit Server password files.

b Run `./adminpwd.sh -c` to change the Audit Connector password file.

➤ Assume that `BEA_HOME` is `/root/bea`.

4 Follow the screen prompts. The following message appears when the password configuration successfully completed.

```
Password has been successfully changed.
```

4 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 OpenView Select Identity* documentation for more information about configuring Select Identity.

This chapter contains the following topics:

- Select Identity Permissions on page 53
- Select Audit Report Access Control on page 55
- Select Identity and J2EE Integration on page 59
- Filtering on page 60

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 Auditor role

An Auditor is a special user in Select Audit who can view all the reports and all the events. Members of this role have access to all the reports and events in Select Audit. For 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 Indentity 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 permission

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 permission

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 manage all services and all contexts.
- An administrator can manage all services, certain context attributes and all attribute values.
- An administrator can manage all services, certain context attributes and certain attribute values.
- An administrator can manage certain services (thus certain context attributes because one service has only one context attribute) and all context attribute values.
- An administrator can manage certain services and certain context attribute values.

User Management permission

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, i.e. 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 kinds of permission data need:

- 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/context list. The Web Services API authenticates Select Audit as a special administrator in Select Identity and passes the login 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 login ID must be the same as the administrator ID used in Select Identity.

If the Select Identity server or database is down, or a login 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 login.

➤ 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 above listed Select Identity reports, 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, for example 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, UserDelete, etc. 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 57 for information about how SI 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 4 Select Identity and J2EE or Select Access Report Access

	Users			Admins	Auditors
	SI User	**Non-SI User**	**SI is unavailable**		
Account Change Report	If the user is allowed in SI on certain report types, the user will have these permissions on related reports: • Read • Execute • Schedule • Ad Hoc	Denied	Denied	Full permissions including: • Read • Write • Delete • Execute • Schedule • Ad Hoc • View permissions • Grant permissions • Revoke permissions	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	Read, Execute, Schedule, Ad Hoc				
Data Integrity Report	Read, Execute, Schedule, Ad Hoc				
Raw Message Report	Denied				

Table 5 lists the Select Identity report types needed to view Select Audit reports.

Table 5 Select Audit Reports Access

To be able to see this Select Audit report	You need ANY of these report types allowed in SI
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 5 Select Audit Reports Access (cont'd)

To be able to see this Select Audit report	You need ANY of these report types allowed in SI
Password Management Report	AuditUser
	AuditUserLogin
	AuditUserPassword
Security Events Report	AuditUser
	AuditUserLogin
	AuditUserPassword
Service Report	AuditService
System Activity Report	*Any report types*
User Activity Report	*Any report types*
User Summary Report	AuditUserSummary
Workflow Events Report	AdminConfiguration
	AuditService
	AuditUser
	AuditUserCreation
	AuditUserDeletion
	AuditUserLogin
	AuditUserPassword
	AuditUserTermination

Select Identity and J2EE Integration

Authentication is performed by WebLogic-supported authenticators. Users and roles are defined in the WebLogic security realm. Select Audit comes with support for three roles:

- Users
- Administrators
- Auditors (Users who are Auditors are allowed to view all the reports.)

To integrate with Select Identity, roles are defined in Select Audit, each of which represent a report type in Select Identity. Select Audit has pre-defined access rules for each role. 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 WebLogic realm.

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 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.

The SiDirectoryProvider is not a real directory provider. It is a wrapper of a real directory provider. The real provider is Jasper's WebLogic directory provider which is used to load the user attributes from the relevant directories.

Filtering

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 25 for more information.

5 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.

➤ 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 OpenView Select Access* documentation for more information about configuring Select Access.

It contains the following topics:

- Integrating Select Access with Select Audit on page 61
- Report Access on page 70

Integrating Select Access with Select Audit

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

1. Create Policy Builder entries.
2. Choose an Identity Location.
3. Copy the required Select Access files.
4. Unassign the `jar` file.
5. Configure a generic enforcer.
6. Create the `bea.enforcer.properties` file.
7. Modify `startWebLogic.cmd`.
8. Create `SARealm`.
9. Set `SARealm` as the default realm.
10. Repackage `auditserver.ear` with Select Access settings.
11. Set `SelectAccessEnable` to true.
12. Modify the Report Server `web.xml` file.
13. Modify `directory.xml` for Select Access.
14. 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`.

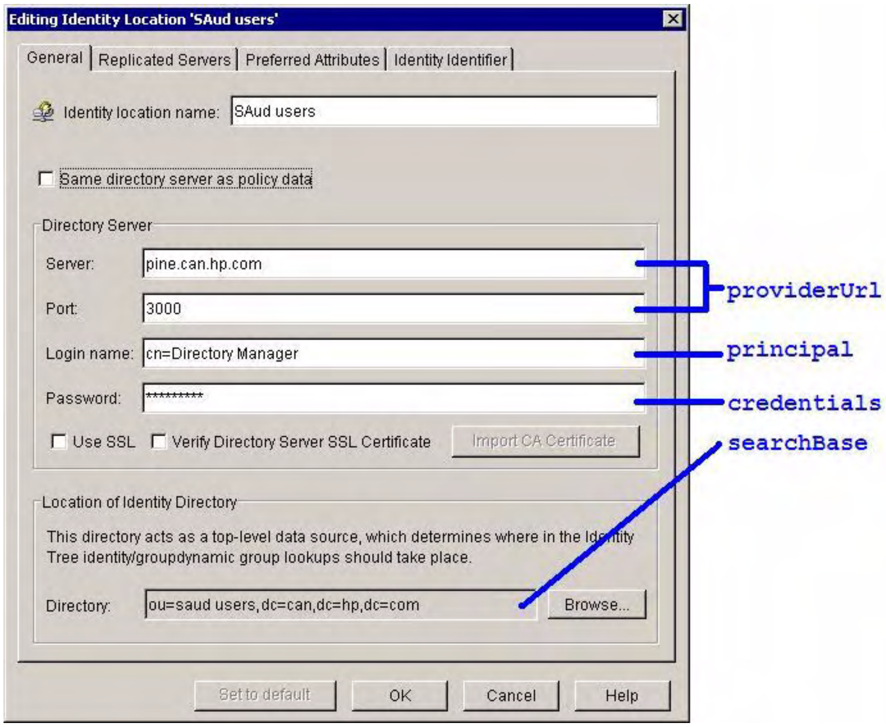
2 Copy the `selectaudit-login.html` file from the SA integration folder to the Select Access install folder, under the `content` folder, for example, `C:\Program Files\HP OpenView\Select Access\content`.

Task 2: Choose an Identity Location

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

1 Choose 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 13: Modify the directory.xml file on page 69.



Editing Identity Location 'SAud users'

Identity location name: SAud users

□ Same directory server as policy data

Directory Server

Server: pine.can.hp.com

Port: 3000

Login name: cn=Directory Manager

Password: *********

□ Use SSL □ Verify Directory Server SSL Certificate

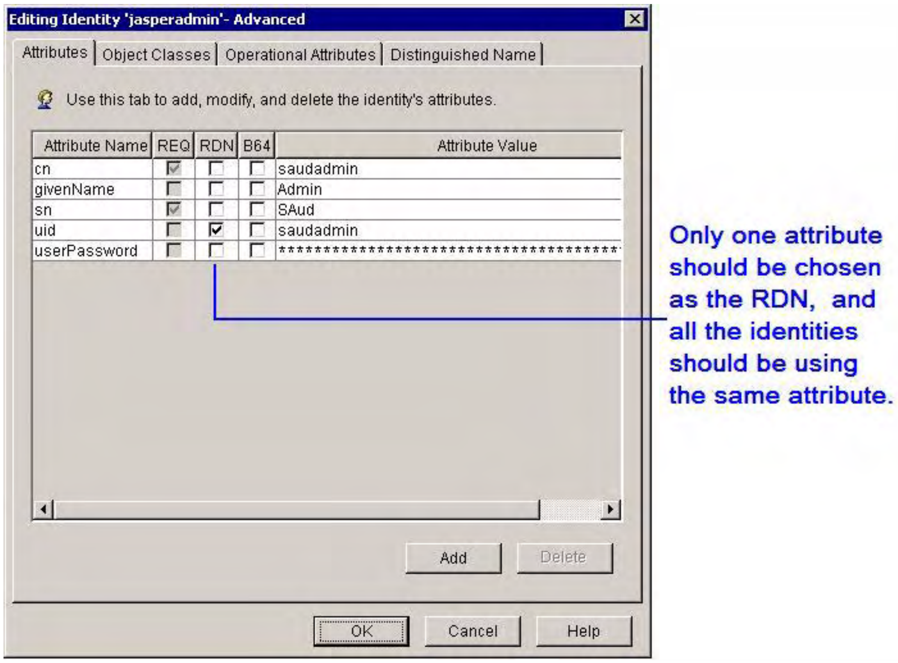
Location of Identity Directory

This directory acts as a top-level data source, which determines where in the Identity Tree identity/groupdynamic group lookups should take place.

Directory: ou=saud users,dc=can,dc=hp,dc=com

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 chosen as the RDN.

➤ In Task 13: Modify the directory.xml file on page 69, this RDN attribute will be the `userSearchAttribute`.

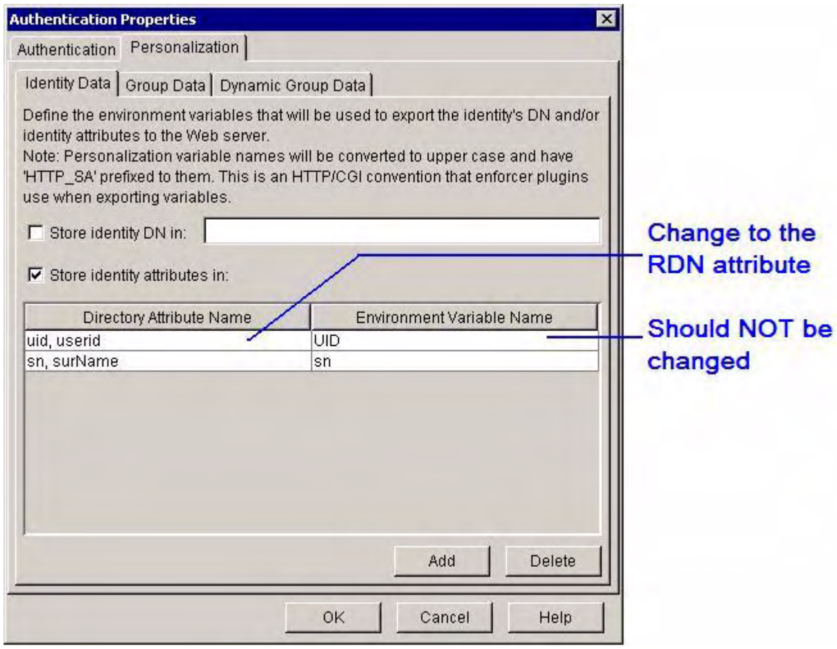


Use this tab to add, modify, and delete the identity's attributes.

Attribute Name	REQ	RDN	B64	Attribute Value
cn	☑	☐	☐	saudadmin
givenName	☐	☐	☐	Admin
sn	☑	☐	☐	SAud
uid	☐	☑	☐	saudadmin
userPassword	☐	☐	☐	**

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, go to **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`.



Define the environment variables that will be used to export the identity's DN and/or identity attributes to the Web server.
Note: Personalization variable names will be converted to upper case and have 'HTTP_SA' prefixed to them. This is an HTTP/CGI convention that enforcer plugins use when exporting variables.

☐ Store identity DN in:

☑ Store identity attributes in:

Directory Attribute Name	Environment Variable Name
uid, userid	UID
sn, surName	sn

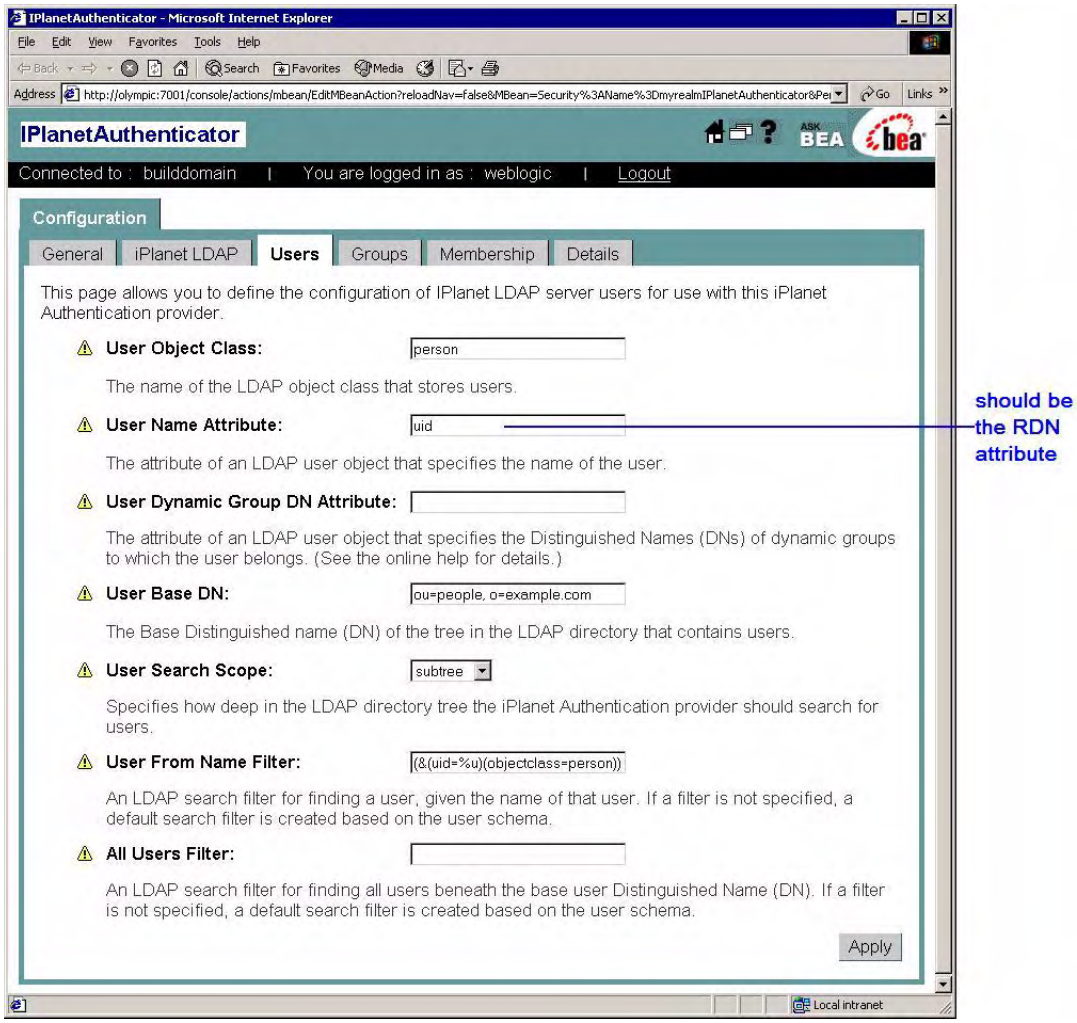
Change to the RDN attribute

Should NOT be changed

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:


IPlanetAuthenticator - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://olympic:7001/console/actions/mbean/EditMBeanAction?reloadNav=false&MBean=Security%3AName%3DmyrealmIPlanetAuthenticator&Pe
Go Links
ASK BEA
bea
Configuration
General iPlanet LDAP Users Groups Membership Details
Apply
Local intranet

IPlanetAuthenticator

Connected to : builddomain | You are logged in as : weblogic | Logout

This page allows you to define the configuration of IPlanet LDAP server users for use with this iPlanet Authentication provider.

User Object Class: person

The name of the LDAP object class that stores users.

User Name Attribute: uid

The attribute of an LDAP user object that specifies the name of the user.

User Dynamic Group DN Attribute:

The attribute of an LDAP user object that specifies the Distinguished Names (DNs) of dynamic groups to which the user belongs. (See the online help for details.)

User Base DN: ou=people, o=example.com

The Base Distinguished name (DN) of the tree in the LDAP directory that contains users.

User Search Scope: subtree

Specifies how deep in the LDAP directory tree the iPlanet Authentication provider should search for users.

User From Name Filter: (&(uid=%u)(objectclass=person))

An LDAP search filter for finding a user, given the name of that user. If a filter is not specified, a default search filter is created based on the user schema.

All Users Filter:

An LDAP search filter for finding all users beneath the base user Distinguished Name (DN). If a filter is not specified, a default search filter is created based on the user schema.

should be the RDN attribute

3 Create identities and groups used by Select Audit.

a In the Identity Location, create the following:

- 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.
- 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 choose the valid RDN attribute. The RDN attribute value “weblogic” will be used in Task 13: Modify the directory.xml file on page 69, 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>`*`/weblogic81/server/lib/mbeantypes/` where *`<BEA_HOME>`* represents the WebLogic home directory.
- Copy the `SAPrincipal.jar` file from the `solution/weblogic` folder to *`<BEA_HOME>`*`/weblogic81/server/lib/sa`.
- Copy the following files from the `servletfilter.war` file to *`<BEA_HOME>`*`/weblogic81/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) to `<BEA_HOME>/weblogic81/server/lib/sa`.
2. Copy `setEnv.bat` (Windows) or `setEnv.sh` (UNIX) to `<BEA_HOME>/weblogic81/server/lib/sa` and modify the it accordingly.
3. Run one of the following:

   For Windows:

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

   For UNIX:

   ```
   ./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/`.

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 startWebLogic.cmd

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

For UNIX:

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

SA_CLASSPATH="${SA_LIB}"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/bcprov-jdk14.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/SAPrincipal.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/castor-0.9.3.19-xml.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/EnforcerAPI.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/jdom.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/ldapjdk.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/protomatter.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/msgsresources.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/shared.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/xercesImpl.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/xml.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/jakarta-oro-2_0.jar"
SA_CLASSPATH="${SA_CLASSPATH}:${SA_LIB}/xml-apis.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%\SAPrincipal.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\castor-0.9.3.19-xml.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\EnforcerAPI.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\jdom.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\ldapjdk.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\protomatter.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\msgsresources.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\shared.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\xercesImpl.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\xml.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\jakarta-oro-2_0.jar
set SA_CLASSPATH=%SA_CLASSPATH%;%SA_LIB%\xml-apis.jar

set WEBLOGIC_CLASSPATH=%WEBLOGIC_CLASSPATH%;%SA_CLASSPATH%

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

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. Enter `DefaultAdjudicator` and click **Create**.
5. In the **Details** tab, uncheck **Require Unanimous Permit** and click **Apply**.
6. In the **Authentication** tab, add the authenticators listed below in the following order:
   - SAAuthenticator
   - DefaultAuthenticator
   - SAIdentityAsserter (uncheck **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 In the WebLogic console, click **Security**.

2 In the **Default Realm** field, select **SARealm**.

3 Click **Apply**.

Task 10: Repackage the auditserver.ear file

You must repackage the `auditserver.ear` file with Select Access settings.

1 Copy the `auditserver.ear` file to your own folder.

➤ The `ear` file is usually located in `/opt/OV/SelectAudit/auditserver/dist`.

2 Copy the `build.sh` and `setEnv.sh` files to the same folder.

➤ These two scripts are available in the `Extras` folder on the product CDs.

3 Modify `setEnv.sh` to point the `BUILD_DIR` to the current folder.

4 Check that the `JAVA_HOME` is set to the correct location.

5 Do one of the following:

- If you are enabling the integration with Select Access, run `./build.sh sa`.
- If you are disabling the integration with Select Access, run `./build.sh bea`.

The script will re-package the `auditserver.ear` file. The original `auditserver.ear` file will be renamed as `auditserver.ear.backup`.

6 Overwrite the `auditserver.ear` file in the Select Audit installed folder (`/opt/OV/SelectAudit/auditserver/dist`).

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 Report Server web.xml file

1 In `/opt/OV/SelectAudit/auditserver/dist/reporting/ReportServer/WEB-INF`, delete the `web.xml` file.

2 Rename the `web.xml.sa` file to `web.xml` if you are switching from BEA to Select Access. Rename the `web.xml.bea` file if switching from Select Access to BEA.

Task 13: Modify the directory.xml file

1 In /opt/OV/SelectAudit/auditserver/dist/reporting/ReportServer/WEB-INF/conf, rename the directory.xml file to directory.xml.bea.

2 Modify directory.xml.sa as follows:

a Replace <credentials>password</credentials> with <credentials isEncrypted="true">$SA_LDAP_LOGIN_PSWD_ENCRYPT$</credentials> using the following command:

