

HP OpenView Select Audit

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

Software Version: 1.01

Installation 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

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

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	Preparing to Install Select Audit	7
	Audience	7
	The Select Audit Documentation Set	7
	Installation Environment	8
	Supported Platforms	8
	Minimum System Requirements	9
	Platform Availability	9
	Chapter Summary	9
2	Select Audit Installation and Deployment	11
	Select Audit Installers	11
	Audit Server	11
	Audit Connector	11
	Deploying Audit Server	12
	Select Audit EAR File	12
	Deployment Wizard	12
3	Installing Select Audit	13
	Before Installing Select Audit	13
	Integrating with Select Identity	13
	Installing on HP-UX	14
	Creating a DBA User	14
	Installing in a Clustered Environment	14
	Running the Select Audit Installers	15
	The Impact of Running Control Panel Applications	15
	The Importance of the Correct Administration Entitlements	15
	Installation Order	15
	Running the Audit Server Installer	16
	To install the Audit Server	16
	Post-Installation Steps	39
	Configuring Log4j	39
	Enabling logging	40
	Setting Appenders	40
	log4j.properties file	40
	Redirecting WebLogic Server Output	42
	Adding Users to WebLogic Roles	43
	To add users	43
	Configuring a Mail Session in WebLogic	43
	To configure a mail session	43

Setting a Default Time Zone for Database Connection Pools	44
To setup the default time zone	44
Configuring UTF-8 Fonts in PDF Channel Reports	44
Running the Audit Connector Installer	46
Select Application Configuration Requirements	46
Select Audit Connector Installer Mode Overview	46
Running the Connector Installer in Default Mode	47
Running the Connector Installer in Console Mode	54
Running the Connector Installer in Silent Mode	55
Uninstalling the Audit Server	56
To uninstall the Audit Server on Windows	56
Uninstalling the Audit Connector	60
To uninstall the Audit Connector	61
4 Using Self-Healing Services	65
Self-Healing Services	65
Data Collector	65
Data Collection Process	66
Data Collected	67
Using the Data Collector in a Clustered Environment	67
Using SHS	67
To start collecting data	68
Index	69

1 Preparing to Install Select Audit

Businesses are subject to legal audit and compliance requirements. The consequences of non-compliance include potential fines, closures, product delays, litigation or even jail. As a result, the management and audit of identity and access across disparate systems, processes, services and environments is a business imperative.

HP OpenView Select Audit is part of HP's business service Identity Management Suite. It manages the complete audit lifecycle and simplifies the fulfillment of regulatory compliance requirements. It helps organizations meet corporate governance requirements by providing a consolidated and tamper-aware identity audit trail. Select Audit is extensible to additional OpenView products and third-party applications.

Audience

This document is intended for system administrators mandated to install and configure HP OpenView Select Audit 1.01 to suit their business and industry environment. This guide assumes a working knowledge of:

- WebLogic application server administration and configuration
- Oracle database administration
- understanding of the J2EE environment

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.

Installation Environment

Select Audit has two installers: a Connector installer and a Server installer. The Connector installer installs the Audit Connector on client machines running one or more of the HP OpenView Select products (Select Identity, Select Access, Select Federation, or any combination of these products). The Server installer installs the Audit Server and any remaining Select Audit components.

Before you begin installing Select Audit, consider your current network architecture and see what limitations can affect your deployment of Select Audit components on various network host machines. Potential limitations are described in the following topics:

- [Minimum System Requirements](#) on page 9
- [Platform Availability](#) on page 9

Supported Platforms

The Select Audit Connector installer supports the following platforms:

- Select Identity 4.0
- Select Access 6.1 SP3 and 6.2
- Select Federation 6.5 and 6.6

The platforms, servers and applications supported by Select Audit are listed in [Table 1](#).

Table 1 Supported Platforms, Servers, and Applications

Operating system support	<ul style="list-style-type: none"> • Microsoft Windows 2003 • HP-UX 11.23 • Red Hat Linux AS 3.0 • Solaris 9 and Solaris 10 (Audit Connector)
Application and portal servers	<ul style="list-style-type: none"> • BEA WebLogic Application Server 8.1 SP5
Audit connectors	<ul style="list-style-type: none"> • HP OpenView Select Identity 4.0 • HP OpenView Select Access 6.1 P3 and 6.2 • HP OpenView Select Federation 6.5 and 6.6
Audit storage and databases	<ul style="list-style-type: none"> • Oracle 9i • Oracle 10g
Compliance report packs	<ul style="list-style-type: none"> • Sarbanes-Oxley (Optional)

Minimum System Requirements

To install any of the Select Audit components, your system must meet the minimum hardware and software requirements outlined in [Table 2](#).

Table 2 Minimum System Requirements

Hardware & Software	Minimum on Windows	Minimum on UNIX
Processor	Pentium 4	Linux: Pentium 4
Memory	1 GB RAM	1 GB RAM
Disk space (combination of temporary space and real space required for a full install)	250 MB	For Linux: 150 MB For HP-UX: 220 MB
Video card	256 colors	256 colors
Operating systems	Windows 2003 Server Service Pack 2	Red Hat Enterprise Linux 3 HP-UX 11.B.11.23 64 bit with all required patches

- ▶ An X11-based X Window System must be running on the Select Audit Server machine for chart rendering purposes.

Platform Availability

The Select Audit components are available for the Windows 2003 and UNIX (Linux and HP-UX) platforms.

You can install Select Audit components on different platforms; all components communicate with each other irrespective of the platform you installed them on.

Chapter Summary

This guide includes the chapters listed in [Table 3](#).

- ▶ 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 3 Chapter Summary

Chapter	Description
Chapter 1, Preparing to Install Select Audit	This chapter describes the installation environment needed for Select Audit.
Chapter 2, Select Audit Installation and Deployment	This chapter describes the Select Audit installer and how Select Audit components are deployed. It also describes how the Report Server is installed.
Chapter 3, Installing Select Audit	This chapter provides an overview of how to install and uninstall the Select Audit components on your network.
Chapter 4, Using Self-Healing Services	HP OpenView Self-Healing Services (SHS) are part of HP's built-in support. This chapter describes SHS and how to use it in Select Audit.

2 Select Audit Installation and Deployment

This chapter describes the Select Audit installers and how Select Audit components are deployed. It also describes how the Report Server is installed.

Select Audit Installers

There are two main modules to install for Select Audit:

- the Audit Server
- the Audit Connector

The Server installer installs the Audit Server, reporting, and Self-healing Services components. For information about Self-healing Services, see [Chapter 4, Using Self-Healing Services](#). The Connector installer installs the Audit Connector on client machines running one or more of the Select products (Select Identity, Select Access, Select Federation, or any combination of these products).

The Connector installer can also be run silently or in a non-GUI (console) mode. The files to be installed are organized as features and sub-features. Users can choose to install only the server, a specific report pack, or everything. Each feature can be customized to only install certain files.

Audit Server

The Server installer copies an EAR file containing the necessary Java files to your system. This EAR file is then deployed to the application server using the Deployment Wizard. For information about the Deployment Wizard, see [Deployment Wizard](#) on page 12.

Audit Connector

The Audit Connector relies on a configuration file that is created via the Connector installer and can be modified via the Audit Server's configuration GUI. It is recommended the Audit Server is already installed and running before installing the Audit Connector.

The Connector installer installs both the `jar` and a LaunchAnywhere native executable file to run the Audit Connector. The Connector requires a set of libraries to execute, which are installed and added to the launcher's classpath.