```
<install_dir>  java -cp "setup/ReplaceText.jar;
     dist/reporting/ReportServer/WEB-INF/lib/scopeserver.jar;
     dist/reporting/ReportServer/WEB-INF/lib/log4j.jar"
     com.hp.ov.selectaudit.build.ModifyTextFileIAProps
     "dist/reporting/ReportServer/WEB-INF/conf/directory.xml"
     "SA_LDAP_LOGIN_PSWD_ENCRYPT=<password>”
```

➤ The jar files are provided in a .zip file with the *Select Audit Patch 1 Upgrade Guide*. Refer to “Step 8: Update external files” in Chapter 1 of the *HP OpenView Select Audit 1.01 Upgrade Guide* for more information.

b Change the providerUrl, principal and searchBase to match the information for your Identity Location directory server.

c Set the userSearchAttribute to the RDN attribute of the identities, for example, uid.

d Set the adminUser to the weblogic.

e Change the adminRole to the Select Audit Administrators.

3 Copy the directory.xml.sa file to directory.xml.

Task 14: Restart WebLogic

1 Restart WebLogic.

2 Login to Select Audit using the uids of users in your Select Access Identity Location.

Report Access

Report access is set in the Report Center using the **Permissions** screen. Refer to Managing Reports on page 94 for more information about setting permissions.

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

Table 6 Report Access with J2EE or Select Access Integration

	Users	Administrators	Auditors
Account Change Report	Read Execute Schedule Ad Hoc	Full permissions including: • Read • Write • Delete • Execute • Schedule • Ad Hoc • View permissions • Grant permissions • Revoke permissions	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			
Raw Message Report	Denied		

6 Models

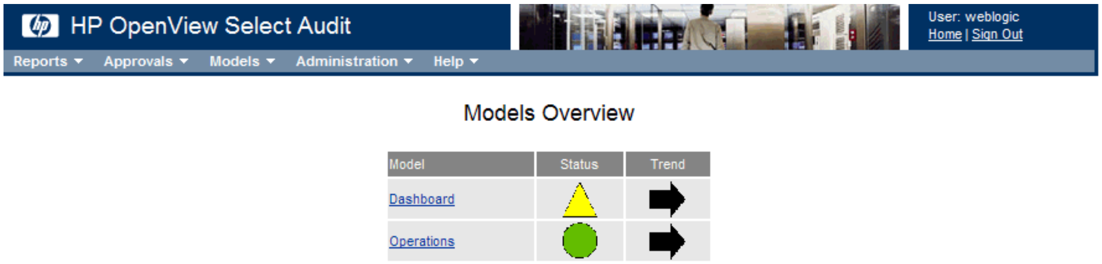
This chapter describes Select Audit models, the model report structure, the Model Loader, and how to use models in Select Audit. The **Models** menu is used to obtain a high-level view of the loaded models, view reports generated by the Operations model, view compliance reports generated by the loaded compliance models, and load, export and update models.

This chapter contains the following topics:

- Overview on page 71
- Operations Model on page 71
- Model Loader on page 75
- Loading the Model in the Audit Portal on page 77

Overview

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



Models Overview

Model	Status	Trend
Dashboard	▲	➡
Operations	●	➡

Figure 23 **Models Overview Screen**

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. The model is run four times a day at 1:00 am, 7:00 am, 1:00 pm and 7:00 pm (based on the machine time).

See Appendix B, Operations Model Thresholds for information about the Operations model thresholds.

Model Reports

The **Operations** folder, under the **Models** folder in the Report Center Library contains reports generated by the Operations model.

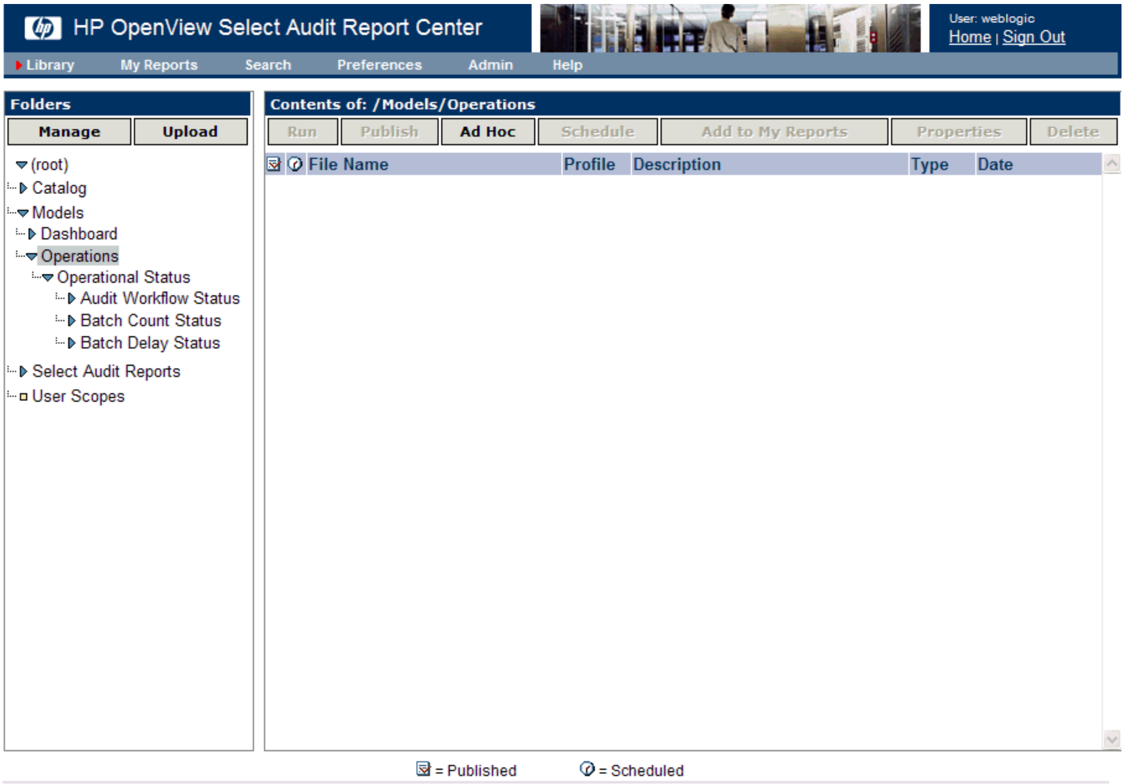


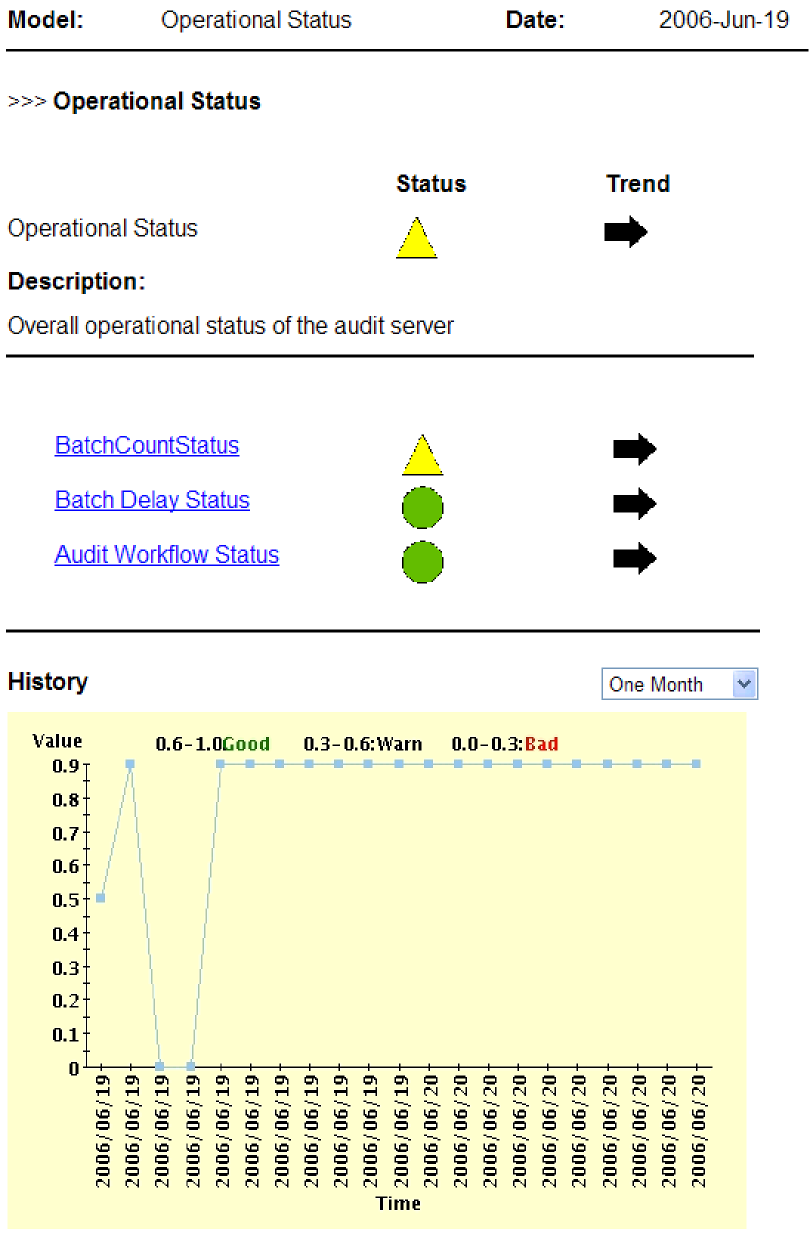
Figure 24 Operations Model Reports Folder

The Operations reports are categorized in the Operational Status subfolder. You can drill down through the subfolder to view smaller levels of data. The Operations reports are run four times a day at 1:00 am, 7:00 am, 1:00 pm and 7:00 pm (based on the machine time).

The report data is represented in a tree structure and shows the results of the analysis of the model node fact data.

Model Report Structure

The model reports show the status, trend and status history of a metric. An example of a model report is shown in Figure 25.



Model: Operational Status **Date:** 2006-Jun-19

>>> **Operational Status**

	Status	Trend
Operational Status	▲	➡

Description:

Overall operational status of the audit server

BatchCountStatus	▲	➡
Batch Delay Status	●	➡
Audit Workflow Status	●	➡

History One Month

Figure 25 Sample Model Report

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:

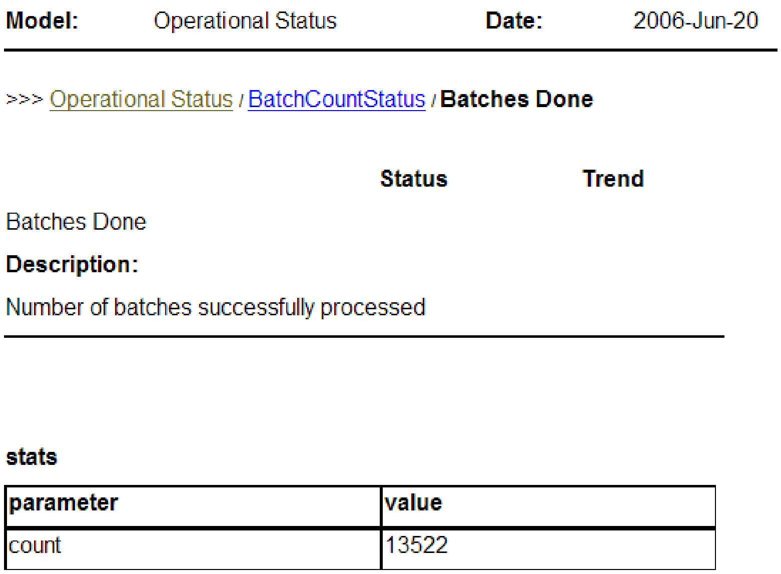
🟢	compliance level is good
▲	compliance level is adequate
🟥	compliance level is poor

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. Some child node reports do not have show a status or trend, as shown in Figure 26.



Model: Operational Status **Date:** 2006-Jun-20

>>> Operational Status / BatchCountStatus / **Batches Done**

Status **Trend**

Batches Done

Description:

Number of batches successfully processed

stats

parameter	value
count	13522

Figure 26 Model Report Without Status

These reports show low-level data elements that compute the model data using data directly from the database. The output and parameters of the element are listed in the Stats table.

History status

The bottom section of the model report shows the status history. The status history is recorded each time the model runs. The graph maps status values over a period of time. The X axis shows the time period which is set using the drop-down list at the top of the graph. The following time periods are available:

- One Month
- Three Months
- Half Year
- One Year

The Y axis represents a scale of "goodness" between 0 and 1, where 0 is red and 1 is green for that particular node.

Deleting Model Reports

You can delete model reports using the Report Center. If you want to delete model reports, you must delete all the reports at each level. Deleting an upper-level report does not automatically delete related reports at a lower level.

➤ When you delete a model from the Audit Server, the reports generated by that model are not deleted.

Model Loader

HP Openview Select Audit includes the ability to load different types of models into the audit modeller.

Model Loader Features

The Model Loader enables users to load and remove models as necessary. The audit modeller has the ability to run multiple models on the same server.

The modeller is a compliance tool that allows users to view reports based on predefined thresholds. These thresholds are set based on compliance criteria such as, if a user enters a wrong password more than a threshold of three times, raise an alert and indicate a compliance "warning" status based on a specific time period.

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 and generate reports based on compliance specifications. The Operations model is included with the Audit Server upon installation. The compliance models are optional add ons. Compliance models for different policies and regulations will be made available periodically.

The model definition is contained within a directory generated as random numbers, under the `models` directory created by the Audit Server installer, for example, `<config dir>/models/1027774882/*`.

Model Tree definition

The main file in the Model Tree is complete.xml. This file contains the root nodes for the model. Subsequent tree nodes can be defined either in predefined node xml files, for example, SAGroups.xml to define a Select Access group, or they can be defined inside the complete.xml as one complete file. The complete.xml file begins with a root tag <Package> with the ID and name as attributes.

Model database/Report definitions

The DBdesc_saudv2.xml file defines the views that are used. This file is referenced in the TRDefault properties file as the DBFile key. This directory includes the SQL file that generates the views, as well as the model graphics definition file for report generation on every tree node defined in the Model Tree Definition. For example, if there was a SAGroups.xml tree node defined, a graphics file with the same name must be defined in the reports definition directory. The Label tag name that is defined in the xml file is the name that is used to create a report directory in Jasper under the main Reports directory in the Report Library.

Model properties file

The TRDefault properties file contains values for how the model interacts with the database and the report generation process. It contains the linkage between the model graphics, the reports and the model database.

Loader Screens

The models are loaded into Select Audit using the Audit Portal. There are two screens:

- the Loader screen
- the loaded model Configuration screen

Model Loader screen

The **Model Loader** screen is used to upload the model file. The Model Loader:

- checks that the model file is a zip file. The loader checks for a .zip ending and makes sure the file is a real zip file.