Deploying Audit Server

The Audit Server must be deployed on a previously-installed J2EE server and database using the platform's administration tools.



The database and application server must already be set up before installing the Audit Server. The installer does not handle this configuration.

To deploy the installed Select Audit application archive, you must use predetermined JNDI names for any required J2EE objects. You can change the JNDI names by modifying the configuration files that are packaged in the Audit Server application archive.

Select Audit EAR File

The Select Audit EAR file can be deployed to the application server using the Deployment Wizard. In the Deployment Wizard, you can specify the server type, the server's installation folder, the host and port the server is running on, an administration username and password, the installation folder to copy the EAR file to, and the deployment targets to run on. The installation folder is only configuration option outside the deployment.

Deployment Wizard

The Deployment Wizard prompts you for information about your J2EE server in order to automatically deploy the Audit Server. The EAR file is copied to the main installation directory (`/SelectAudit/auditserver/dist`) at installation time. Post-installation, the wizard calls the `Weblogic.admin` task to deploy the Audit Server. If any errors are detected as you move through the wizard, you will be returned to the screen containing the error, with information about the error.

3 Installing Select Audit

Because HP employs InstallAnywhere installers, Select Audit is as simple to install as it is to configure. This chapter provides an overview of how to install and uninstall the Select Audit components on your network.

Before Installing Select Audit

Before Select Audit is installed, you must:

- 1 Install WebLogic 8.1 SP5.
- 2 Create a new domain. This will be used to deploy the Audit Server application on the **Deployment Settings** screen.
- 3 Create a new database instance.

You will need the database server name, the new database instance port number and SID. Have this information available before you start the Select Audit installation process. The Oracle Database server must have the Java option installed, and the Audit user must have permissions to run Java stored procedures.

The Audit Server installer creates the audit user in the users tablespace. By default, the users tablespace is limited to a maximum size of 32 GB. This could lead to the improper functioning of the Audit Server. Because each database implementation is different, HP recommends that you review the *Oracle Database Administrator's Guide* and develop a strategy for managing the users tablespace datafiles.

Integrating with Select Identity

If you are integrating with Select Identity (SI), you must first create all the Select Identity users that will be using Select Audit, in Select Audit. You can do this by creating the users in either WebLogic's native user store (embedded LDAP), or an external LDAP, when using J2EE authentication. Alternatively, create the users in the Select Access identity location when using Select Access authentication. The user login name should be the same as the login name used in Select Identity.

If you have to create the GLOBALUSER correlation table, make sure the GUID is the same as the login name in Select Identity. See [Correlating Users Between Applications](#) in the *HP OpenView Select Audit 1.01 Administration Guide* for more information about the GLOBALUSERS table.

Make sure you have the following information available before beginning:

For the SI server:

- host name
- port number

- super administrator name
- super administrator password

For the SI database:

- host name
- port number
- database name (SID)
- login user name
- login user password, etc.

Installing on HP-UX

If you are installing Select Audit on HP-UX, change the default name lookup order from `dns files` to `files dns` in `/etc/nsswitch.conf`.

On the **Deployment Wizard: Server Connection: Cluster** screen, if the command `telnet localhost` returns the error “localhost: Unknown host”, the name `localhost` failed to resolve to the address `127.0.0.1`. To fix this problem, make sure that the `/etc/nsswitch.conf` file contains either of the following lines:

```
hosts: dns [NOTFOUND=continue] files
```

OR

```
hosts: files dns
```

and that the `/etc/hosts` file contains the following line:

```
127.0.0.1 localhost loopback
```

When `localhost` resolves correctly to `127.0.0.1`, the command `telnet localhost` should return a login prompt if the Telnet service is enabled.

Creating a DBA User

You must have a DBA username and password in order to install the Select Audit database tables and complete all the database-level setup needed by the application. This database admin user must have **sysdba** privileges in the database.

Installing in a Clustered Environment

If you want to run Select Audit in a clustered environment, you must follow these steps before running the Audit Server installer.

- 1 Create a WebLogic Cluster domain.
- 2 Run `nodemanager` on each of the managed server machines.
- 3 Start all managed servers.
- 4 Create a shared directory on the administration server machine.

- 5 Mount the shared filesystem on the WebLogic Administration server machine as well as all the machines hosting a managed server. Make sure the mounted path is identical on each of the cluster member machines.



Its important to make sure the mounted filesystem has read/write permissions on each managed server.

When you run the Audit Server installer, you are given the option of installing in a single server or clustered environment. See [Step 11](#) on page 23 for more information.

Running the Select Audit Installers

This section describes some factors that affect the running of the Select Audit installers.

The Impact of Running Control Panel Applications

If you are uninstalling and/or installing, or configuring Select Audit components on a Windows host computer, ensure that you do not have the Services window or any other Control Panel application open. This open Control Panel application triggers conflicts that can cause the installer to behave abnormally.

The Importance of the Correct Administration Entitlements

On Windows, HP recommends that only administrators with local administration entitlements install the product. Otherwise, the installer cannot create the required registry entries.

On UNIX, only run installers using the same user that WebLogic is running on.

- 1 Ensure that `printenv` is in your path.
 - On Solaris, it is usually located in `/usr/ucb`.
 - On HP-UX or Linux, it is usually located in `usr/bin`.
- 2 Include a Java Virtual Machine in your path. If you are running the Audit Server installer, it is recommended to prepend to the path `<BEA_HOME>/jrockit81sp5_142_08/bin`.

Installation Order

HP recommends that you install the Audit Server first and then the Audit Connector. When you run the Connector installer, you need to know two things:

- the IP address of the Audit Server
- the username and password used by the Audit Connector to log to the Audit Server

In order to know these two items, you need to have previously installed the Audit Server and created a WebLogic user the Administrator role, that corresponds to your connector.

If you know this information beforehand and install the Audit Connector first, the Audit Connector will log the events locally on the client machine and will not be able to send batches to the Audit Server (it does not exist yet). Once the Audit Server is installed successfully, your connector will be automatically registered by the Audit Server, as long as you installed the Audit Server at the IP address specified in the Connector installer.

If the Audit Server IP address differs from that specified during the Audit Connector install, the Audit Connector will not be able to register with the Audit Server and send batches to it. You must manually change the IP address specified at Connector install time in the `connector.props` file.

Running the Audit Server Installer

The Audit Server installer takes you through the following steps for installing and deploying the Audit Server:

- entering installation information
- configuring the server
- entering deployment information
- configuring database settings
- deploying Select Audit

To install the Audit Server

- 1 Start the Audit Server installation program by running the corresponding setup file from the root of the Select Audit product CD:

- **On Windows:**

Double-click `SelectAuditServerInstall.exe`.



You should be logged in as an Administrator to install the Audit Server or Audit Connector.



If you are uninstalling and/or installing, or configuring Select Audit components on a Windows host computer, ensure that you do not have the Services window or any other Control Panel application open. This open Control Panel application triggers conflicts that can cause the installer to behave abnormally.

OR

- **On HP-UX or Linux:**

Enter the following command:

`SelectAuditServerInstall.bin`.



You should be logged in using the same user that WebLogic is running on to install the Audit Server or Audit Connector.

The installer extracts the installation files, then prepares the Select Audit Install wizard. When it has finished loading, the **Server Installer Introduction** screen appears, as shown in Figure 1.