- checks that 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 displayed. 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 WebLogic 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.

Model Configuration screen

The left-hand tree view displays the name of the loaded models with links to a configuration page for each model. The **Operations Model Configuration** screen has three buttons, **Update**, **Export** and **Cancel**. The compliance model **Configuration** screens have two buttons: **Export** and **Delete**.

The **Update** button loads a modified model `zip` file.

The **Export** button zips up the model directory and downloads the `zip` file to the client browser machine.

The **Delete** button deletes the model from the model directory and all the files in the directory.

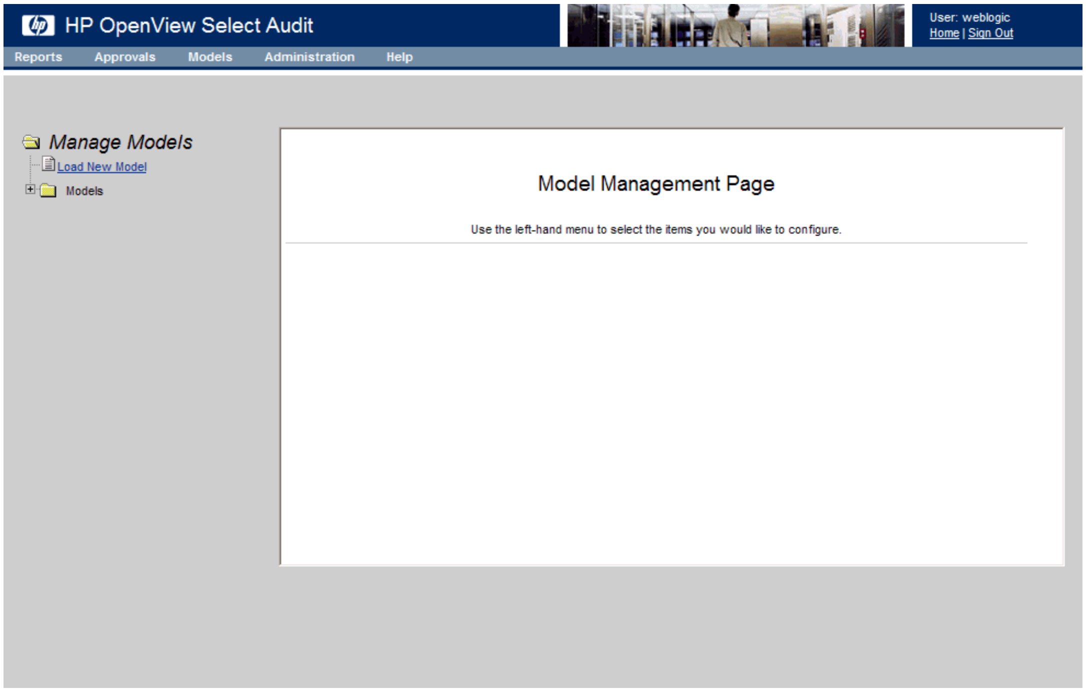
Model File

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`.

Loading the Model in the Audit Portal

You can configure the models used in Select Audit using the **Models** menu on the Audit Portal.

1 Select **Models** → **Manage Models**. The **Model Management** screen appears.



Model Management Page

Use the left-hand menu to select the items you would like to configure.

Figure 27 Model Management Screen

Using the Model Management screen, you can load new models and view the available models.

2 Click **Load New Model** under Manage Models on the left side of the screen.

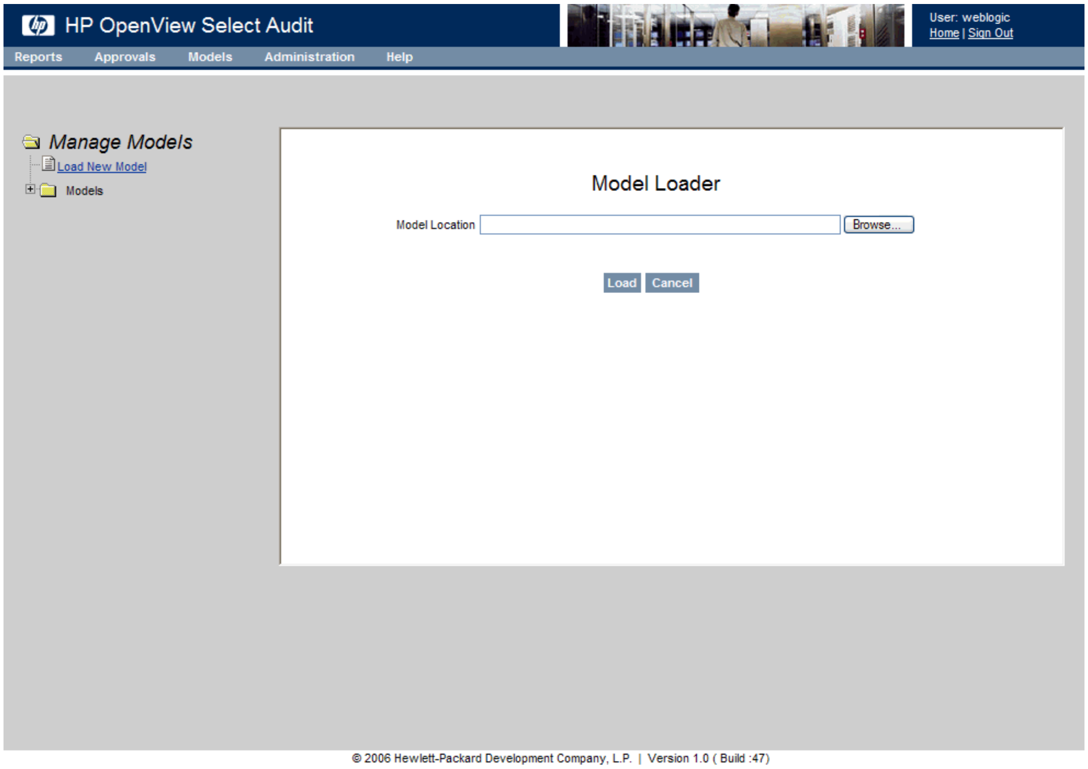


Figure 28 Model Loader Screen

3 Click **Browse** and navigate to select the XML model file you want to load.

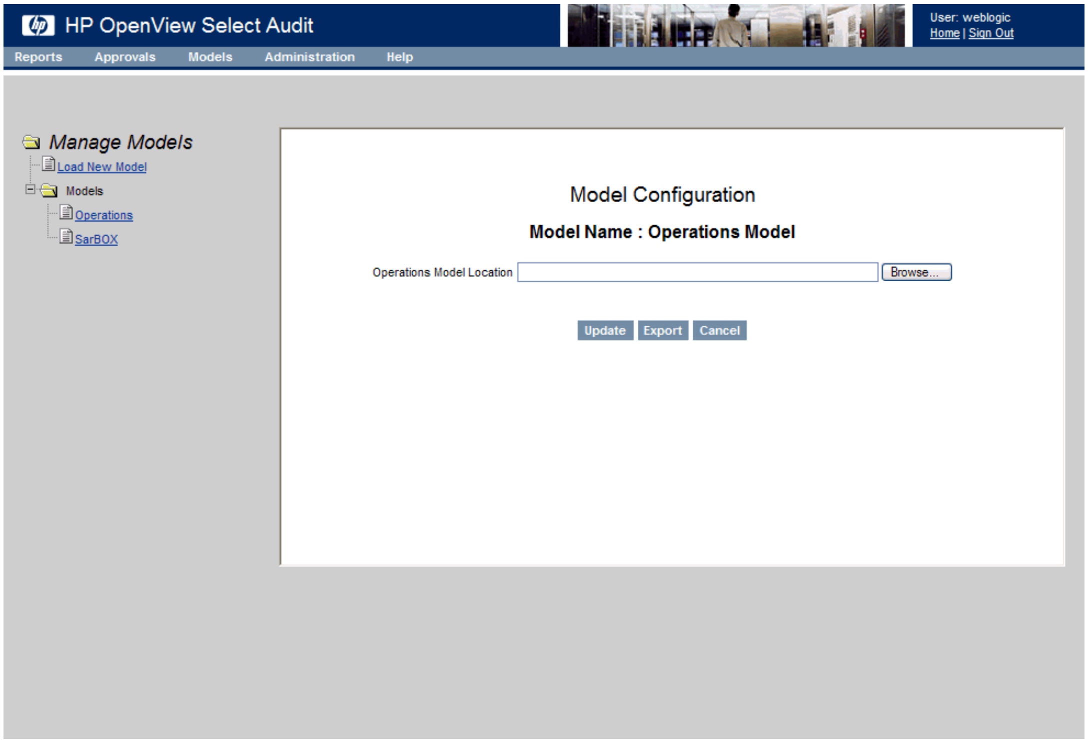
4 Click **Load**. The new model is loaded into Select Audit.

5 Restart the WebLogic server.

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 appears.

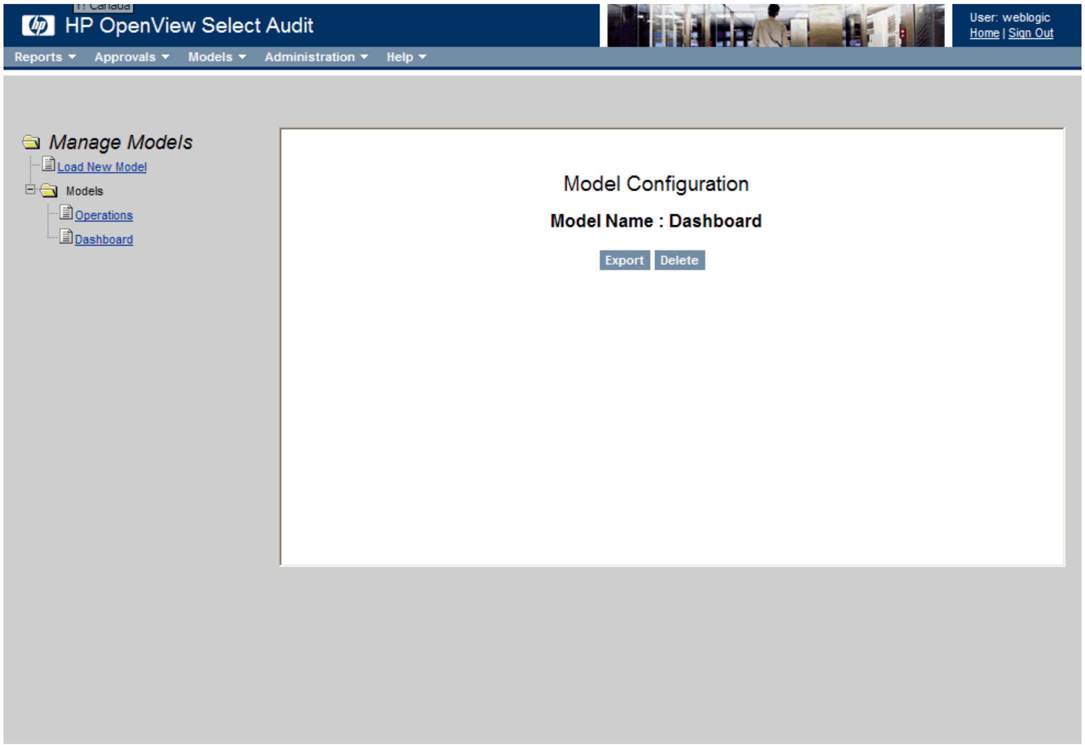


Model Name : Operations Model

Figure 29 Operations Model Configuration Screen

Using the **Operations Model Configuration** screen, you can update or export the model.

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



Model Name : Dashboard

Figure 30 Compliance Model Configuration Screen

Using the compliance model **Configuration** screen, you can export or delete the model.

To update a model

You can update a model by exporting the model, making any desired changes and re-importing the model. Use the update function once you have modified the model.

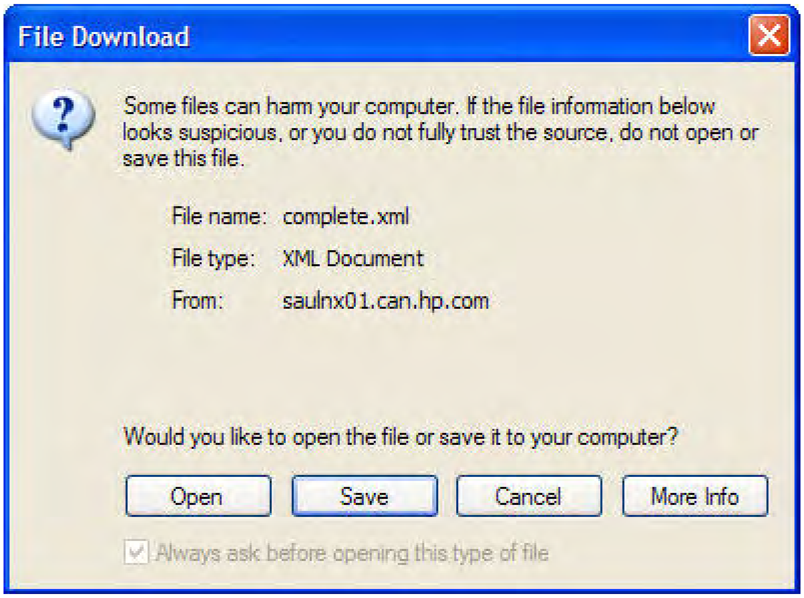
1 On the **Operations Model Configuration** screen, click **Browse** and navigate to select the XML model file you want to update.

2 Click **Update**. The updated model is loaded into Select Audit.

3 Restart the WebLogic server.

To export a model

1 On the Model Configuration screen, click **Export Model**. The File Download window appears.



File Download

Some files can harm your computer. If the file information below looks suspicious, or you do not fully trust the source, do not open or save this file.

File name: complete.xml

File type: XML Document

From: saulnx01.can.hp.com

Would you like to open the file or save it to your computer?

Figure 31 File Download Window

2 Click **Save**. The **Save As** window appears.

3 Browse to the location you which to save the file and click **Save**. The **Download Complete** window appears.

4 Click **Close**.

To delete a model

Click **Delete Model**. 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 reports generated by that model are not deleted.

7 Using Select Audit

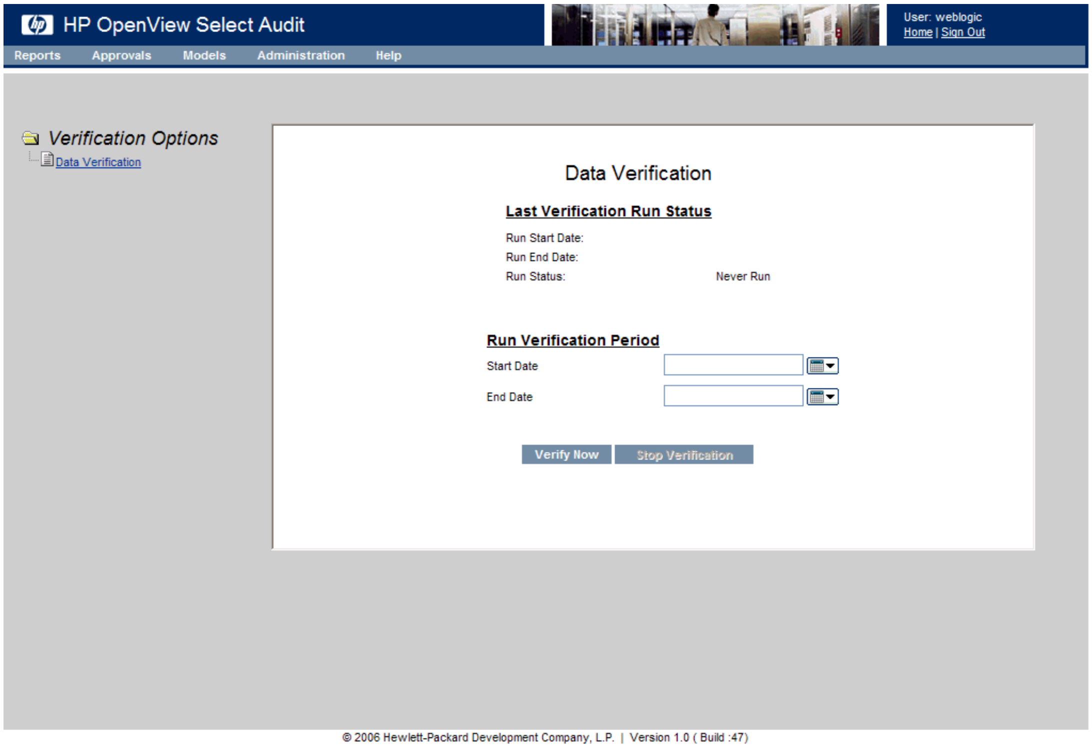
This chapter describes how to verify data integrity and how to approve reports using the Audit Portal. This chapter contains the following topics:

- Verifying Audit Data Integrity on page 81
- Approving Reports on page 82

Verifying Audit Data Integrity

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 appears.



Data Verification

Last Verification Run Status

Run Start Date:

Run End Date:

Run Status: Never Run

Run Verification Period

Start Date

End Date

© 2006 Hewlett-Packard Development Company, L.P. | Version 1.0 (Build :47)

Figure 32 Data Verification Screen

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

2 Enter a **Start Date** and an **End Date** manually or by using the calendars.

➤ 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” appears at the top of the screen to indicate that data verification is running.

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

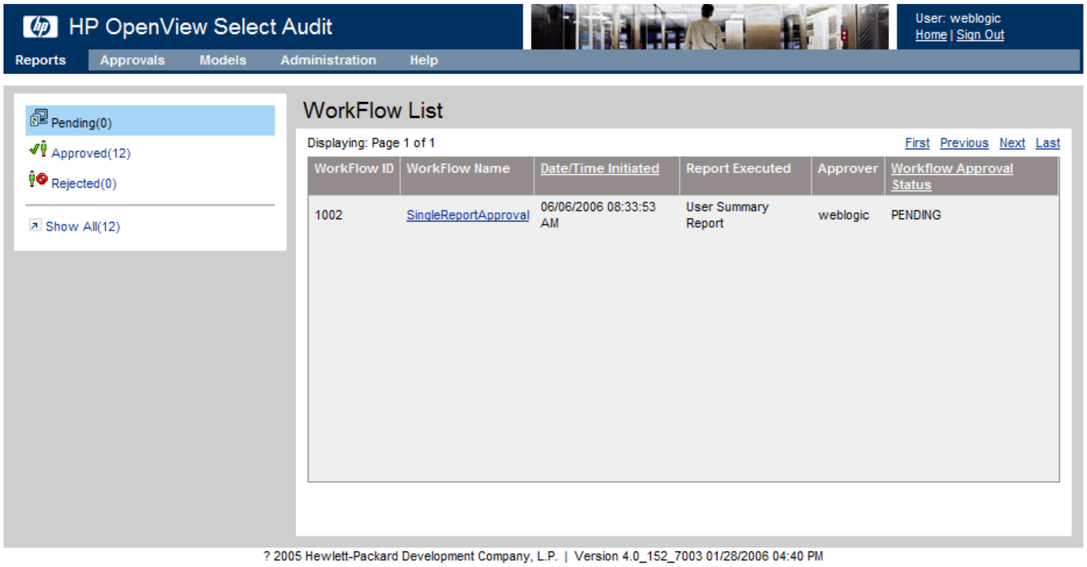
Approving Reports

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 appears as shown in Figure 33.

➤ 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 List

Displaying: Page 1 of 1

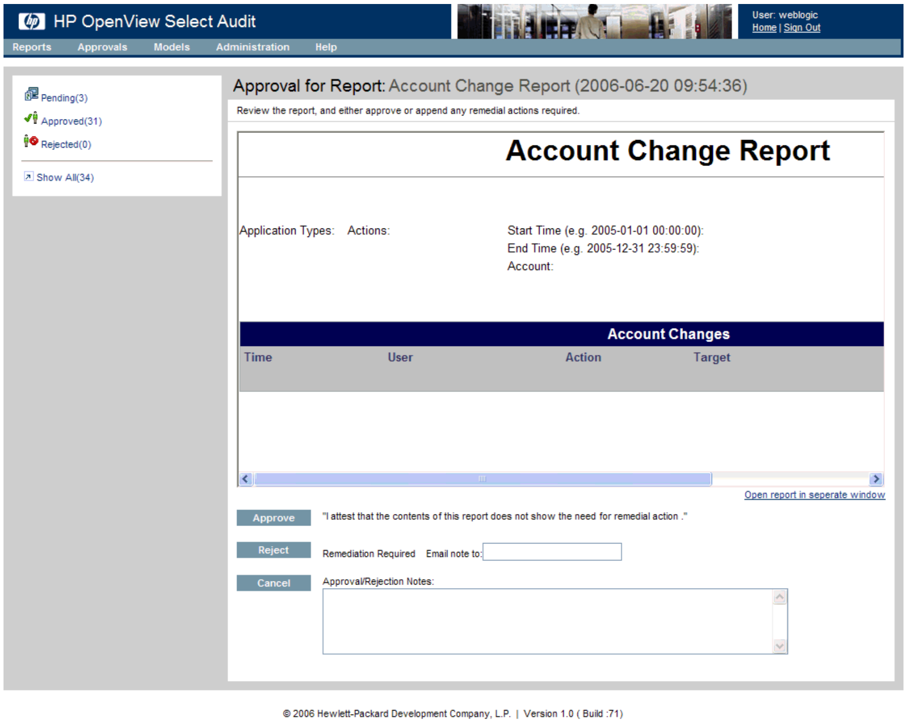
WorkFlow ID	WorkFlow Name	Date/Time Initiated	Report Executed	Approver	Workflow Approval Status
1002	SingleReportApproval	06/06/2006 08:33:53 AM	User Summary Report	weblogic	PENDING

? 2005 Hewlett-Packard Development Company, L.P. | Version 4.0_152_7003 01/28/2006 04:40 PM

Figure 33 Workflow List Screen

2 Click the report you wish to approve. The report appears in the browser.

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



Approval for Report: Account Change Report (2006-06-20 09:54:36)

Review the report, and either approve or append any remedial actions required.

Account Change Report

Application Types: Actions:

Start Time (e.g. 2005-01-01 00:00:00):
End Time (e.g. 2005-12-31 23:59:59):
Account:

Account Changes

Time	User	Action	Target

"I attest that the contents of this report does not show the need for remedial action ."

Remediation Required Email note to:

Approval/Rejection Notes:

© 2006 Hewlett-Packard Development Company, L.P. | Version 1.0 (Build :71)

Figure 34 Sample Report Approval

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 entering an email address in the **Email note to:** field.

8 Using Reports in Select Audit

This chapter describes the features of the reporting tools in Select Audit. Reports are accessed via the **Reports** menu on the Select Audit toolbar.

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

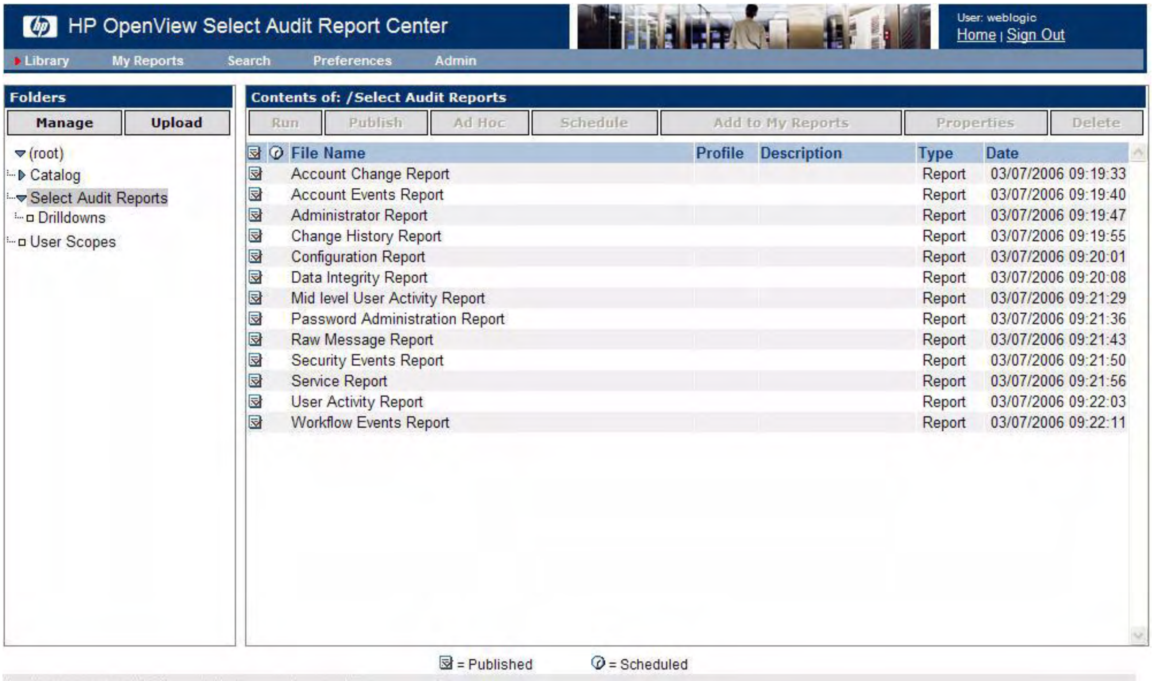
For more detailed information about report creation and design, refer to the *HP OpenView Select Audit 1.01 Report Center User's Guide*, *HP OpenView Select Audit 1.01 Report Designer's Guide*, and *HP OpenView Select Audit 1.01 Report Developer's Guide*.

Reports are viewed, scheduled and modified using the Report Center. This chapter contains the following topics:

- Using the Report Center on page 85
- Using My Reports on page 87
- Using the Library on page 87
- Running the Ad Hoc Wizard on page 98
- Searching for Reports on page 108
- Setting Preferences on page 110
- Editing Report Schedules on page 112

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.



File Name	Profile	Description	Type	Date
Account Change Report			Report	03/07/2006 09:19:33
Account Events Report			Report	03/07/2006 09:19:40
Administrator Report			Report	03/07/2006 09:19:47
Change History Report			Report	03/07/2006 09:19:55
Configuration Report			Report	03/07/2006 09:20:01
Data Integrity Report			Report	03/07/2006 09:20:08
Mid level User Activity Report			Report	03/07/2006 09:21:29
Password Administration Report			Report	03/07/2006 09:21:36
Raw Message Report			Report	03/07/2006 09:21:43
Security Events Report			Report	03/07/2006 09:21:50
Service Report			Report	03/07/2006 09:21:56
User Activity Report			Report	03/07/2006 09:22:03
Workflow Events Report			Report	03/07/2006 09:22:11

☑ = Published ⊘ = Scheduled

Figure 35 Report Center

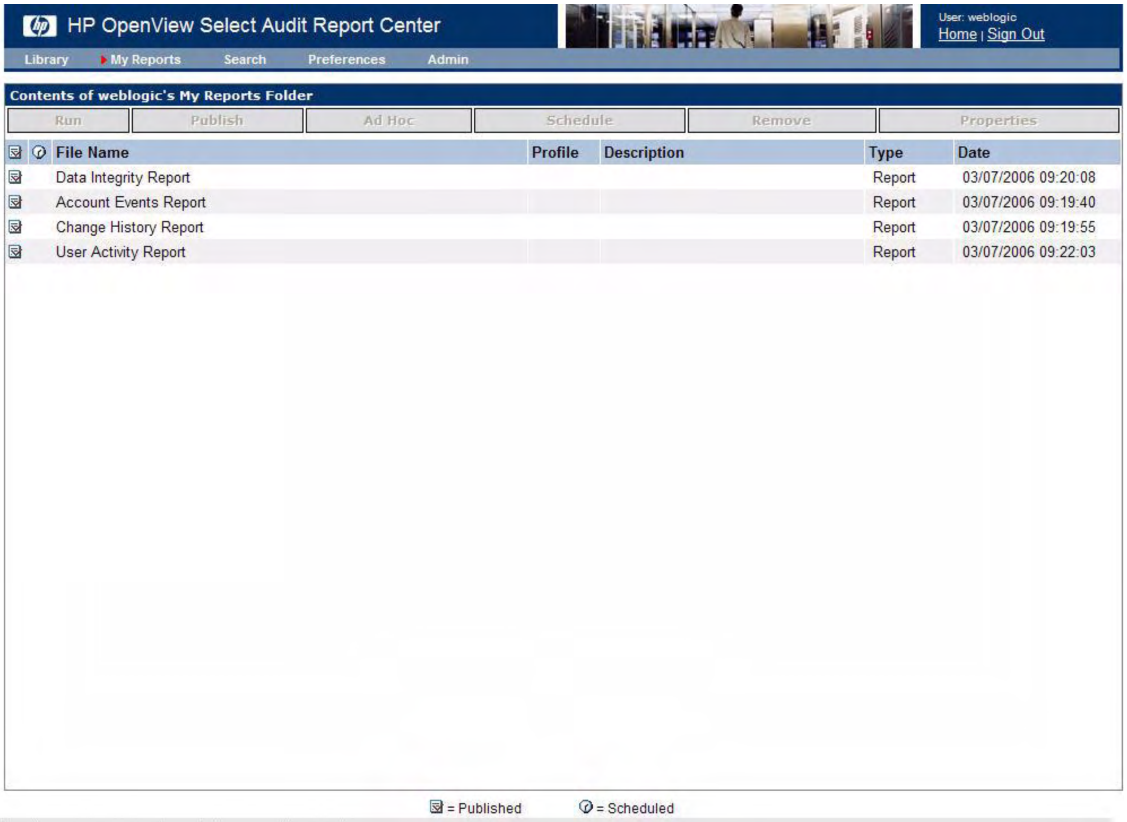
The Report Center has five main sections:

Table 7 Report Center Sections

Section	Description
Library	Use the Library to access and arrange the reports on the Report Server.
My Reports	My Reports provides a shortcut to frequently-viewed reports.
Search	Use Search to locate files in the Library by name, type or description.
Preferences	Preferences is used to set user preferences, such as your start page.
Admin	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.



	File Name	Profile	Description	Type	Date
☑	Data Integrity Report			Report	03/07/2006 09:20:08
☑	Account Events Report			Report	03/07/2006 09:19:40
☑	Change History Report			Report	03/07/2006 09:19:55
☑	User Activity Report			Report	03/07/2006 09:22:03

Figure 36 My Reports Folder