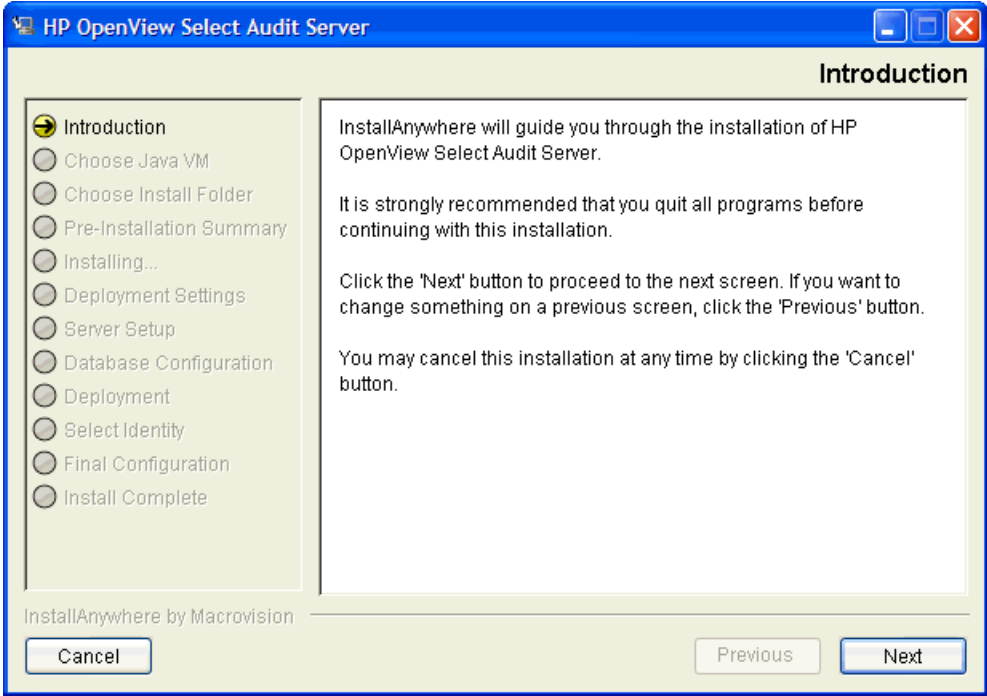


Figure 1 Server Installer Introduction Screen

- 2 Click **Next**. The **Choose Java Virtual Machine** screen appears, as shown in Figure 2.

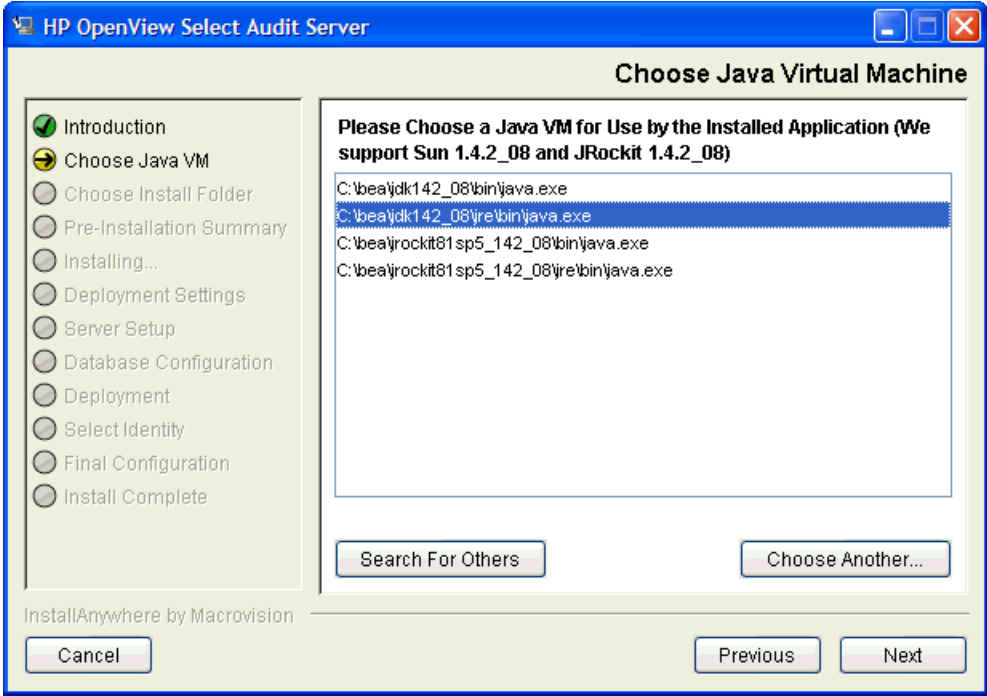


Figure 2 Choose Java Virtual Machine Screen

- 3 Select one of the supported Java VMs.

▶ If you select an unsupported Java VM, a warning screen appears, as shown in Figure 3. Re-select a supported Java Virtual Machine.



Figure 3 Wrong Java VM Version Screen

- 4 Click **Next**. The **Choose Install Folder** screen appears, as shown in Figure 4.

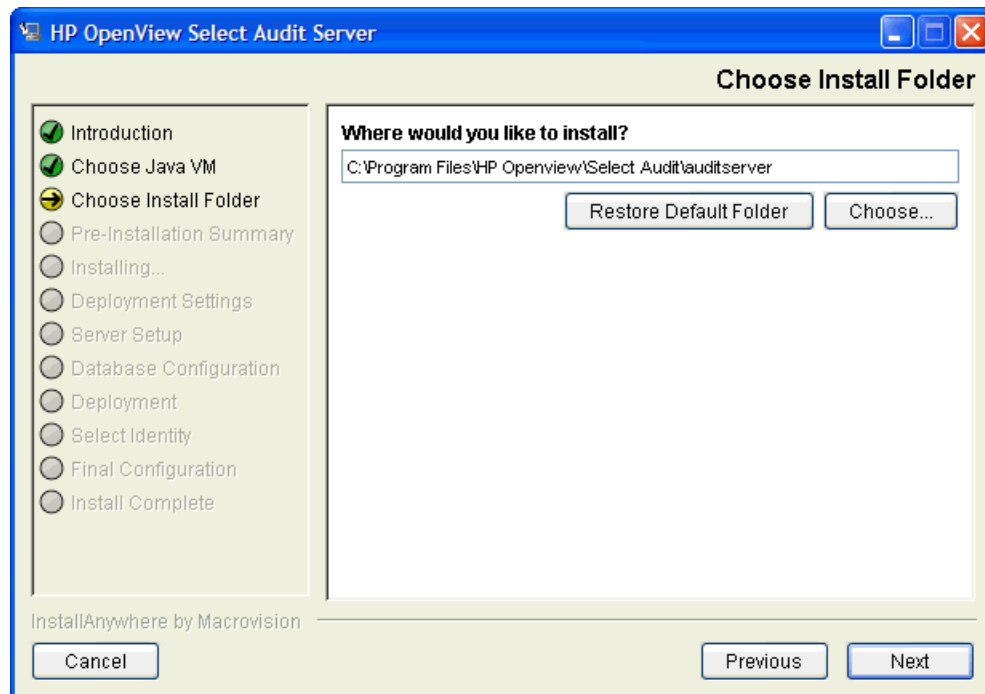


Figure 4 Choose Install Screen

- 5 Select the location where you wish to install the Audit Server and click **Next**. The **Pre-Installation Summary** screen appears, as shown in [Figure 5](#).

▶ The following characters are not valid in file or folder names when specifying where to install the Audit Server:

() { } [] / \ : ; " ' < > | \$ * ? # & ,

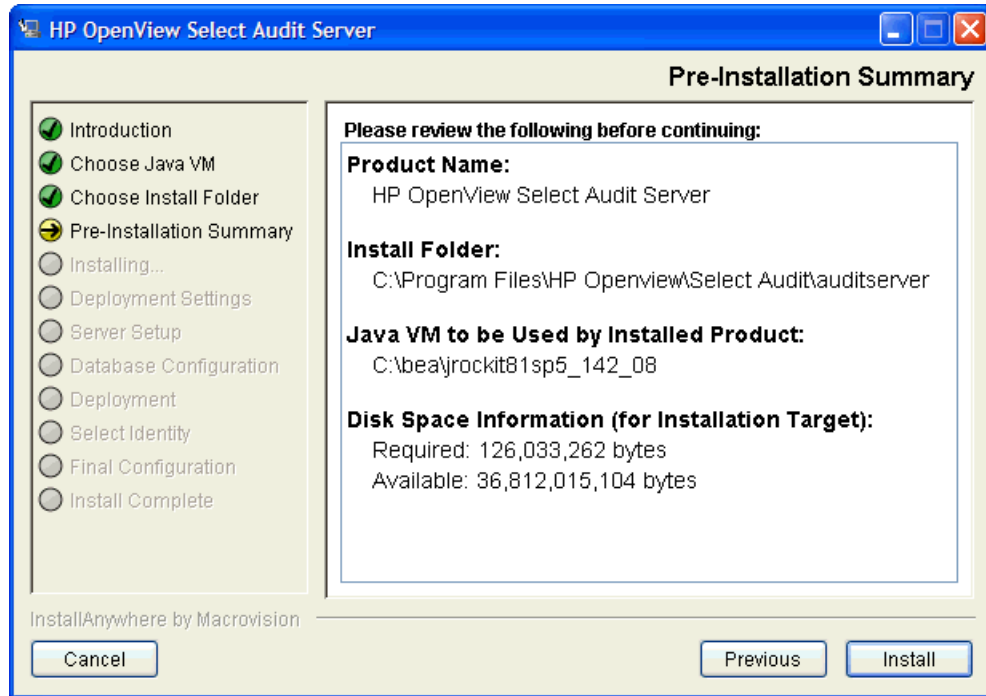


Figure 5 Pre-Installation Summary Screen

The **Pre-Installation Summary** screen creates a digest of the following installation information you provided to this point:

- The installation folder you chose to install the Audit Server in.
 - The installation location of the Java Virtual Machine that the Select Audit Install wizard has automatically installed. The Java Virtual Machine is required to run both the maintenance program as well as Select Audit components.
 - The amount of disk space required for the components you selected to install. If the disk space required exceeds what is available on this computer, free up space.
- 6 Review the information on the **Pre-Installation Summary** screen. If the information is correct, click **Install**.
- ▶ To change any of the installation settings, click **Previous** to return to the screen containing the settings you want to change.

The Audit Server begins to install and the **Server Installation Progress** screen appears, as shown in [Figure 6](#).

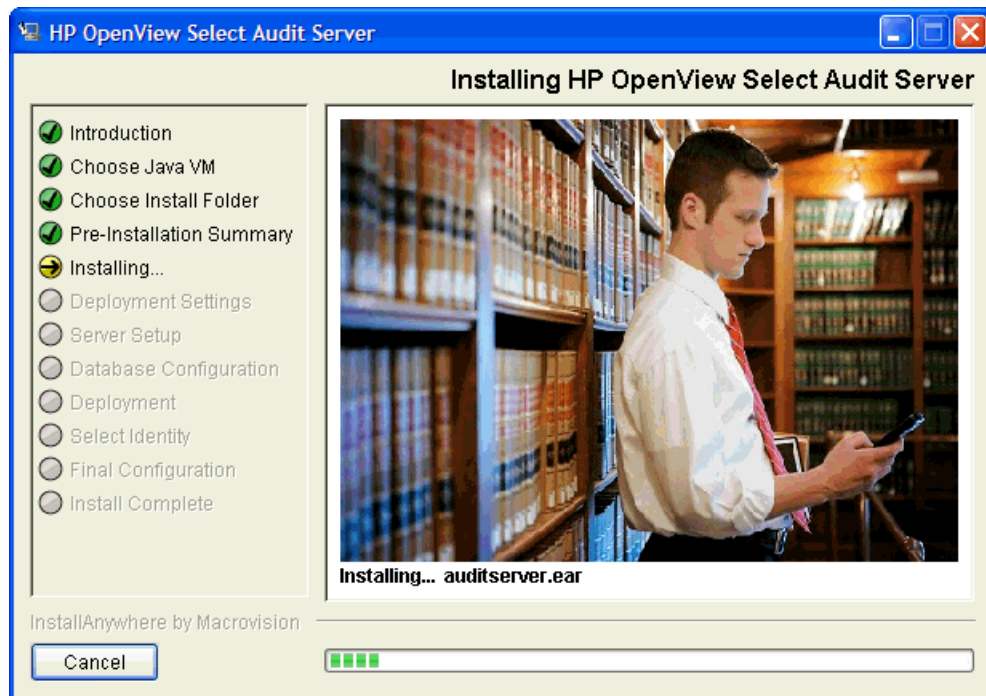


Figure 6 Server Installation Progress Screen

When the Audit Server installer is finished, click **Next**. The Deployment Settings screen appears as shown in [Figure 7](#).

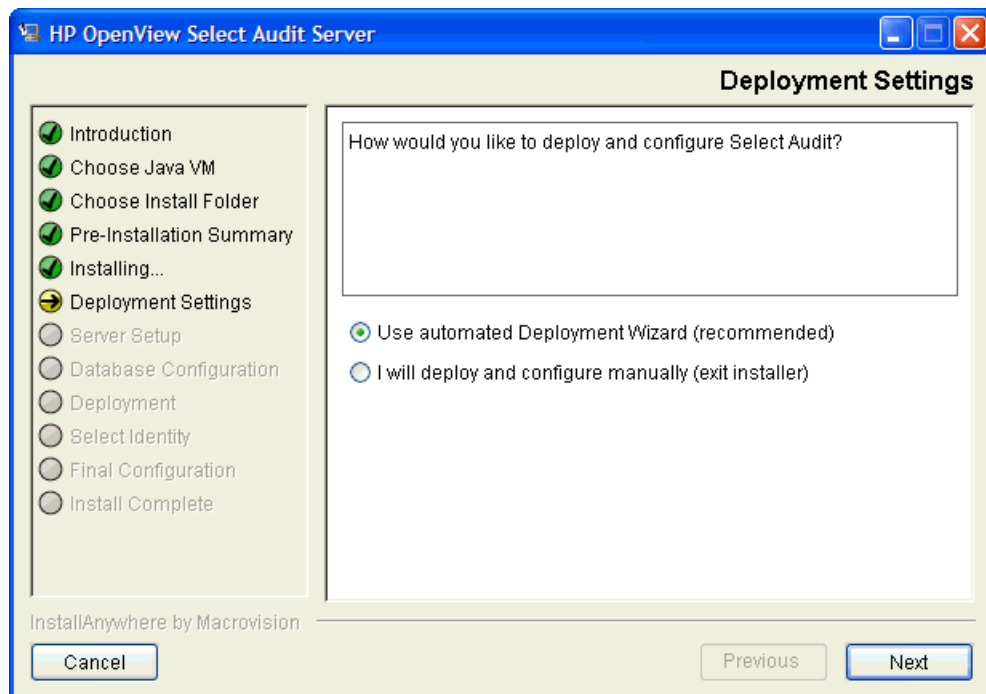


Figure 7 Deployment Settings Screen

7 Do one of the following:

- Select the **Use automated Deployment wizard (recommended)** radio button and click **Next**. The **Deployment Wizard: Server Installation** screen appears, as shown in [Figure 8](#). Proceed to [Step 8](#) on page 22.