The **My Reports** screen displays a single window listing the Library files that you have previously selected using the **Add to My Reports** button. Refer to Managing Reports on page 94 and Running the Ad Hoc Wizard on page 98 to for information about using the **My Reports** buttons.

Using the Library

The Library is divided into two panels, used to manage folders and reports. The left-hand **Folders** panel displays the folders containing reports. The right-hand **Contents of** panel displays 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.

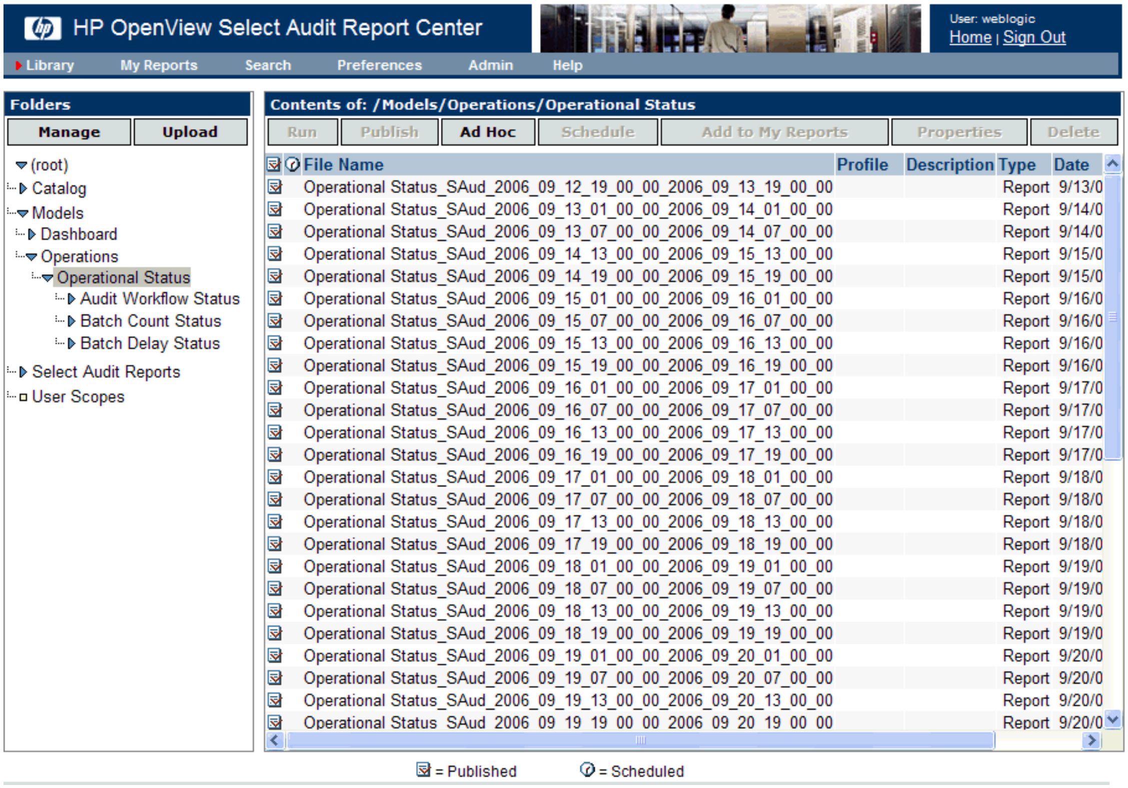
The Folders panel has four standard folders: **Catalog**, **Models**, **Select Audit Reports** and **User Scopes**.

Catalog

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

Models

The Models folder contains reports generated by the loaded models. The structure of the folder is shown in Figure 37.



- (root)
  - Catalog
  - Models
    - Dashboard
    - Operations
      - Operational Status
        - Audit Workflow Status
        - Batch Count Status
        - Batch Delay Status
  - Select Audit Reports
  - User Scopes

Contents of: /Models/Operations/Operational Status

☑	⊘	File Name	Profile	Description	Type	Date
☑		Operational Status_SAud_2006_09_12_19_00_00_2006_09_13_19_00_00			Report	9/13/0
☑		Operational Status_SAud_2006_09_13_01_00_00_2006_09_14_01_00_00			Report	9/14/0
☑		Operational Status_SAud_2006_09_13_07_00_00_2006_09_14_07_00_00			Report	9/14/0
☑		Operational Status_SAud_2006_09_14_13_00_00_2006_09_15_13_00_00			Report	9/15/0
☑		Operational Status_SAud_2006_09_14_19_00_00_2006_09_15_19_00_00			Report	9/15/0
☑		Operational Status_SAud_2006_09_15_01_00_00_2006_09_16_01_00_00			Report	9/16/0
☑		Operational Status_SAud_2006_09_15_07_00_00_2006_09_16_07_00_00			Report	9/16/0
☑		Operational Status_SAud_2006_09_15_13_00_00_2006_09_16_13_00_00			Report	9/16/0
☑		Operational Status_SAud_2006_09_15_19_00_00_2006_09_16_19_00_00			Report	9/16/0
☑		Operational Status_SAud_2006_09_16_01_00_00_2006_09_17_01_00_00			Report	9/17/0
☑		Operational Status_SAud_2006_09_16_07_00_00_2006_09_17_07_00_00			Report	9/17/0
☑		Operational Status_SAud_2006_09_16_13_00_00_2006_09_17_13_00_00			Report	9/17/0
☑		Operational Status_SAud_2006_09_16_19_00_00_2006_09_17_19_00_00			Report	9/17/0
☑		Operational Status_SAud_2006_09_17_01_00_00_2006_09_18_01_00_00			Report	9/18/0
☑		Operational Status_SAud_2006_09_17_07_00_00_2006_09_18_07_00_00			Report	9/18/0
☑		Operational Status_SAud_2006_09_17_13_00_00_2006_09_18_13_00_00			Report	9/18/0
☑		Operational Status_SAud_2006_09_17_19_00_00_2006_09_18_19_00_00			Report	9/18/0
☑		Operational Status_SAud_2006_09_18_01_00_00_2006_09_19_01_00_00			Report	9/19/0
☑		Operational Status_SAud_2006_09_18_07_00_00_2006_09_19_07_00_00			Report	9/19/0
☑		Operational Status_SAud_2006_09_18_13_00_00_2006_09_19_13_00_00			Report	9/19/0
☑		Operational Status_SAud_2006_09_18_19_00_00_2006_09_19_19_00_00			Report	9/19/0
☑		Operational Status_SAud_2006_09_19_01_00_00_2006_09_20_01_00_00			Report	9/20/0
☑		Operational Status_SAud_2006_09_19_07_00_00_2006_09_20_07_00_00			Report	9/20/0
☑		Operational Status_SAud_2006_09_19_13_00_00_2006_09_20_13_00_00			Report	9/20/0
☑		Operational Status_SAud_2006_09_19_19_00_00_2006_09_20_19_00_00			Report	9/20/0

☑ = Published ⊘ = Scheduled

Figure 37 Models Folder

The model reports are categorized into subfolders including one folder for the Operations model and folders for any loaded compliance models. The Operations reports are categorized in the **Operational Status** subfolder. You can drill down through the subfolders to view smaller levels of data.

The Operations reports are run at 1:00 am, 7:00 am, 1:00 pm and 7:00 pm. The compliance model reports are initially created when the model is loaded. They are run every 24 hours at 2:00 am. See Chapter 6, Models for more information about the Select Audit models and their reports.

Select Audit Reports

The Select Audit Reports folder contains 15 predefined Select Audit Reports, as listed in Table 8:

Table 8 Select Audit Reports

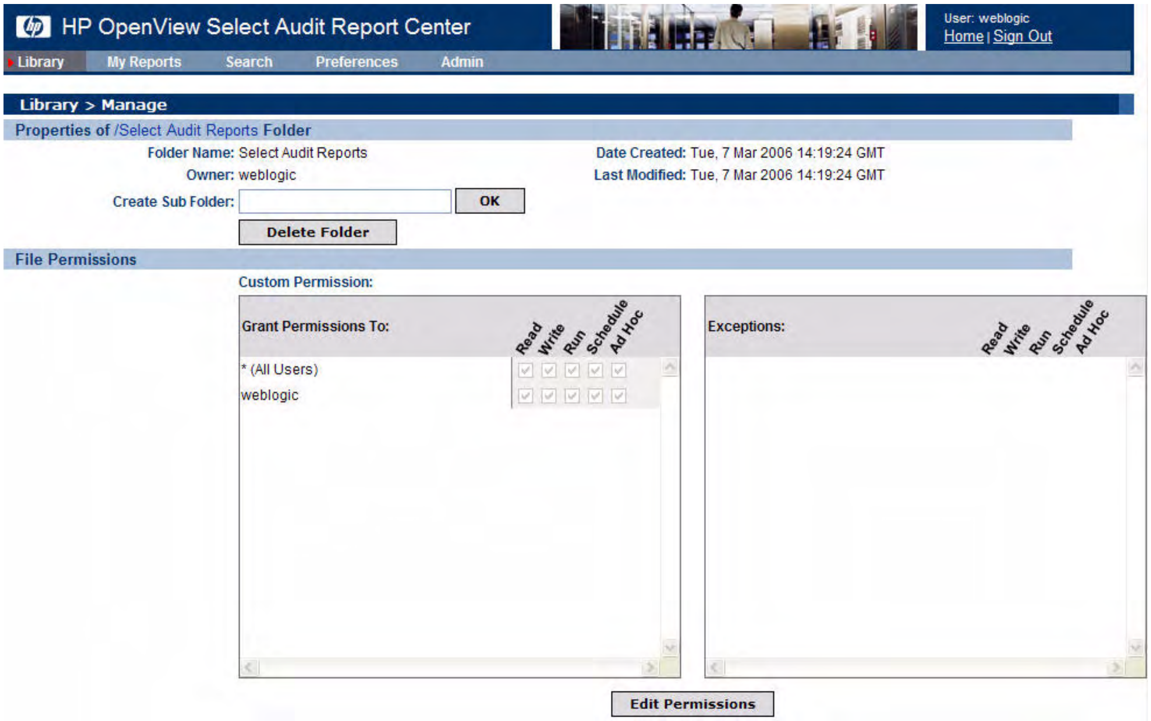
Report Name	Details
Account Change Report	Contains all user account change actions (add, delegate, change, etc.).
Account Events Report	Contains all account event actions (security violations, admin login errors, expired passwords, etc.).
Administrator Report	Contains all administrator actions (configuration changes, authentication changes, password resets, etc.).
Attestation Report	Contains all attestation actions (approved, pending, denied).
Change History Report	Contains 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	Contains all configuration change actions (add, change, etc.).
Data Integrity Report	Contains a list of tampered records IDs and tampered signature record IDs, with change actions (added, modified, removed).
Password Management Report	Contains all password administration actions (expire, logon, etc.).
Raw Message Report	Contains raw audit messages that aren't normalized through the standard process.
Security Events Report	Contains all security events (security violation, configuration changes, etc.).
Service Report	Contains configuration changes to Select Identity services.
System Activity Report	Contains all system activities (login, logout, changes made, etc.).
User Activity Report	Contains all user activities (login, logout, changes made, etc.).
User Summary Report	Contains a summary of user activities.
Workflow Events Report	Contains all workflow event messages.

User Scopes

User Scopes is the default 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.



Folder Name: Select Audit Reports

Owner: weblogic

Date Created: Tue, 7 Mar 2006 14:19:24 GMT

Last Modified: Tue, 7 Mar 2006 14:19:24 GMT

Grant Permissions To:	Read	Write	Run	Schedule	Ad Hoc
* (All Users)	☑	☑	☑	☑	☑
weblogic	☑	☑	☑	☑	☑

Exceptions:	Read	Write	Run	Schedule	Ad Hoc

Figure 38 Library > Manage Screen

To create a sub-folder

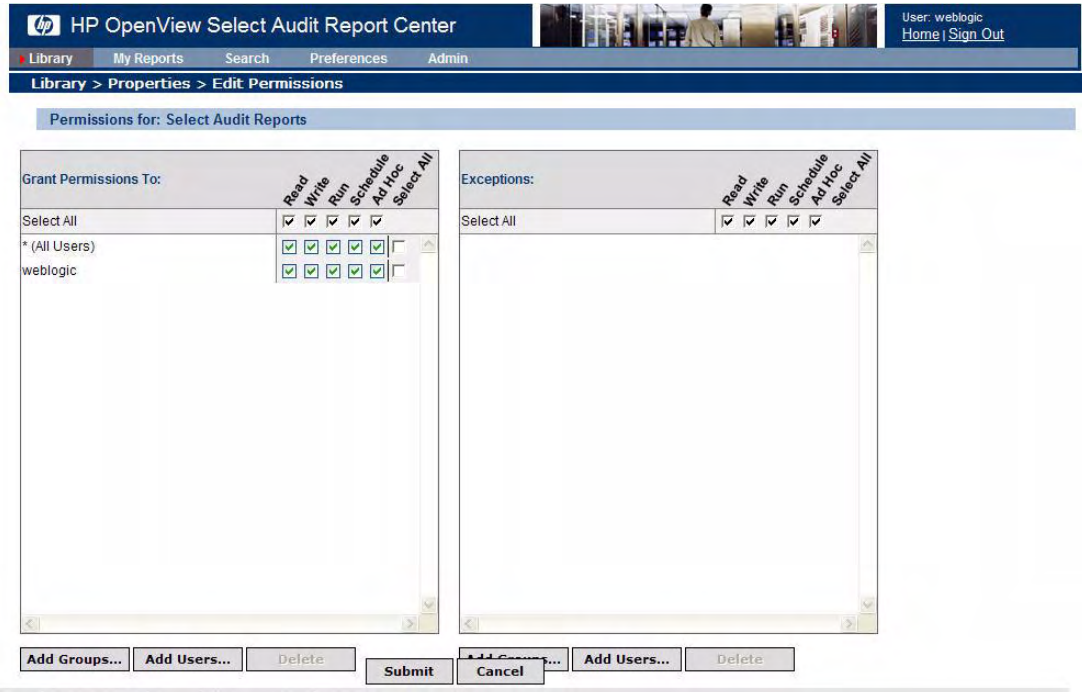
1. Type a folder name in the **Create Sub Folder** field on the **Library > Manage** screen.
2. Click **OK**. The new folder appears in the Library Folder list.

To delete a folder

1. In the Library, select the folder you want to delete and click **Manage**. The **Library > Manage** screen appears.
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 appears 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 appears.



Permissions for: Select Audit Reports

Grant Permissions To:	Read	Write	Run	Schedule	Ad Hoc	Select All
Select All	☑	☑	☑	☑	☑	
* (All Users)	☑	☑	☑	☑	☑	☐
weblogic	☑	☑	☑	☑	☑	☐

Exceptions:	Read	Write	Run	Schedule	Ad Hoc	Select All
Select All	☑	☑	☑	☑	☑	

Figure 39 Edit Permissions Screen

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 Gives users/group members the ability to read the RDL file.

Write Gives users/group members the ability to edit the RDL file.

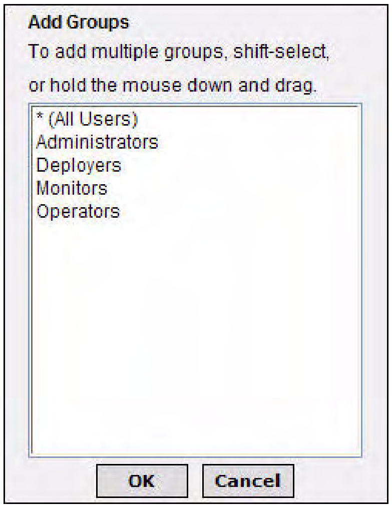
Run Gives users/group members the ability to run a report.

Schedule Gives users/group members the ability to schedule a report.

Ad Hoc Gives users/group members the ability to create a new report using the current report as the starting point.

3 Click **Submit**. The **Library > Manage** screen appears, showing the updated folder permissions.

4 To add groups, click **Add Groups...**. The **Add Groups** dialog box appears.



Add Groups

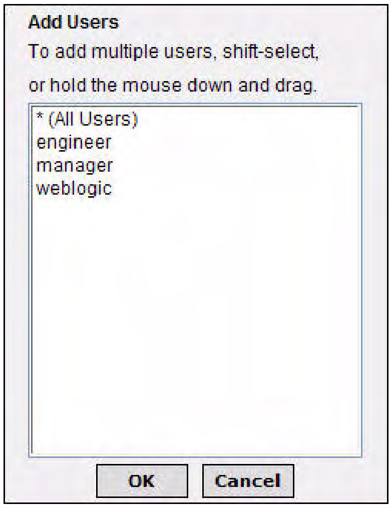
To add multiple groups, shift-select,
or hold the mouse down and drag.

* (All Users)
Administrators
Deployers
Monitors
Operators

Figure 40 Add Groups Dialog Box

5 Select the groups you want to add and click **OK**. The new groups appear in the **Grant Permissions To** or the **Exceptions** list.

6 To add users, click **Add Users...**. The **Add Users** dialog box appears.



Add Users

To add multiple users, shift-select,
or hold the mouse down and drag.

* (All Users)
engineer
manager
weblogic

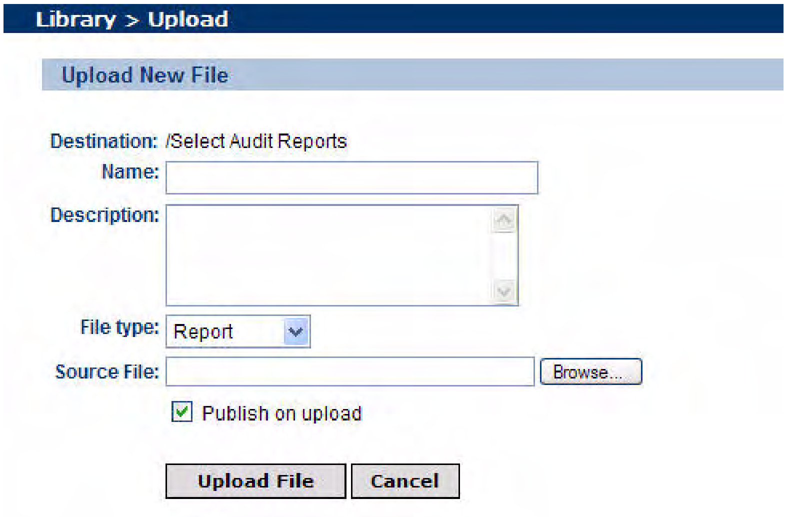
Figure 41 Add Users Dialog Box

7 Select the users you want to add and click **OK**. The new users appear 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 appears.



Library > Upload

Upload New File

Destination: /Select Audit Reports

Name:

Description:

File type: Report

Source File:

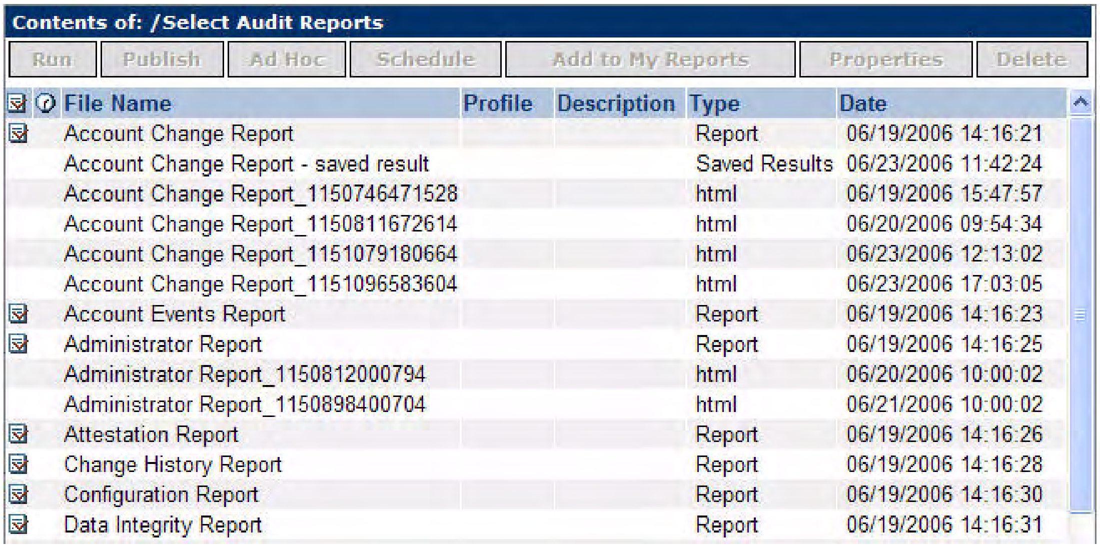
☑ Publish on upload