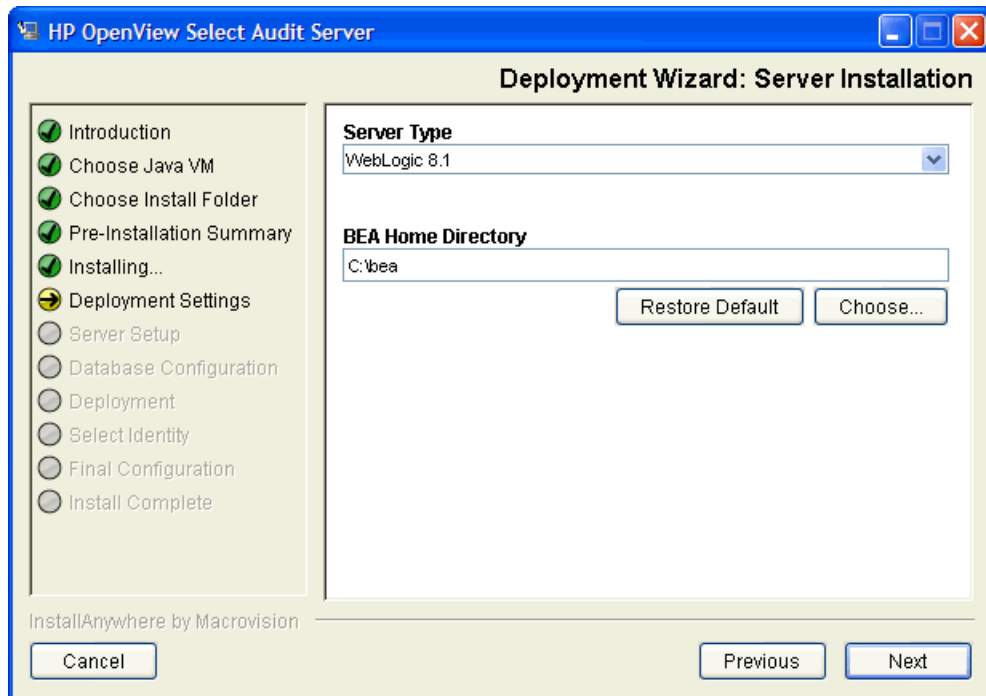


Figure 8 Deployment Wizard: Server Installation Screen

- Select the **I will deploy and configure manually (exit installer)** radio button and click **Next**. The **Install Complete** screen appears.

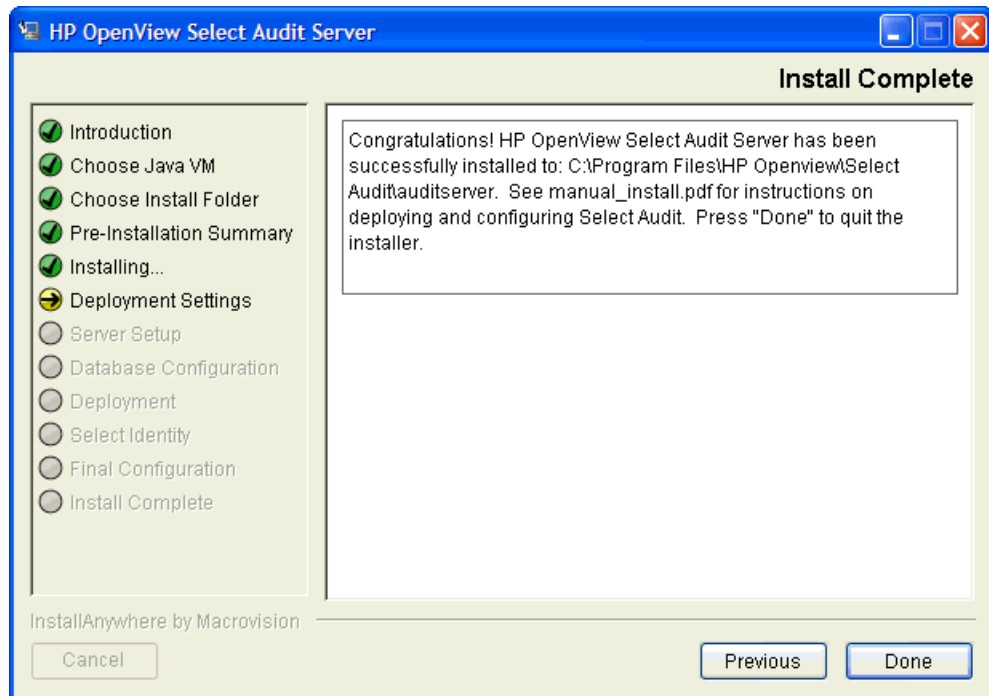


Figure 9 Install Complete Screen

Click **Done**. The installer closes. Follow the instructions provided in the *HP OpenView Select Audit 1.01 Manual Audit Server Installation & Setup Guide* to complete the Audit Server manual installation.

- 8 Do one of the following:
 - If the default values are acceptable, proceed to [Step 9](#).
 - Complete the required information as follows:
 - Select a server type from the **Server Type** drop-down list.
 - Enter the location of the server installation folder in the **BEA Home Directory** field.
 - ▶ Click **Restore Default** to restore the Select Audit defaults.
- 9 Click **Next**. The **Deployment Settings** screen appears, as shown in [Figure 10](#).

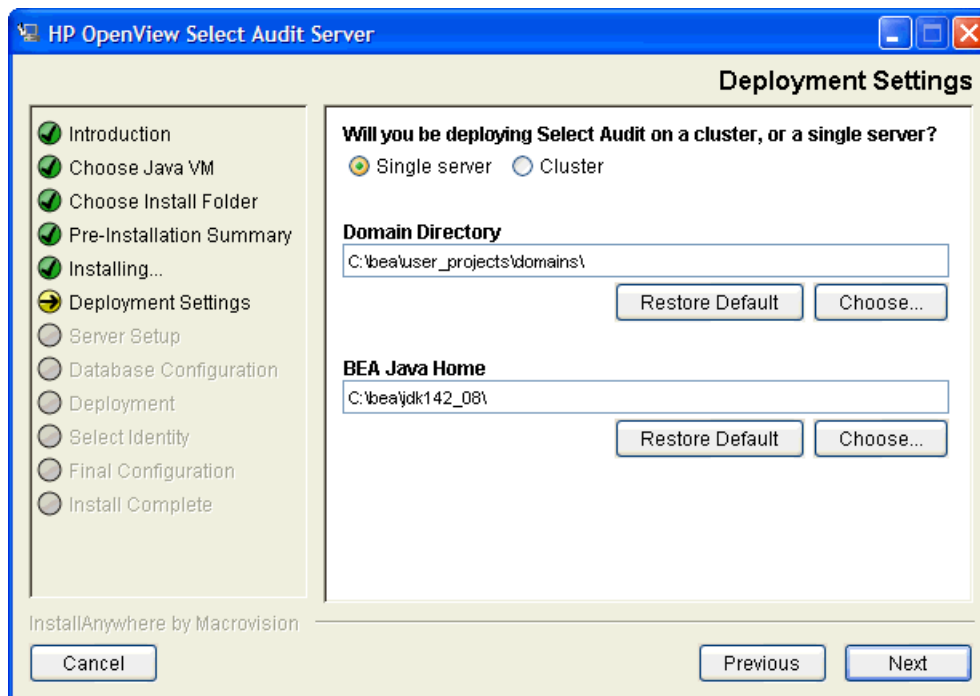


Figure 10 Deployment Settings Screen

- 10 Do the following:
 - Select whether to deploy Select Audit as a standalone server or on a cluster.
 - Enter the path of the domain directory in the **Domain Directory** field.
 - Use the root or the domain directory for this field.
 - Enter the location of the JDK in the **BEA Java Home** field.
 - Click **Restore Default** to restore the Select Audit defaults.
- 11 Click **Next**. The **Deployment Wizard: Server Connection** screen appears. The screen has different fields, depending on whether you chose a standalone or clustered deployment.

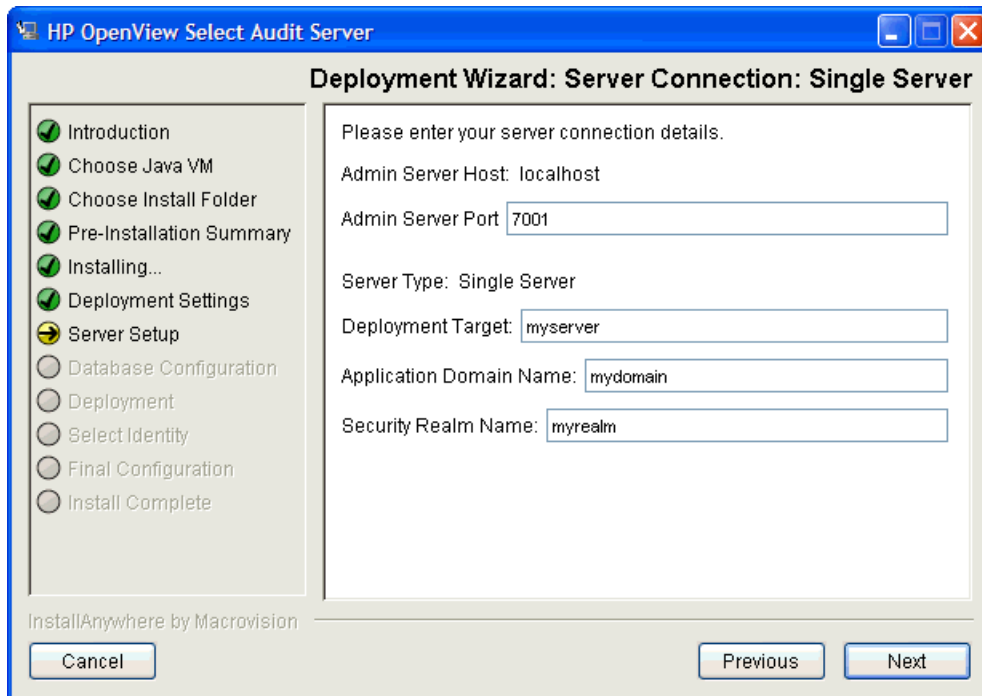


Figure 11 Deployment Wizard: Server Connection: Single Server Screen

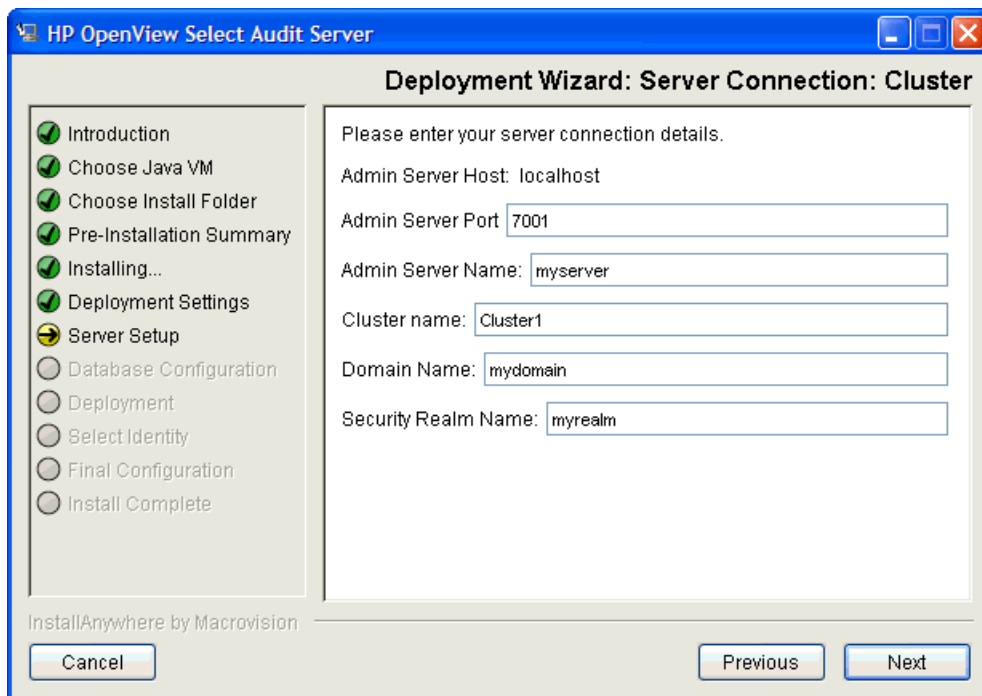


Figure 12 Deployment Wizard: Server Connection: Cluster Screen

- 12 Enter the installation directory information for the BEA WebLogic server by doing one of the following:
 - **Deploying a standalone server:**
 - Enter the Administration server port number in the **Admin Server Port** field.
 - Enter the name of the deployment target in the **Deployment Target** field.
 - Enter the domain name in the **Application Domain Name** field.
 - Enter the realm name in the **Security Realm Name** field.
 - **Deploying on a cluster:**
 - Enter the Administration server port number in the **Admin Server Port** field.
 - Enter the Administration server name in the **Admin Server Name** field.
 - Enter the server's cluster name in the **Cluster Name** field.
 - Enter the domain name in the **Domain Name** field.
 - Enter the realm name in the **Security Realm Name** field.
- ▶ When specifying Select Audit installation path, make sure to specify the mounted filesystem to ensure consistent paths on both the WebLogic Administration server as well as managed servers.
- 13 Click **Next**. The **Deployment Wizard: External Address** screen appears, as shown in [Figure 13](#).