Figure 42 Upload Screen

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



Contents of: /Select Audit Reports

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

Figure 43 **Contents Of Panel**

The buttons at the top of the **Contents of** panel are described in Table 9:

Table 9 Report Buttons

Button	Description
Run	Generates the report from the file.
Publish	Publishes the report. If the report has already been published, this button is grayed out.
Ad Hoc	Creates a new report using the Ad Hoc wizard. Refer to Running the Ad Hoc Wizard on page 98 for more information about using the Ad Hoc wizard.
Schedule	Used to create and manage a schedule for automatically generating reports.
Add To My Reports	Adds the file to a list of frequently-used files.
Properties	Used to view file properties and performance statistics, and modify scheduling and permissions.
Delete	Deletes the report file from the Library.

To run a report

Select a report and click **Run**. A new window opens displaying the report.

➤ 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.

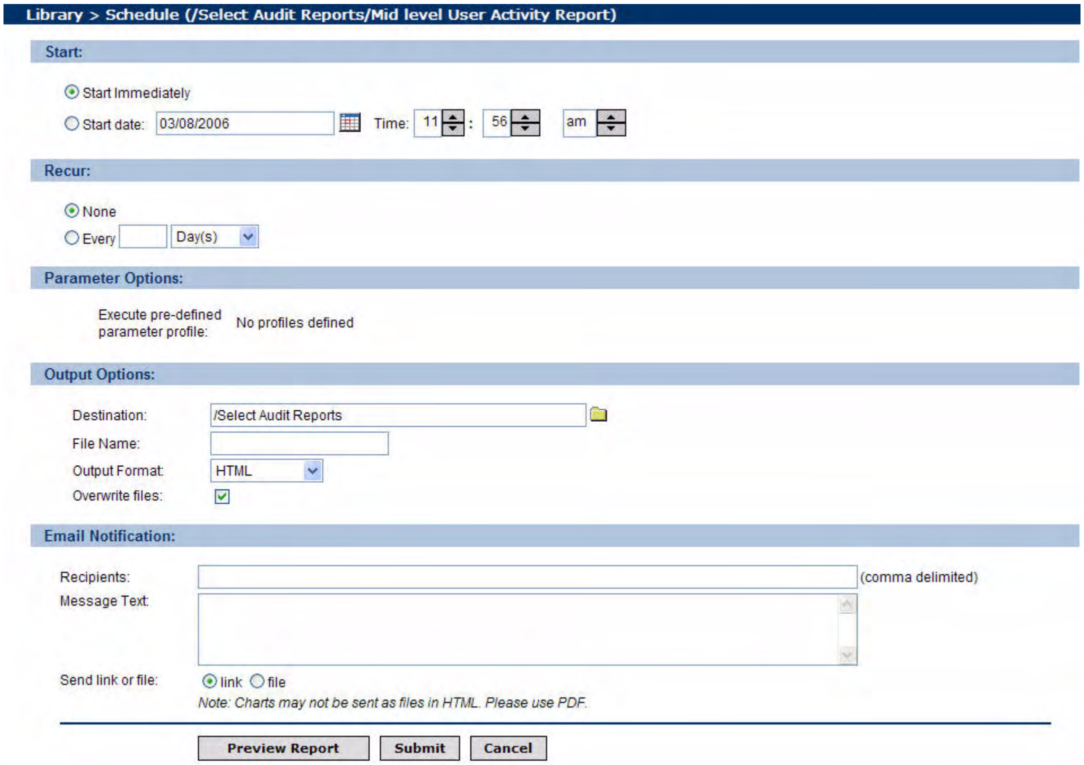
The published icon ☑ appears beside the report.

2 To unpublish a report, select the report, then click **Properties**. The **Properties** screen appears.

3 Click **Unpublish** in the Publish section. The status changes to unpublished and the ☑ icon is no longer displayed beside the report name in the **Contents of** panel.

To schedule report execution

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



Library > Schedule (/Select Audit Reports/Mid level User Activity Report)

Start:

● Start Immediately

○ Start date: 03/08/2006 Time: 11 : 56 am

Recur:

● None

○ Every Day(s)

Parameter Options:

Execute pre-defined parameter profile: No profiles defined

Output Options:

Destination: /Select Audit Reports

File Name:

Output Format: HTML

Overwrite files: ☑

Email Notification:

Recipients: (comma delimited)

Message Text:

Send link or file: ● link ○ file

Note: Charts may not be sent as files in HTML. Please use PDF.

Figure 44 Library > Schedule

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 Specify the frequency. Possible choices are Minutes, Hours, Weeks, Days, and Months.

End Specify a date and time or number of occurrences.

Output Options

- Specify a destination folder.
- Choose a file name.
- Specify output format – HTML, XML, PDF, CSV, or Excel.
- Check **Overwrite files** if you want new scheduled output to override the old.

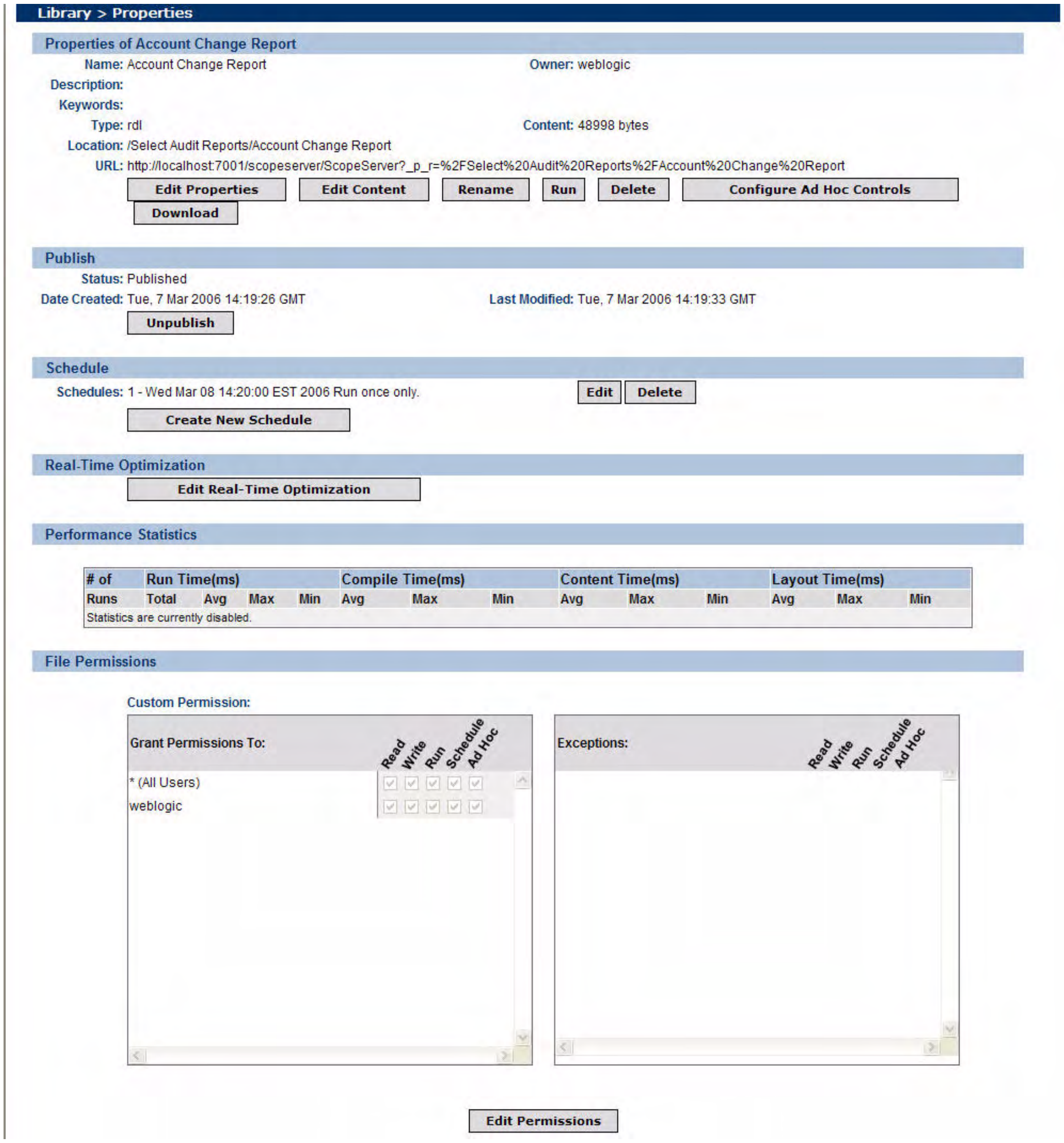
Email Notifications Enter one or more email addresses to receive email alerts, and specify whether to send the output as a link or as an attached file.

3 Click **Submit**. The 🕒 icon appears 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 appears.



Library > Properties

Properties of Account Change Report

Name: Account Change Report Owner: weblogic
Description:
Keywords:
Type: rdl Content: 48998 bytes
Location: /Select Audit Reports/Account Change Report
URL: http://localhost:7001/scopeserver/ScopeServer?_p_r=%2FSelect%20Audit%20Reports%2FAccount%20Change%20Report

Publish

Status: Published
Date Created: Tue, 7 Mar 2006 14:19:26 GMT Last Modified: Tue, 7 Mar 2006 14:19:33 GMT

Schedule

Schedules: 1 - Wed Mar 08 14:20:00 EST 2006 Run once only.

Real-Time Optimization

Performance Statistics

# of	Run Time(ms)				Compile Time(ms)			Content Time(ms)			Layout Time(ms)		
Runs	Total	Avg	Max	Min	Avg	Max	Min	Avg	Max	Min	Avg	Max	Min
Statistics are currently disabled.													

File Permissions

Custom Permission:

Grant Permissions To:	Read	Write	Run	Schedule	Ad Hoc
* (All Users)	☑	☑	☑	☑	☑
weblogic	☑	☑	☑	☑	☑

Exceptions:	Read	Write	Run	Schedule	Ad Hoc

Figure 45 Library > Properties Screen

The **Properties** screen enables you to view report properties and performance statistics, or to reset schedule or permissions. The sections of the screen are described in Table 10.

Table 10 Properties Screen Sections

Section	Description
Properties <*report name*>	Displays the selected report's properties. It contains the following buttons: • Edit Properties provides a report description, or lets you specify search keywords. • Edit Content is used to modify the RDL file. • Run runs the report. • Delete removes the current report from the Library. • Configure Ad Hoc Controls configures the Ad Hoc controls for the current report.
Publish	Indicates the Status and Date Published. To unpublish report, click **Unpublish**.
Schedule	Allows you to create a new schedule for the report.
Real-Time Optimization	Click **Edit Real-Time Optimization** to upload or add a new optimization descriptor.
Performance Statistics	Lists the following statistics: • The number of report runs • The time taken to run • The time taken to compile • The time taken to build content • The time taken to create layout You turn on Performance Statistics using the Admin Dashboard. See Configuring the Report Server on page 36 for more information.
File Permissions	Displays existing file permissions. Click **Edit Permissions** 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. At any point in the wizard, you can save the report or preview it in its current state.

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 OpenView Select Audit 1.01 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 displayed 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 display in a standard format, use the following line:

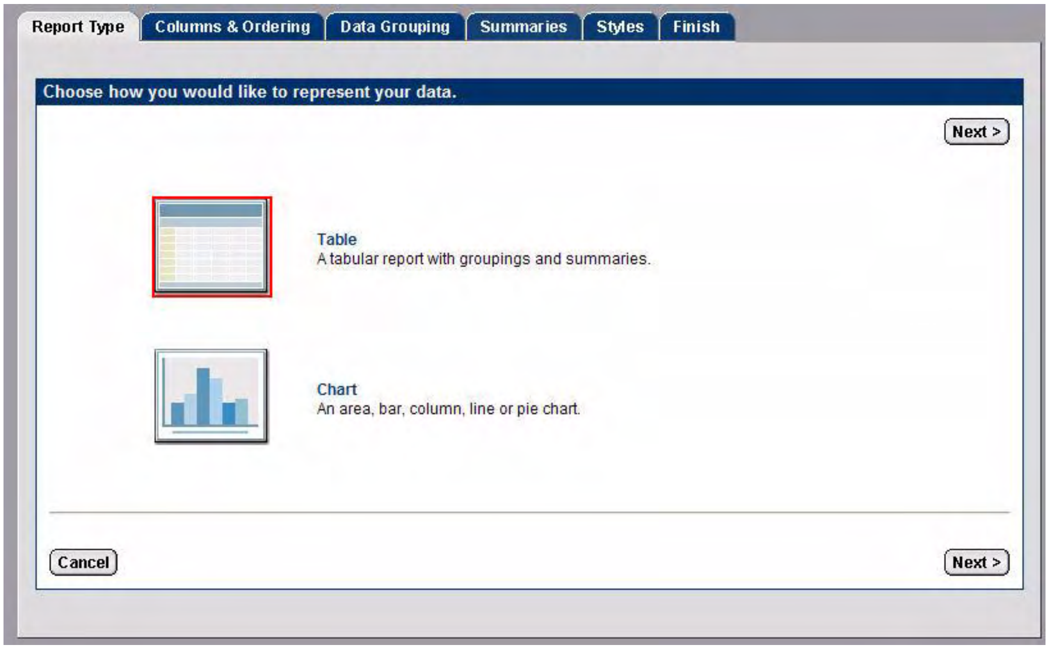
```
<Property name="dateFormat">yyyy-MM-dd HH:mm:ss Z</Property>
```

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, then click **Ad Hoc**. The **Report Type** screen appears.



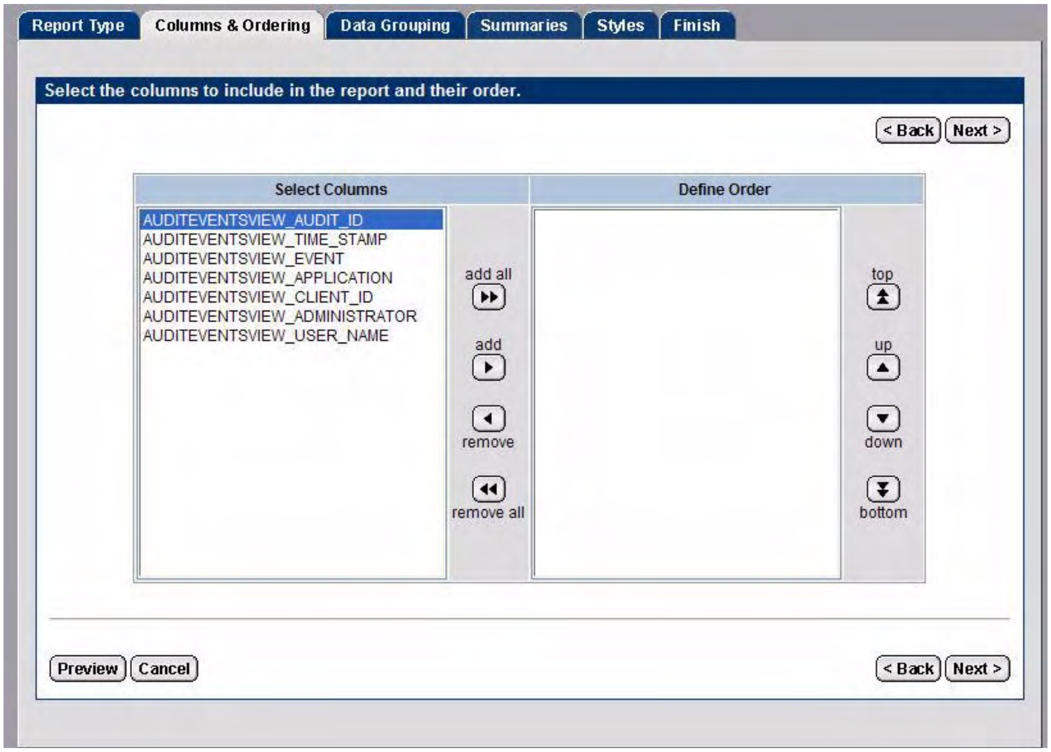
Choose how you would like to represent your data.

Table
A tabular report with groupings and summaries.

Chart
An area, bar, column, line or pie chart.

Figure 46 Report Type Screen

2 Select **Table** and click **Next**. The **Columns and Ordering** screen appears.



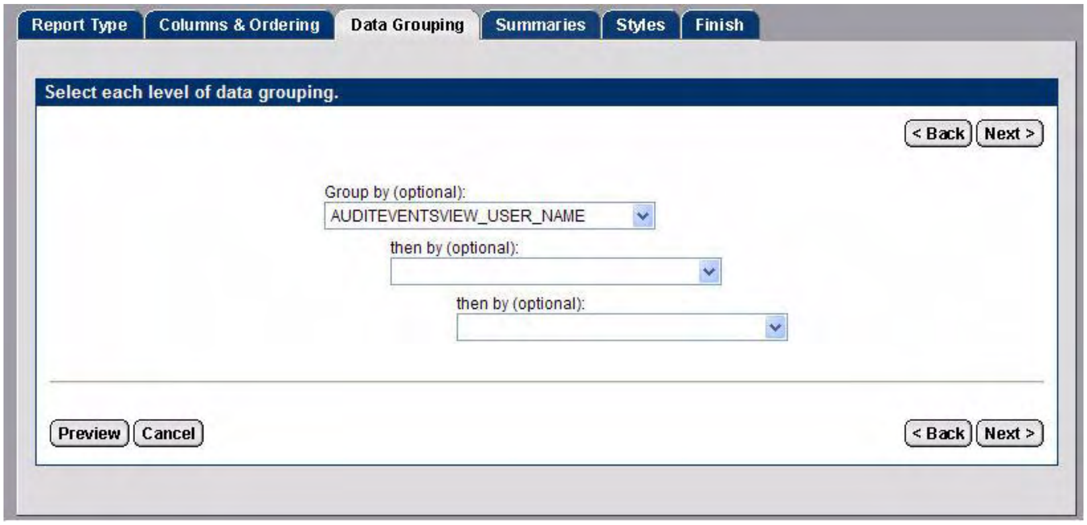
Select the columns to include in the report and their order.

AUDITEVENTSVIEW_AUDIT_ID
AUDITEVENTSVIEW_TIME_STAMP
AUDITEVENTSVIEW_EVENT
AUDITEVENTSVIEW_APPLICATION
AUDITEVENTSVIEW_CLIENT_ID
AUDITEVENTSVIEW_ADMINISTRATOR
AUDITEVENTSVIEW_USER_NAME

Figure 47 Columns and Ordering Screen

3 Select the columns you want to include in the report and use the **Up** and **Down** arrows to define the order of the columns.

4 Click **Next**. The **Data Grouping** screen appears.



Select each level of data grouping.

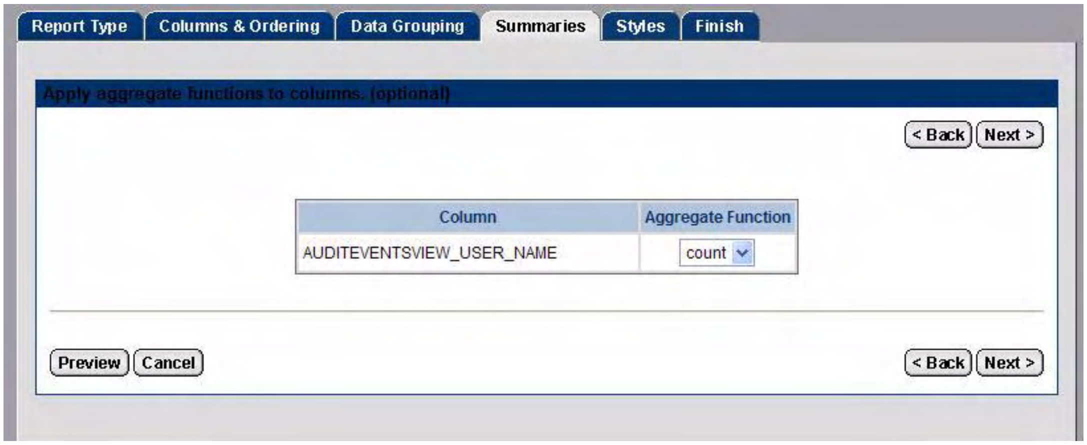
Group by (optional): AUDITEVENTSVIEW_USER_NAME

then by (optional):

then by (optional):

Figure 48 Data Grouping Screen

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

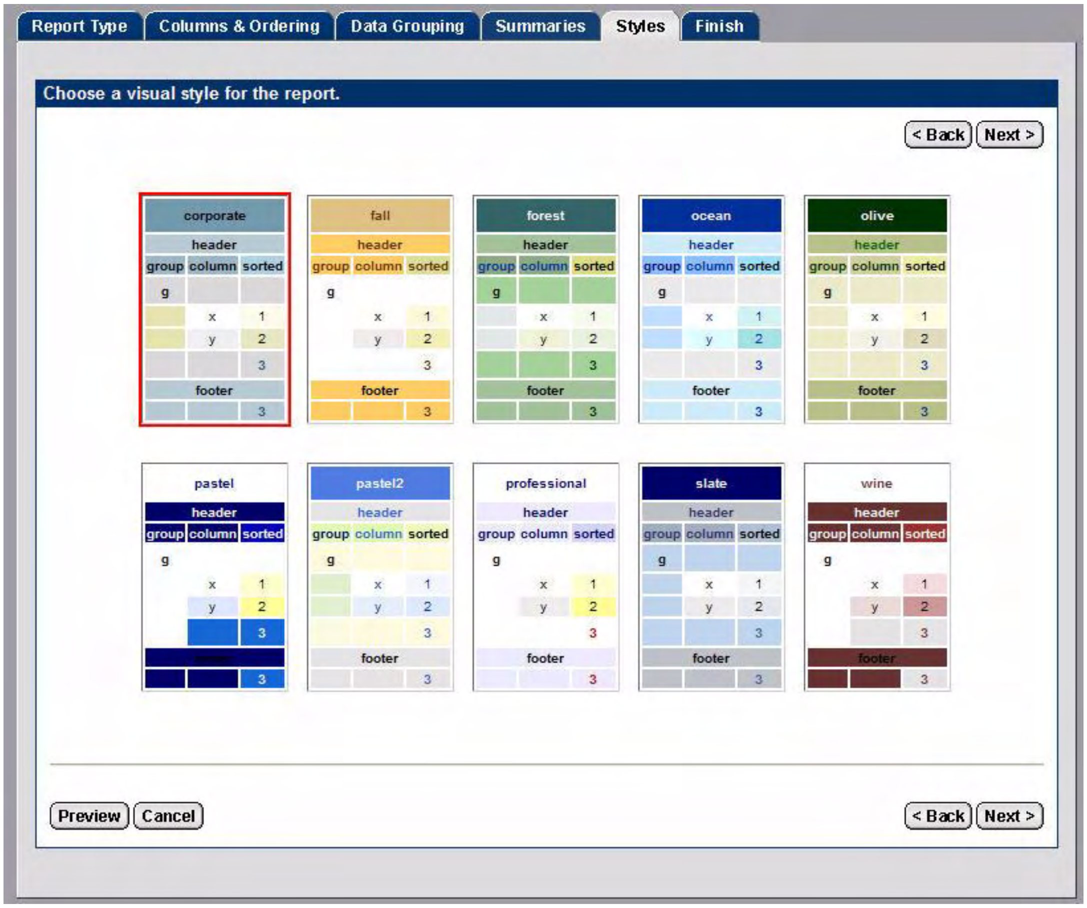


Apply aggregate functions to columns. (optional)

Column	Aggregate Function
AUDITEVENTSVIEW_USER_NAME	count

Figure 49 Summaries Screen

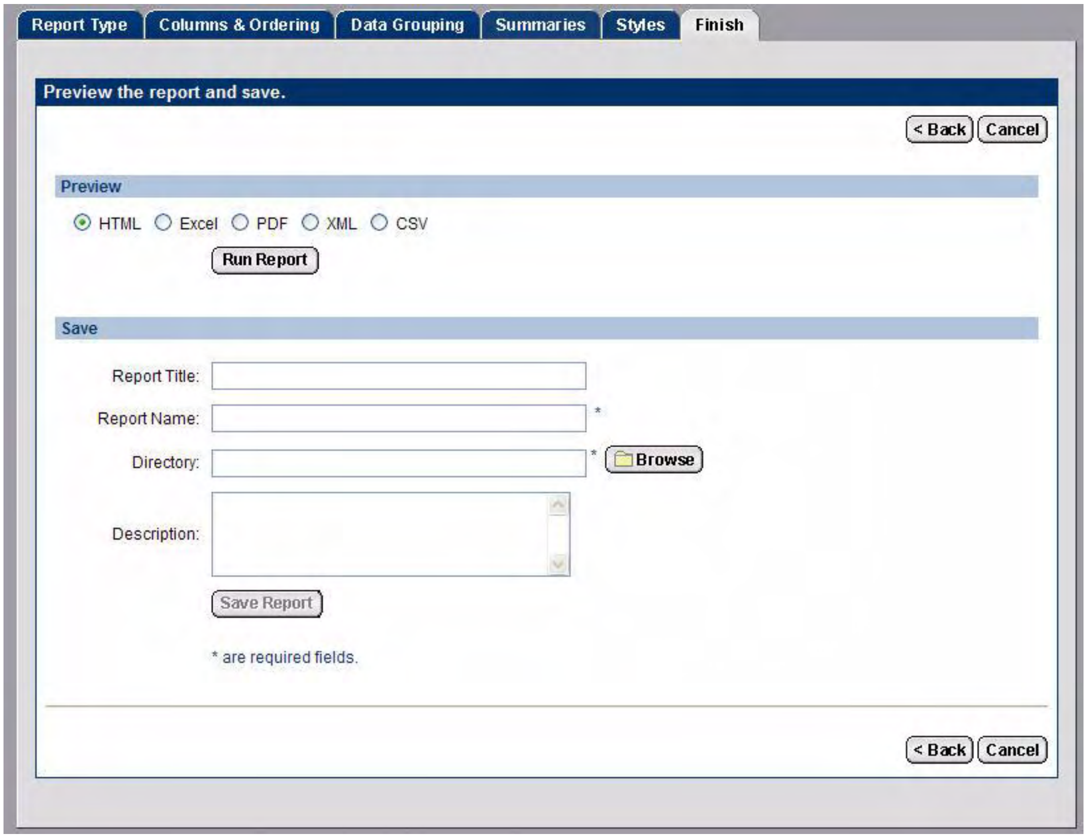
6 Optionally, select an aggregate function for the column and click **Next**. The **Styles** screen appears.



Choose a visual style for the report.

Figure 50 Styles Screen

7 Select a style for the report and click **Next**. The **Finish** screen appears.



Preview the report and save.

Preview

● HTML ○ Excel ○ PDF ○ XML ○ CSV

Save

Report Title:

Report Name: *

Directory: *

Description:

* are required fields.

Figure 51 Finish Screen

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

9 Enter a **Report Title**, **Report Name**, **Directory**, and **Description** for the report in the corresponding fields.

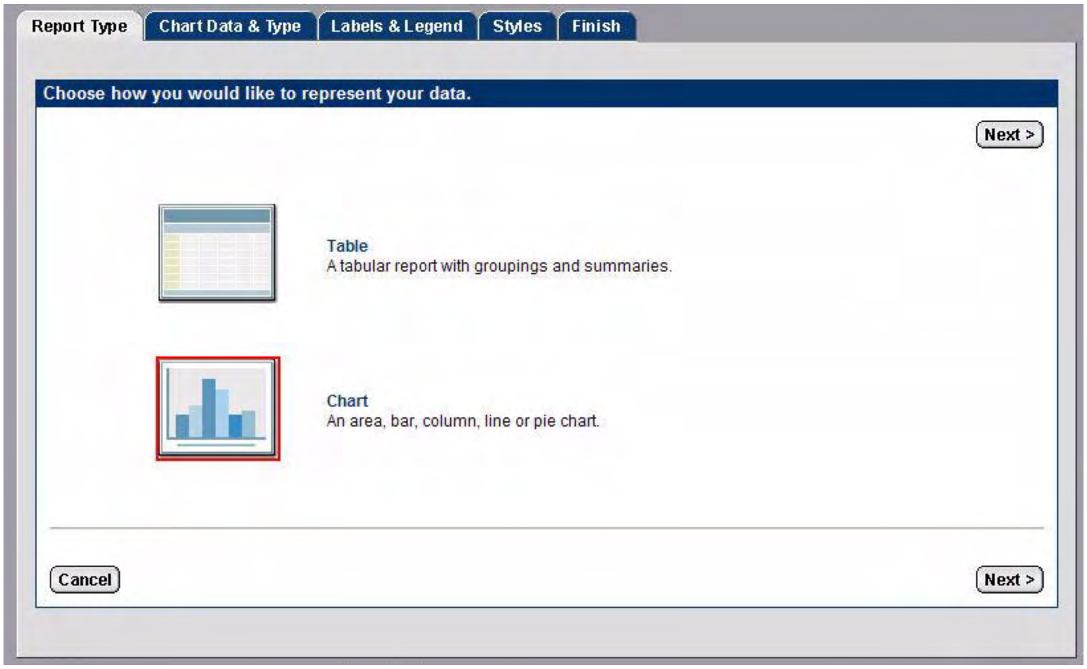
➤ Click **Browse** to select the directory where you want to save the report.

10 Click **Save Report**. The Ad Hoc wizard displays a confirmation message when the report has been saved.

11 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, then click **Ad Hoc**. The **Report Type** screen appears.



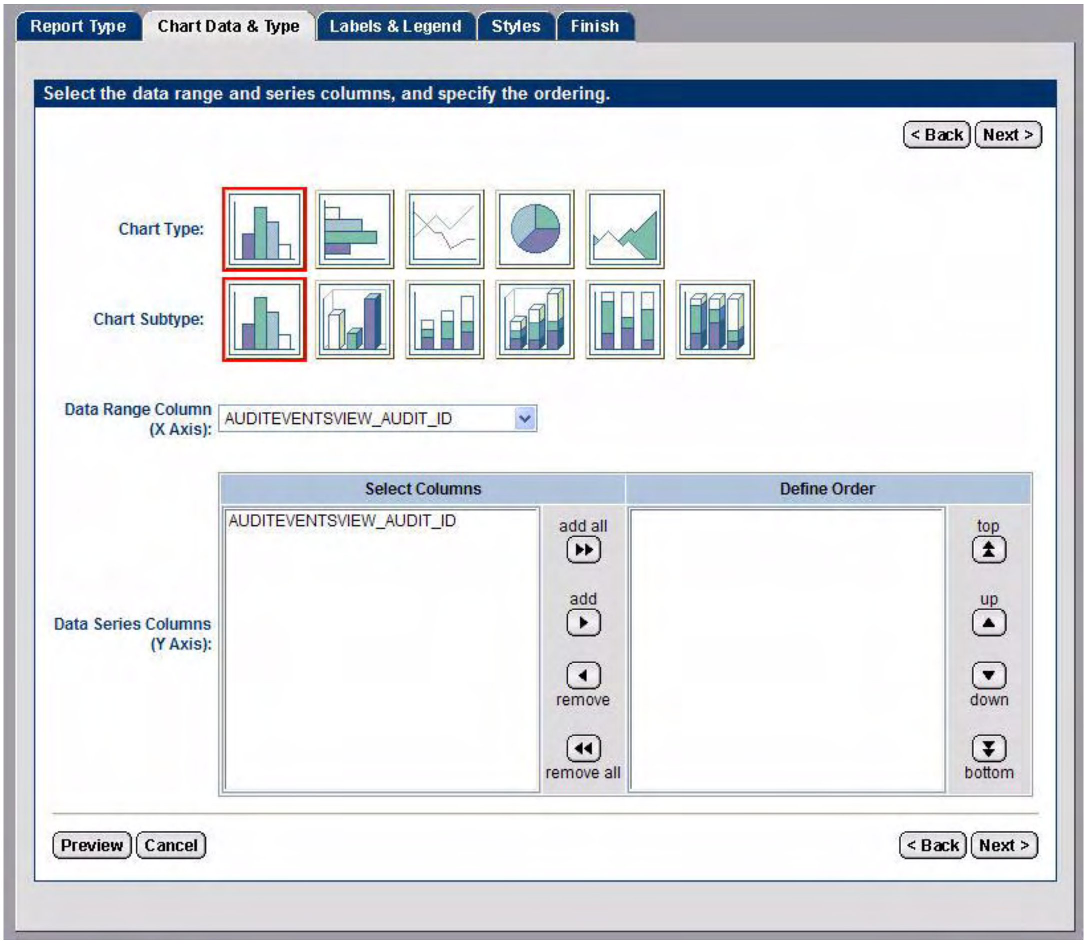
Choose how you would like to represent your data.

Table
A tabular report with groupings and summaries.

Chart
An area, bar, column, line or pie chart.

Figure 52 Report Type Screen

2 Select **Chart** and click **Next**. The **Chart Data & Type** screen appears.



Select the data range and series columns, and specify the ordering.