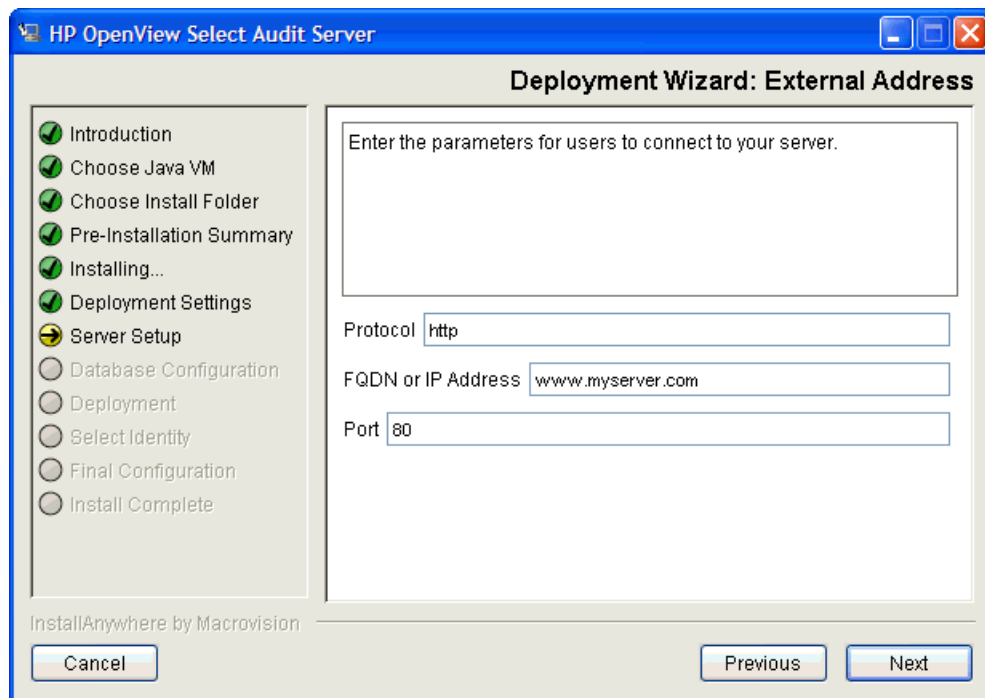


Figure 13 Deployment Wizard: External Address Screen

- 14 Enter the URL that users will use to connect to the system in the **FQDN or IP Address:** field.
 - ▶ Be sure to change the default values to valid ones. Incorrect values can affect the proper functioning of the Audit Server.

The **Deployment Wizard: Authentication** screen appears, as shown in [Figure 14](#).



Figure 14 Deployment Wizard: Authentication Screen

- 15 Enter the **Server administrator login name** and **Server administrator password** in the appropriate fields.

The Server Administrator login name and Server Administrator password refer to the name and password of the WebLogic administrator that was created with the WebLogic server installation. The WebLogic administrator information is a prerequisite for installing the Audit Server.

- 16 Click **Next**. The **Please Wait** screen appears while the Audit Server is deployed.

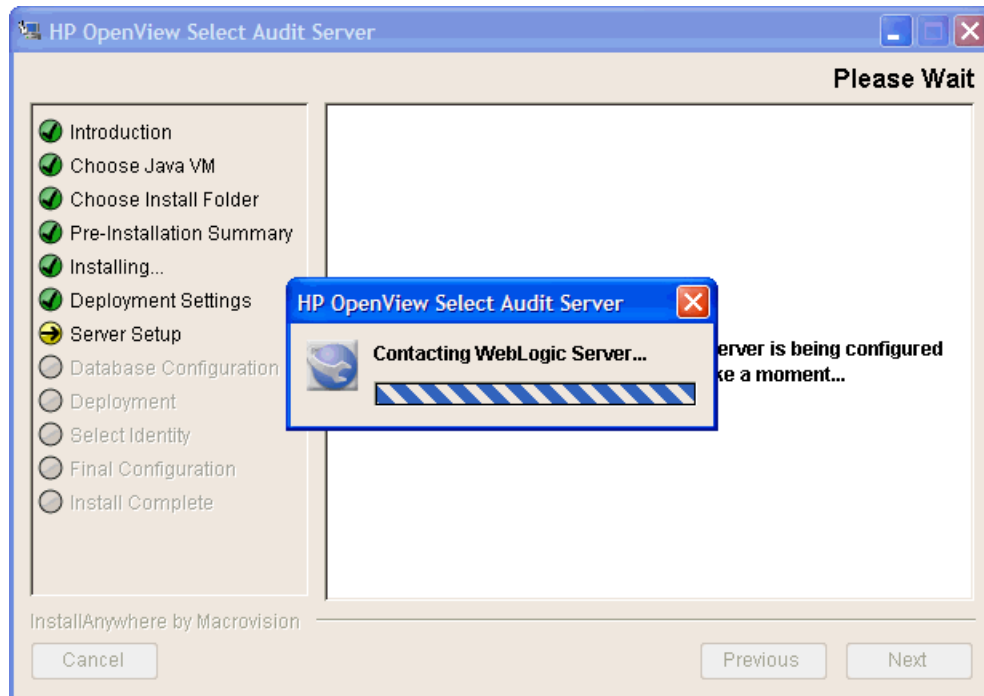


Figure 15 Please Wait Screen

When the Audit Server is deployed, the **Database Configuration: JDBC Services** screen appears, as shown in [Figure 16](#).

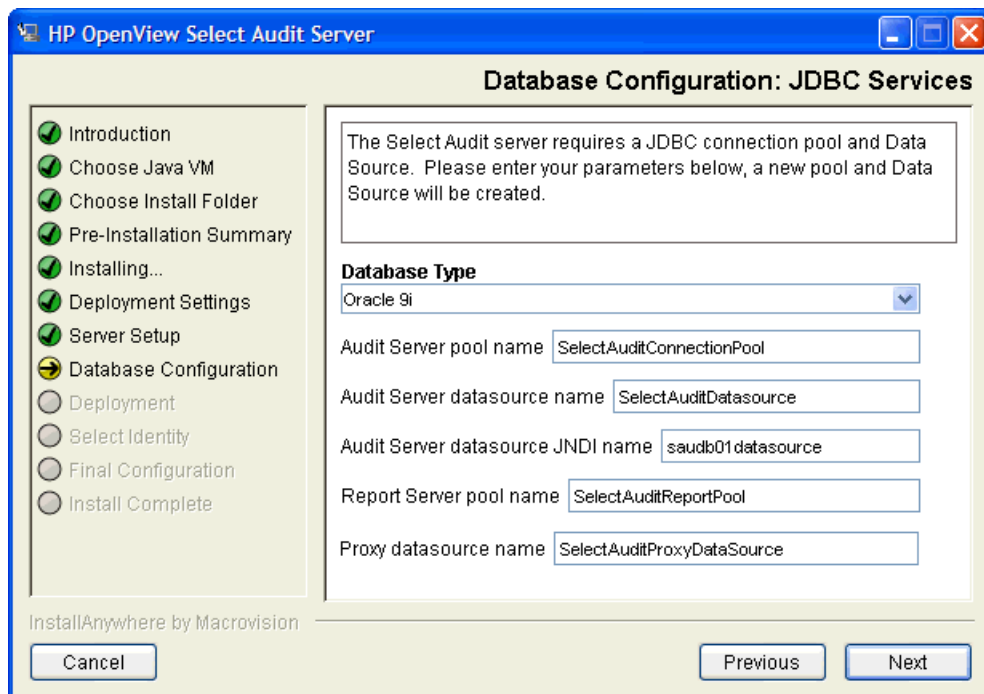


Figure 16 Database Configuration: JDBC Services Screen

17 Complete the screen as follows:

- Select a database type from the **Database Type** drop-down list.
- Enter the name of the pool in the **Audit Server pool name** field.

- Enter the data source name in the **Audit Server datasource name** field.
 - Enter the JNDI name in the **Datasource JNDI Name** field.
 - Enter the pool name for the Report Server in the **Report Server pool name** field.
 - Enter the name for the proxy data source in the **Proxy datasource name** field.
- 18 Click **Next**. The **Database Configuration: Connection Details** screen appears, as shown in Figure 17.