Data Range Column (X Axis): AUDITEVENTSVIEW_AUDIT_ID

Data Series Columns (Y Axis): AUDITEVENTSVIEW_AUDIT_ID

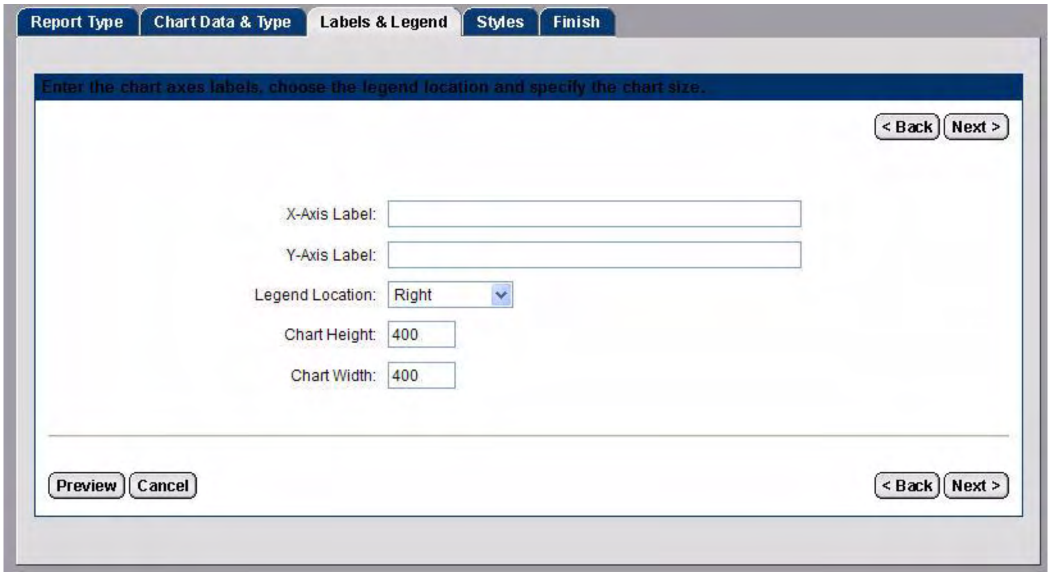
Figure 53 Chart Data & Type Screen

3 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.

4 Click **Next**. The **Labels & Legend** screen appears.



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

X-Axis Label:

Y-Axis Label:

Legend Location: Right

Chart Height: 400

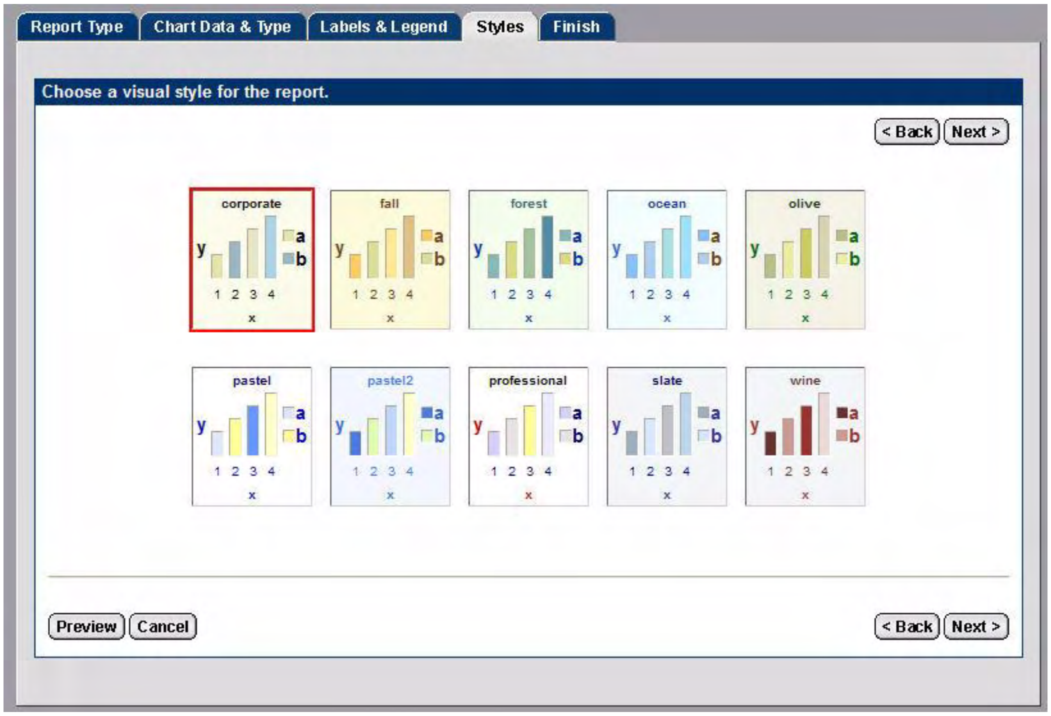
Chart Width: 400

Figure 54 Labels & Legend Screen

5 Do the following:

- Enter an **X Axis Label**.
- Enter a **Y Axis Label**.
- Select a location for the legend from the **Legend Location** drop-down list.
- Enter the **Chart Height**.
- Enter the **Chart Width**.

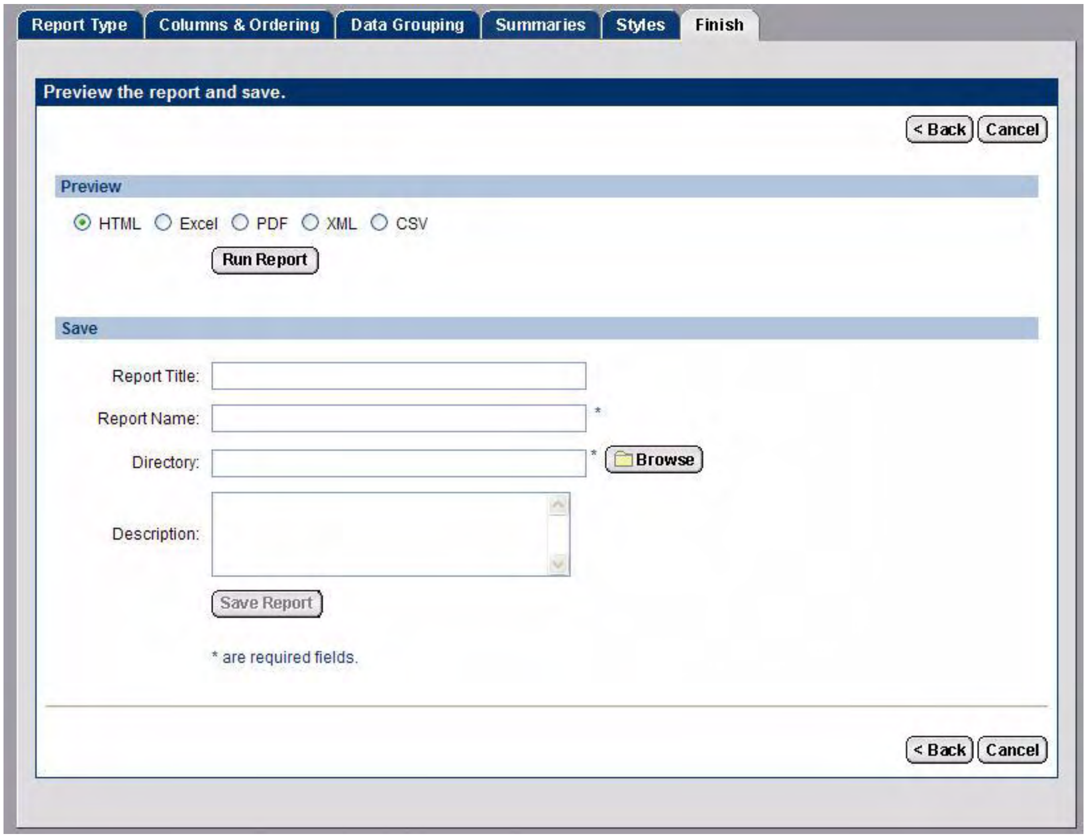
6 Click **Next**. The **Styles** screen appears.



Choose a visual style for the report.

Figure 55 Styles Screen

7 Select a style for the chart and click **Next**. The **Finish** screen appears.



Preview the report and save.

Preview

● HTML ○ Excel ○ PDF ○ XML ○ CSV

Save

Report Title:

Report Name: *

Directory: *

Description:

* are required fields.

Figure 56 Finish Screen

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

9 Enter a **Report Title**, **Report Name**, **Directory**, and **Description** for the chart in the corresponding fields.

> Click **Browse** to select the directory where you want to save the chart.

10 Click **Save Report**. The Ad Hoc wizard displays a confirmation message when the chart has been saved.

11 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.

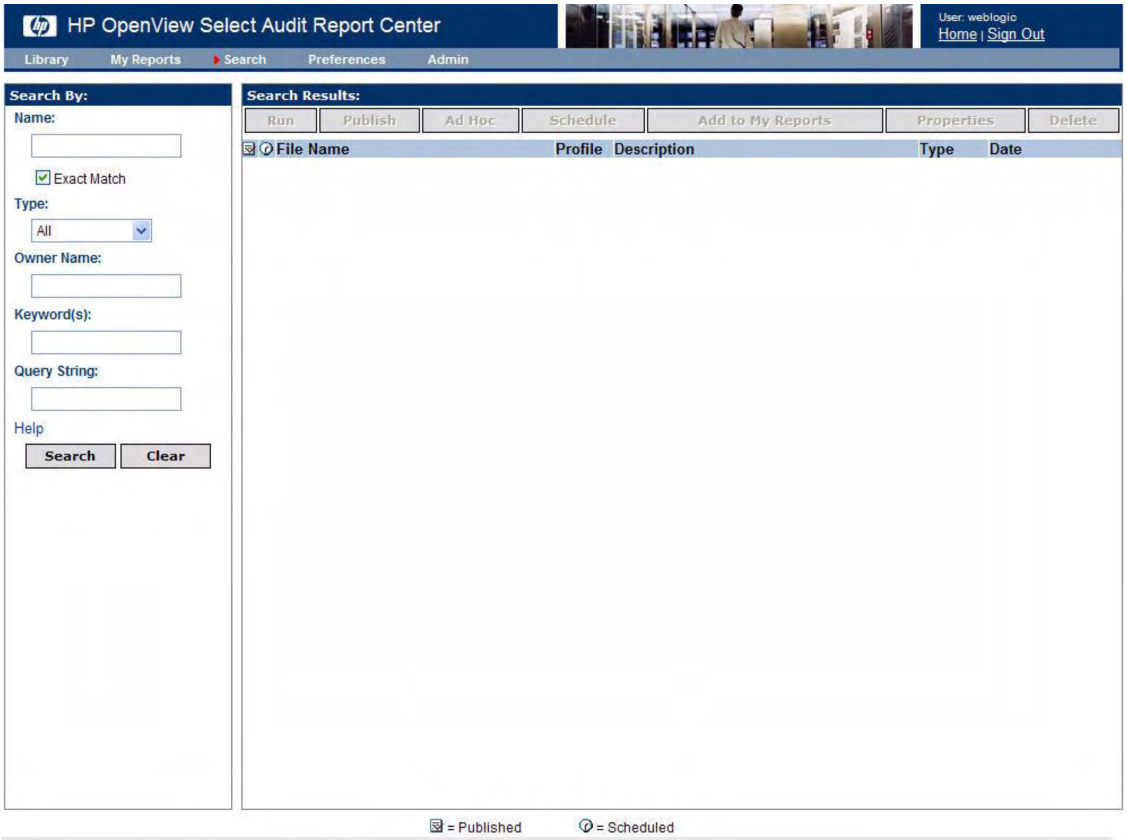


Figure 57 Search Screen

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

If you enter values in multiple fields in the **Search By** 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 appears.
2. In the **Search By** panel, complete any of the fields as follows:

   Name Enter the name of the report that you are searching for.

   Type Choose whether you are looking for report files (`Report`), already-run scheduled static output (`Output`), interactive views of static data (`Saved Results`), or all files (`all`).

   Owner Name Enter the name of the file's owner.

   Keyword(s) Enter any number of keywords associated with the report that you are looking for.

   Query String Enter a string to filter the returned reports.

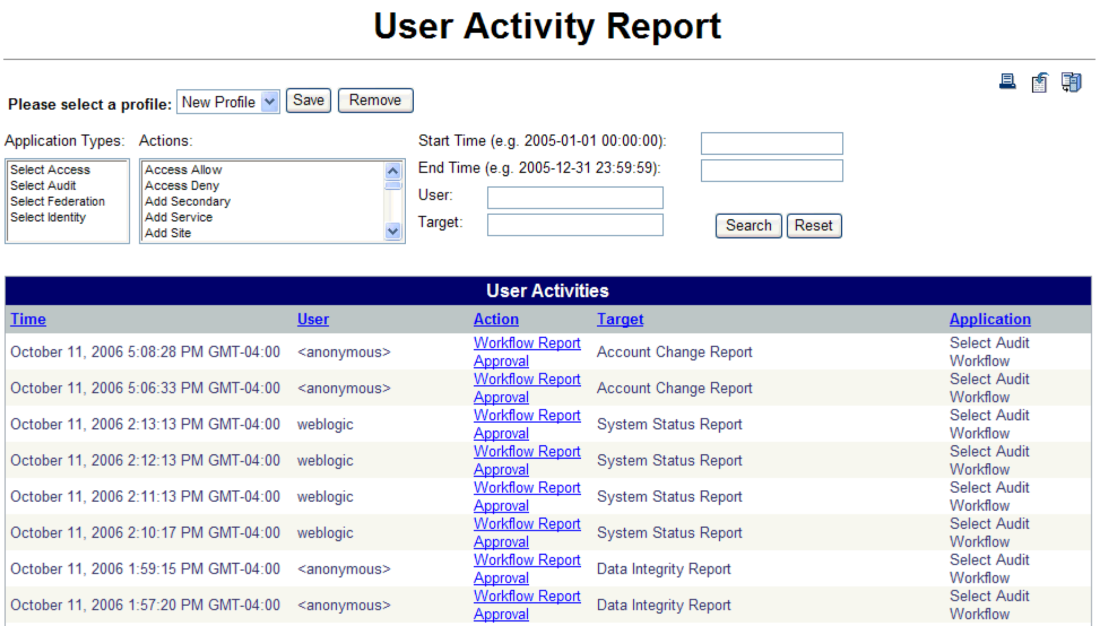
3. Click **Search**. Any matching reports appear in the **Search Results** panel.

For more information about searching for reports, refer to the *HP OpenView Select Audit 1.01 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

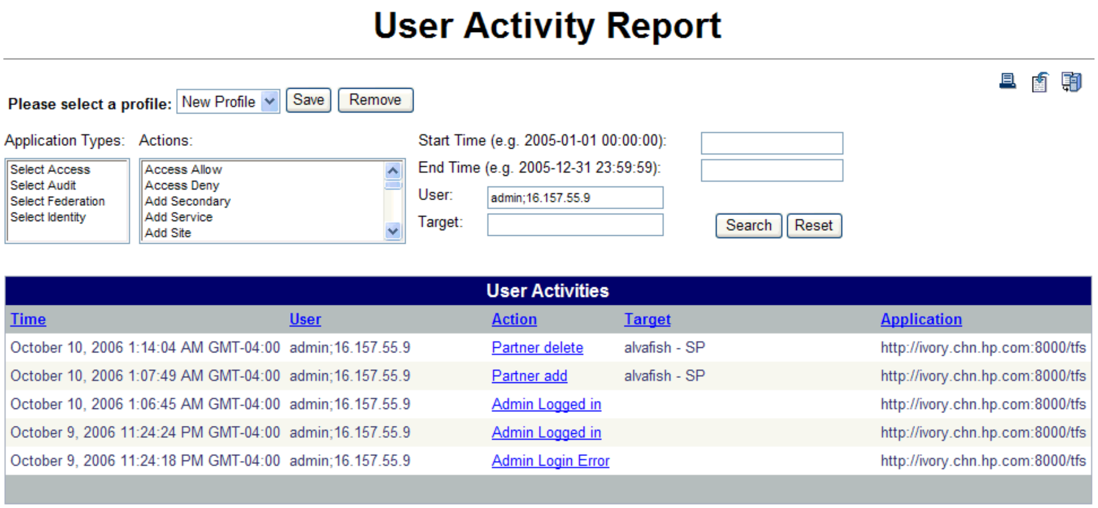
Please select a profile: New Profile

User Activities

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

Figure 58 Report Window

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



User Activity Report

Please select a profile: New Profile

Application Types: Select Access, Select Audit, Select Federation, Select Identity

Actions: Access Allow, Access Deny, Add Secondary, Add Service, Add Site

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

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

User: admin;16.157.55.9

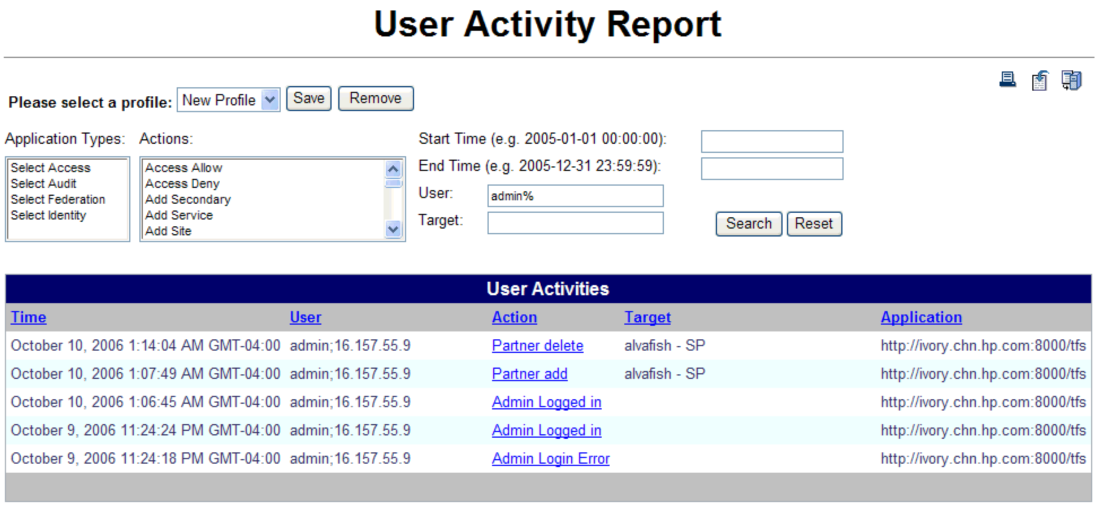
Target:

User Activities

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

Figure 59 Report Search Results

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 singe 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: New Profile

Application Types: Select Access, Select Audit, Select Federation, Select Identity

Actions: Access Allow, Access Deny, Add Secondary, Add Service, Add Site

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

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

User: admin%

Target:

User Activities

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

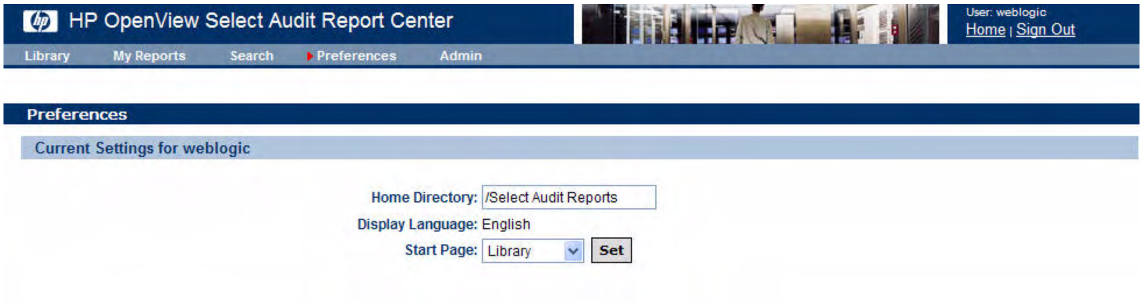
Figure 60 Report Wildcard Search Results

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 appear when you launch the Report Center).

➤ Library is the default start page.

1 Click **Preferences**. The **Preferences** screen appears.



Home Directory: /Select Audit Reports

Display Language: English

Start Page: Library

Figure 61 Preferences Screen

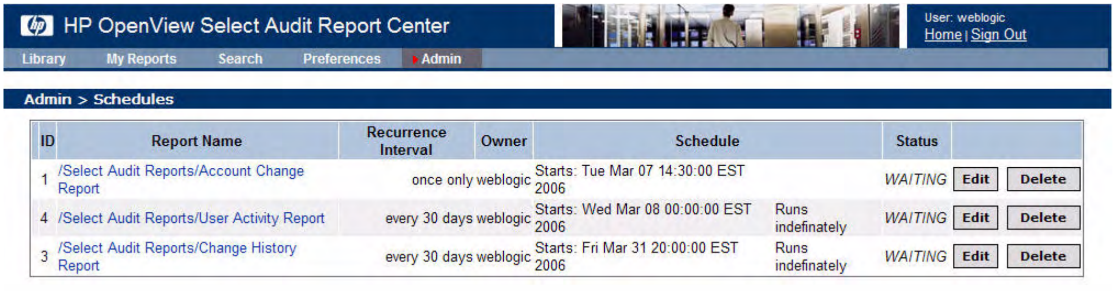
2 Enter the directory path in the **Home Directory** field.

3 Select a page from the **Start Page** drop-down list and click **Set**.

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 appears.



ID	Report Name	Recurrence Interval	Owner	Schedule		Status		
1	/Select Audit Reports/Account Change Report	once only	weblogic	Starts: Tue Mar 07 14:30:00 EST 2006		*WAITING*	Edit	Delete
4	/Select Audit Reports/User Activity Report	every 30 days	weblogic	Starts: Wed Mar 08 00:00:00 EST 2006	Runs indefinately	*WAITING*	Edit	Delete
3	/Select Audit Reports/Change History Report	every 30 days	weblogic	Starts: Fri Mar 31 20:00:00 EST 2006	Runs indefinately	*WAITING*	Edit	Delete

Figure 62 Report Center Schedules Screen

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 appears.

b Make the changes and click **Submit** to return to the **Schedules** screen.

4 To remove a schedule:

a Click **Delete**. A confirmation box appears.

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 11 Select Identity Event Filtering

If you have this report type assigned in SI	You will be able to see these events in Select Audit		
	Audit Event Name	**Application**	**Component Event Name**
Audit User	Sent Login request	SelectFederation	SF Protocol Sent Login Request
Audit User	Sent Logout request	SelectFederation	SF Protocol Sent Logout Request
Audit User	Received Login request	SelectFederation	SF Protocol Received Login Request
Audit User	Received Login request	SelectFederation	SF Protocol Received Logout Request
Audit User	Received Logout request	SelectFederation	SF API Received logout request
Audit User	Logged In	SelectAccess	Login
Audit User	Logged In	SelectIdentity	SI login
Audit User	Logged In	SelectFederation	SF Internal Logged In
Audit User	Logged Out	SelectAccess	Logout
Audit User	Logged Out	SelectIdentity	SI logout
Audit User	Logged Out	SelectFederation	SF Internal Logged Out
Audit User	Login Error	SelectAccess	Login error
Audit User	Login Error	SelectFederation	SF Internal Login Error
Audit User	Admin Logged in	SelectAccess	Admin Login
Audit User	Admin Logged in	SelectAccess	Delegate Admin Login
Audit User	Admin Logged in	SelectFederation	SF Admin Logged In
Audit User	Admin Logged Out	SelectAccess	Admin Logout
Audit User	Admin Logged Out	SelectAccess	Delegate Admin Logout
Audit User	Admin Logged Out	SelectFederation	SF Admin Logged Out
Audit User	Admin Login Error	SelectAccess	Admin Login error

Table 11 Select Identity Event Filtering (cont'd)

Audit User	Admin Login Error	SelectAccess	Delegate Admin Login error
Audit User	Admin Login Error	SelectFederation	SF Admin Login Error
Audit User	Credential expire	SelectAccess	Credential expire
Audit User	User Authenticated	SelectFederation	SF Internal User Authenticated
Audit User	User Authentication Error	SelectFederation	SF Internal User Authentication Error
Audit User	Access Allow	SelectAccess	Allow
Audit User	Access Deny	SelectAccess	Deny
Audit User	Reset Password	SelectIdentity	SI Reset Password
Audit User	Change Password	SelectIdentity	SI Change Password
Audit User	Change Password	SelectFederation	SF AdminAdm Password Changed
Audit User	Error Changing Password	SelectFederation	SF AdminAdm Error Changing Password
Audit User	Forget Password	SelectIdentity	SI Forget Password
Audit User	Expire Password Notification	SelectIdentity	SI Expire Password Notification
Audit User	Expire Password	SelectIdentity	SI Expire Password
Audit User	Hint Setup	SelectIdentity	SI Hint Setup
Audit User	Password Policy change	SelectAccess	passwordPolicyChange
Audit User	Password Reset Config Change	SelectAccess	password Reset Config Change
Audit User	User Add	SelectAccess	UserAdd
Audit User	User Add	SelectIdentity	SI Add NewUser
Audit User	User Delete	SelectAccess	UserDelete
Audit User	User Change	SelectAccess	UserChange
Audit User	User Change	SelectIdentity	SI Modify user
Audit User	Terminate User	SelectIdentity	SI Terminate User
Audit User	Modify Profile	SelectIdentity	SI Modify Profile
Audit User	Manage User Expiration	SelectIdentity	SI Manage User Expiration
Audit User	Move User	SelectIdentity	SI Move User
Audit User	disable before terminate	SelectIdentity	SI disable before terminate

Table 11 Select Identity Event Filtering (cont’d)

Audit User	Added Admin	SelectFederation	SF AdminAdm Added Admin
Audit User	Deleted Admin	SelectFederation	SF AdminAdm Deleted Admin
Audit User	User Consented	SelectFederation	SF User Consented
Audit User	Copy User	SelectIdentity	SI Copy User
Audit User	User Source Add	SelectAccess	userSourceAdd
Audit User	User Source Delete	SelectAccess	userSourceDelete
Audit User	User Source Change	SelectAccess	userSourceChange
Audit User	Security Violation	SelectIdentity	SI Security Violation
Audit User	Group Add	SelectAccess	GroupAdd
Audit User	Group Delete	SelectAccess	GroupDelete
Audit User	Group Change	SelectAccess	GroupChange
Audit User	User Role Add	SelectAccess	UserRoleAdd
Audit User	User Role Delete	SelectAccess	UserRoleDelete
Audit User	User Role Change	SelectAccess	UserRoleChange
Audit User	Admin Role Add	SelectIdentity	SI Admin role create
Audit User	Admin Role Delete	SelectIdentity	SI Admin role delete
Audit User	Admin Role Change	SelectIdentity	SI Admin role modify
Audit User	User role delegation Activate	SelectIdentity	SI User Role Delegation Activate
Audit User	User role delegation Deactivate	SelectIdentity	SI User Role Delegation Deactivate
Audit User	Folder Add	SelectAccess	FolderAdd
Audit User	Folder Delete	SelectAccess	FolderDelete
Audit User	Folder Change	SelectAccess	FolderChange
Audit User	Authn Add	SelectAccess	authnAdd
Audit User	Authn Delete	SelectAccess	authnDelete
Audit User	Authn Change	SelectAccess	authnChange
Audit User	Delegate delegated	SelectAccess	delegate delegate
Audit User	Delegate undelegate	SelectAccess	delegate undelegate
Audit User	Delegate inherit	SelectAccess	delegate inherit
Audit User	Delegate Change	SelectAccess	delegateChange

Table 11 Select Identity Event Filtering (cont'd)

Audit User	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
Audit User	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
Audit User	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
Audit User	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
Audit User	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
Audit User			
Audit User	Workflow create	SelectIdentity	SI workflow create
Audit User	Workflow delete	SelectIdentity	SI workflow delete
Audit User	Workflow modify	SelectIdentity	SI workflow modify
Audit User	Workflow view	SelectIdentity	SI workflow view
Audit User	Workflow copy	SelectIdentity	SI workflow copy
Audit User	Workflow import	SelectIdentity	SI workflow import
Audit User	Workflow export	SelectIdentity	SI workflow export
Audit User	Enable Service Membership	SelectIdentity	SI Enable Service Membership
Audit User	Disable Service Membership	SelectIdentity	SI Disable Service Membership
Audit User	Enable All Services	SelectIdentity	SI Enable All Services
Audit User	View resource attribute	SelectIdentity	SI View resource attribute
Audit User	View attribute	SelectIdentity	SI View attribute
Audit User	activeAttributes	SelectAccess	activeAttributes
Audit User	User Federated	SelectFederation	SF Internal User Federated
Audit User	User Federation Error	SelectFederation	SF Internal User Federation Error
Audit User	View Service Membership	SelectIdentity	SI View Service Membership
Audit User	Ignore Add	SelectIdentity	SI Ignore Add
Audit User	Ignore Modify	SelectIdentity	SI Ignore Modify
Audit User	Ignore Delete	SelectIdentity	SI Ignore Delete
Audit Service	WorkflowConfigChange	SelectAccess	WorkflowConfigChange

Table 11   Select Identity Event Filtering (cont'd)

Audit Service	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
Audit Service	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
Audit Service	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
Audit Service	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
Audit Service			
Audit Service	Workflow create	SelectIdentity	SI workflow create
Audit Service	Workflow delete	SelectIdentity	SI workflow delete
Audit Service	Workflow modify	SelectIdentity	SI workflow modify
Audit Service	Workflow view	SelectIdentity	SI workflow view
Audit Service	Workflow copy	SelectIdentity	SI workflow copy
Audit Service	Workflow import	SelectIdentity	SI workflow import
Audit Service	Workflow export	SelectIdentity	SI workflow export
Audit Service	Add Service	SelectIdentity	SI Add Service
Audit Service	Create service	SelectIdentity	SI Create service
Audit Service	Delete service	SelectIdentity	SI Delete service
Audit Service	Modify service	SelectIdentity	SI Modify service
Audit Service	Copy service	SelectIdentity	SI Copy service
Audit Service	Set service attribute values	SelectIdentity	SI Set service attribute values
Audit Service	Set service attribute properties	SelectIdentity	SI Set service attribute properties
Audit Service	Create service view	SelectIdentity	SI Create service view
Audit Service	Delete service view	SelectIdentity	SI Delete service view
Audit Service	Modify service view	SelectIdentity	SI Modify service view
Audit Service	Create service role	SelectIdentity	SI Create service role
Audit Service	Delete service role	SelectIdentity	SI Delete service role
Audit Service	Create service context	SelectIdentity	SI Create service context
Audit Service	Delete service context	SelectIdentity	SI Delete service context
Audit Service	Modify service context	SelectIdentity	SI Modify service context

Table 11 Select Identity Event Filtering (cont'd)

Audit Service	Import service	SelectIdentity	SI Import service
Audit Service	Modify service role	SelectIdentity	SI Modify service role
Audit Service	Svc Change Recon Modify User	SelectIdentity	SI Svc Change Recon Modify User
Audit Service	Svc Change Recon Add resource	SelectIdentity	SI Svc Change Recon Add resource
Audit Service	Svc Change Recon Delete resource	SelectIdentity	SI Svc Change Recon Delete resource
Audit Service	Service Export	SelectIdentity	SI Service Export
Audit Service	Create attribute	SelectIdentity	SI Create attribute
Audit Service	Delete attribute	SelectIdentity	SI Delete attribute
Audit Service	Modify attribute	SelectIdentity	SI Modify attribute
Audit Service	View attribute	SelectIdentity	SI View attribute
Audit Service	Copy attribute	SelectIdentity	SI Copy attribute
Audit Service	Attribute import	SelectIdentity	SI attribute export
Audit User Creation	User Add	SelectAccess	UserAdd
Audit User Creation	User Add	SelectIdentity	SI Add NewUser
Audit User Creation	Move User	SelectIdentity	SI Move User
Audit User Creation	Added Admin	SelectFederation	SF AdminAdm Added Admin
Audit User Creation	Copy User	SelectIdentity	SI Copy User
Audit User Creation	User Source Add	SelectAccess	userSourceAdd
Audit User Creation	Group Add	SelectAccess	GroupAdd
Audit User Creation	User Role Add	SelectAccess	UserRoleAdd
Audit User Creation	Admin Role Add	SelectIdentity	SI Admin role create
Audit User Creation	Folder Add	SelectAccess	FolderAdd
Audit User Creation	Authn Add	SelectAccess	authnAdd
Audit User Creation	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
Audit User Creation	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
Audit User Creation	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved

Table 11 Select Identity Event Filtering (cont'd)

Audit User Creation	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
Audit User Creation	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
Audit User Creation			
Audit User Creation	Workflow create	SelectIdentity	SI workflow create
Audit User Creation	Workflow delete	SelectIdentity	SI workflow delete
Audit User Creation	Workflow modify	SelectIdentity	SI workflow modify
Audit User Creation	Workflow view	SelectIdentity	SI workflow view
Audit User Creation	Workflow copy	SelectIdentity	SI workflow copy
Audit User Creation	Workflow import	SelectIdentity	SI workflow import
Audit User Creation	Workflow export	SelectIdentity	SI workflow export
Audit User Creation	Enable Service Membership	SelectIdentity	SI Enable Service Membership
Audit User Creation	Enable All Services	SelectIdentity	SI Enable All Services
Audit User Deletion	User Delete	SelectAccess	UserDelete
Audit User Deletion	Move User	SelectIdentity	SI Move User
Audit User Deletion	Deleted Admin	SelectFederation	SF AdminAdm Deleted Admin
Audit User Deletion	User Source Delete	SelectAccess	userSourceDelete
Audit User Deletion	Group Delete	SelectAccess	GroupDelete
Audit User Deletion	User Role Delete	SelectAccess	UserRoleDelete
Audit User Deletion	Admin Role Delete	SelectIdentity	SI Admin role delete
Audit User Deletion	Folder Delete	SelectAccess	FolderDelete
Audit User Deletion	Authn Delete	SelectAccess	authnDelete
Audit User Deletion	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
Audit User Deletion	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
Audit User Deletion	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
Audit User Deletion	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
Audit User Deletion	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted

Table 11 Select Identity Event Filtering (cont'd)

Audit User Deletion			
Audit User Deletion	Workflow create	SelectIdentity	SI workflow create
Audit User Deletion	Workflow delete	SelectIdentity	SI workflow delete
Audit User Deletion	Workflow modify	SelectIdentity	SI workflow modify
Audit User Deletion	Workflow view	SelectIdentity	SI workflow view
Audit User Deletion	Workflow copy	SelectIdentity	SI workflow copy
Audit User Deletion	Workflow import	SelectIdentity	SI workflow import
Audit User Deletion	Workflow export	SelectIdentity	SI workflow export
Audit User Deletion	Disable Service Membership	SelectIdentity	SI Disable Service Membership
Audit User Termination	Terminate User	SelectIdentity	SI Terminate User
Audit User Termination	disable before terminate	SelectIdentity	SI disable before terminate
Audit User Termination	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
Audit User Termination	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
Audit User Termination	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
Audit User Termination	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
Audit User Termination	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
Audit User Termination			
Audit User Termination	Workflow create	SelectIdentity	SI workflow create
Audit User Termination	Workflow delete	SelectIdentity	SI workflow delete
Audit User Termination	Workflow modify	SelectIdentity	SI workflow modify
Audit User Termination	Workflow view	SelectIdentity	SI workflow view

Table 11 Select Identity Event Filtering (cont'd)

Audit User Termination	Workflow copy	SelectIdentity	SI workflow copy
Audit User Termination	Workflow import	SelectIdentity	SI workflow import
Audit User Termination	Workflow export	SelectIdentity	SI workflow export
Audit User Password	Reset Password	SelectIdentity	SI Reset Password
Audit User Password	Change Password	SelectIdentity	SI Change Password
Audit User Password	Change Password	SelectFederation	SF AdminAdm Password Changed
Audit User Password	Error Changing Password	SelectFederation	SF AdminAdm Error Changing Password
Audit User Password	Forget Password	SelectIdentity	SI Forget Password
Audit User Password	Expire Password Notification	SelectIdentity	SI Expire Password Notification
Audit User Password	Expire Password	SelectIdentity	SI Expire Password
Audit User Password	Password Policy change	SelectAccess	passwordPolicyChange
Audit User Password	Password Reset Config Change	SelectAccess	password Reset Config Change
Audit User Password	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
Audit User Password	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
Audit User Password	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
Audit User Password	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
Audit User Password	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
Audit User Password			

Table 11 Select Identity Event Filtering (cont'd)

Audit User Password	Workflow create	SelectIdentity	SI workflow create
Audit User Password	Workflow delete	SelectIdentity	SI workflow delete
Audit User Password	Workflow modify	SelectIdentity	SI workflow modify
Audit User Password	Workflow view	SelectIdentity	SI workflow view
Audit User Password	Workflow copy	SelectIdentity	SI workflow copy
Audit User Password	Workflow import	SelectIdentity	SI workflow import
Audit User Password	Workflow export	SelectIdentity	SI workflow export
Audit User Hint	Hint Setup	SelectIdentity	SI Hint Setup
Audit User Login	Sent Login request	SelectFederation	SF Protocol Sent Login Request
Audit User Login	Sent Logout request	SelectFederation	SF Protocol Sent Logout Request
Audit User Login	Received Login request	SelectFederation	SF Protocol Received Login Request
Audit User Login	Received Login request	SelectFederation	SF Protocol Received Logout Request
Audit User Login	Received Logout request	SelectFederation	SF API Received logout request
Audit User Login	Logged In	SelectAccess	Login
Audit User Login	Logged In	SelectIdentity	SI login
Audit User Login	Logged In	SelectFederation	SF Internal Logged In
Audit User Login	Logged Out	SelectAccess	Logout
Audit User Login	Logged Out	SelectIdentity	SI logout
Audit User Login	Logged Out	SelectFederation	SF Internal Logged Out
Audit User Login	Login Error	SelectAccess	Login error
Audit User Login	Login Error	SelectFederation	SF Internal Login Error
Audit User Login	Admin Logged in	SelectAccess	Admin Login
Audit User Login	Admin Logged in	SelectAccess	Delegate Admin Login
Audit User Login	Admin Logged in	SelectFederation	SF Admin Logged In

Table 11 Select Identity Event Filtering (cont’d)

Audit User Login	Admin Logged Out	SelectAccess	Admin Logout
Audit User Login	Admin Logged Out	SelectAccess	Delegate Admin Logout
Audit User Login	Admin Logged Out	SelectFederation	SF Admin Logged Out
Audit User Login	Admin Login Error	SelectAccess	Admin Login error
Audit User Login	Admin Login Error	SelectAccess	Delegate Admin Login error
Audit User Login	Admin Login Error	SelectFederation	SF Admin Login Error
Audit User Login	Credential expire	SelectAccess	Credential expire
Audit User Login	Reset Password	SelectIdentity	SI Reset Password
Audit User Login	Password Reset Config Change	SelectAccess	password Reset Config Change
Audit User Login	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
Audit User Login	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
Audit User Login	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved
Audit User Login	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
Audit User Login	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
Audit User Login			
Audit User Login	Workflow create	SelectIdentity	SI workflow create
Audit User Login	Workflow delete	SelectIdentity	SI workflow delete
Audit User Login	Workflow modify	SelectIdentity	SI workflow modify
Audit User Login	Workflow view	SelectIdentity	SI workflow view
Audit User Login	Workflow copy	SelectIdentity	SI workflow copy
Audit User Login	Workflow import	SelectIdentity	SI workflow import
Audit User Login	Workflow export	SelectIdentity	SI workflow export
Admin Configuration	WorkflowConfigChange	SelectAccess	WorkflowConfigChange
Admin Configuration	WorkflowChangeRequest submitted	SelectAccess	WorkflowChangeRequest submitted
Admin Configuration	WorkflowChangeRequest approved	SelectAccess	WorkflowChangeRequest approved

Table 11 Select Identity Event Filtering (cont’d)

Admin Configuration	WorkflowChangeRequest rejected	SelectAccess	WorkflowChangeRequest rejected
Admin Configuration	WorkflowChangeRequest reverted	SelectAccess	WorkflowChangeRequest reverted
Admin Configuration			
Admin Configuration	Workflow create	SelectIdentity	SI workflow create
Admin Configuration	Workflow delete	SelectIdentity	SI workflow delete
Admin Configuration	Workflow modify	SelectIdentity	SI workflow modify
Admin Configuration	Workflow view	SelectIdentity	SI workflow view
Admin Configuration	Workflow copy	SelectIdentity	SI workflow copy
Admin Configuration	Workflow import	SelectIdentity	SI workflow import
Admin Configuration	Workflow export	SelectIdentity	SI workflow export
Admin Configuration	Logging Config Change	SelectAccess	loggingConfigChange
Admin Configuration	Select Audit Report Config	SelectAudit	

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 12 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 13 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 14 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 14 Audit Workflow Status Thresholds (cont'd)

Node	Description	Red	Yellow	Green
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