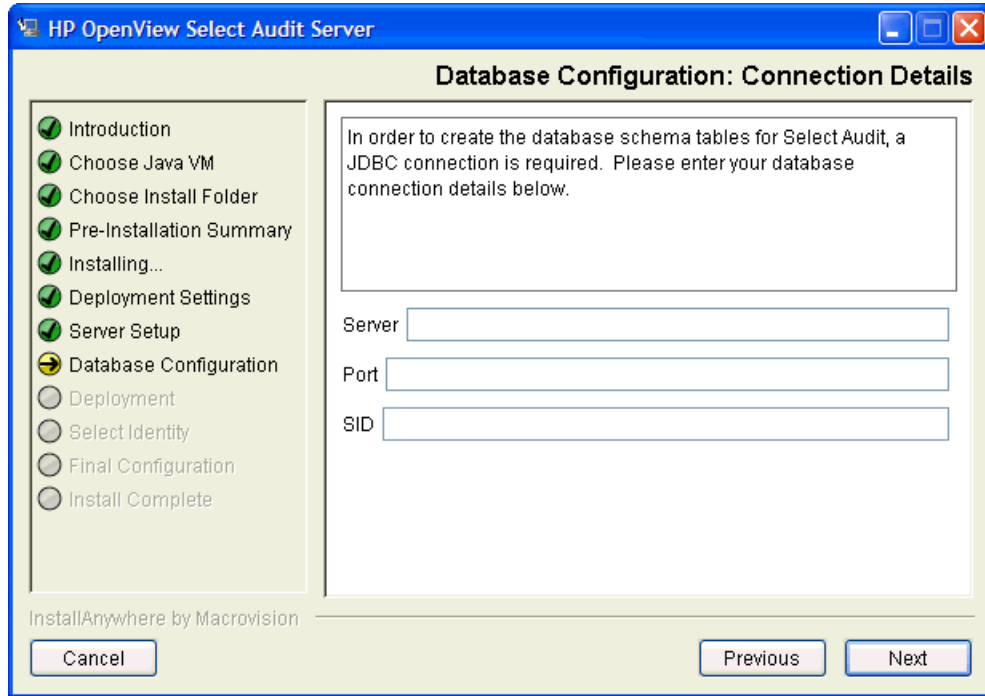


Figure 17 Database Configuration: Connection Details Screen

- 19 Complete the required information as follows:
- Enter the database server address in the **Server** field.
 - Enter the database listener port number in the **Port** field.
 - Enter the Oracle database SID in the **SID** field.
- 20 Click **Next**. The **Database Configuration: DB Users** screen appears, as shown in Figure 18.

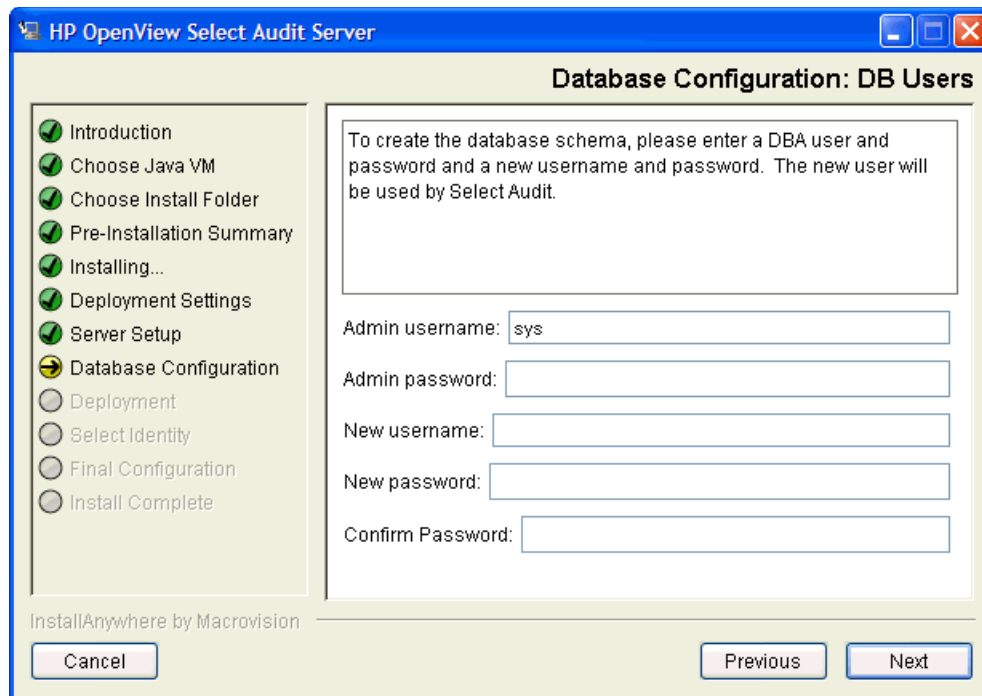


Figure 18 Database Configuration: DB Users Screen

21 Complete the required information as follows:

- Enter the DBA username in the **Admin username** field.



The database admin user must have **sysdba** privileges in the database.

- Enter the DBA password in the **Admin password** field.
- Enter a new username in the **New username** field.



You cannot re-use an old username.

- Enter a new user password in the **New password** field.
- Re-enter the password in the **Confirm Password** field.



A database instance must already be created prerequisite before installing Select Audit.

The **New username** and **New password** are set up so that the DBA account is not trusted with everything Select Audit does. Select Audit uses the DBA account to set up the schema when more permissions are needed, and it uses the new account for everything else (writing batches to the database, normalizing the data, creating tables, etc.).

22 Click **Next**. The **Please Wait** screen appears while installer deploys the database schema and configures Select Audit, as shown in [Figure 19](#).

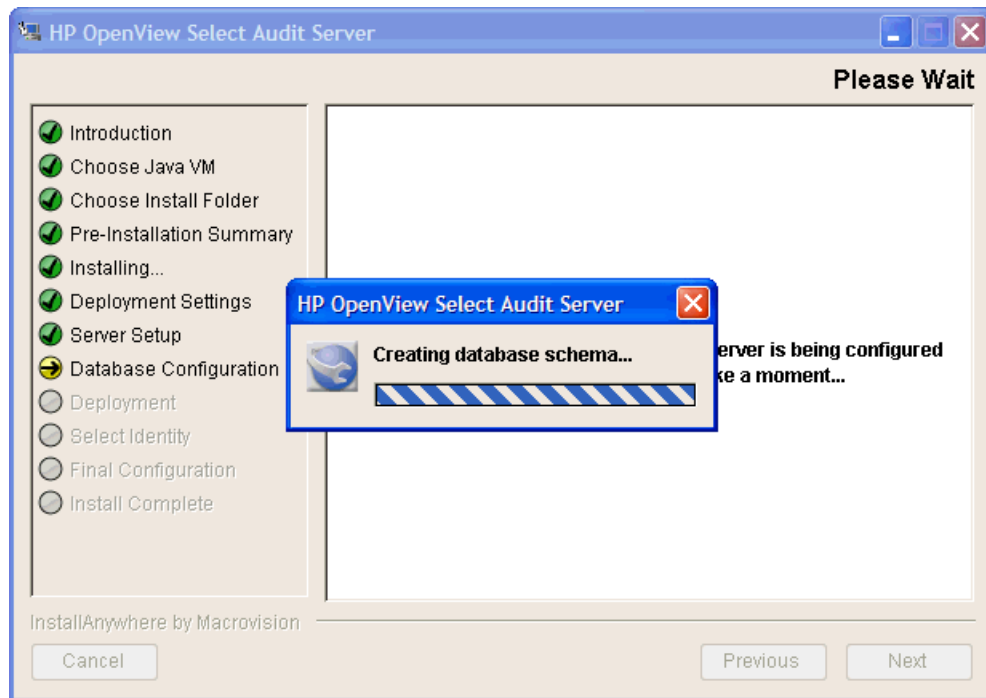


Figure 19 Please Wait Screen

On completion, the **Report Notification** screen appears, as shown in [Figure 20](#).

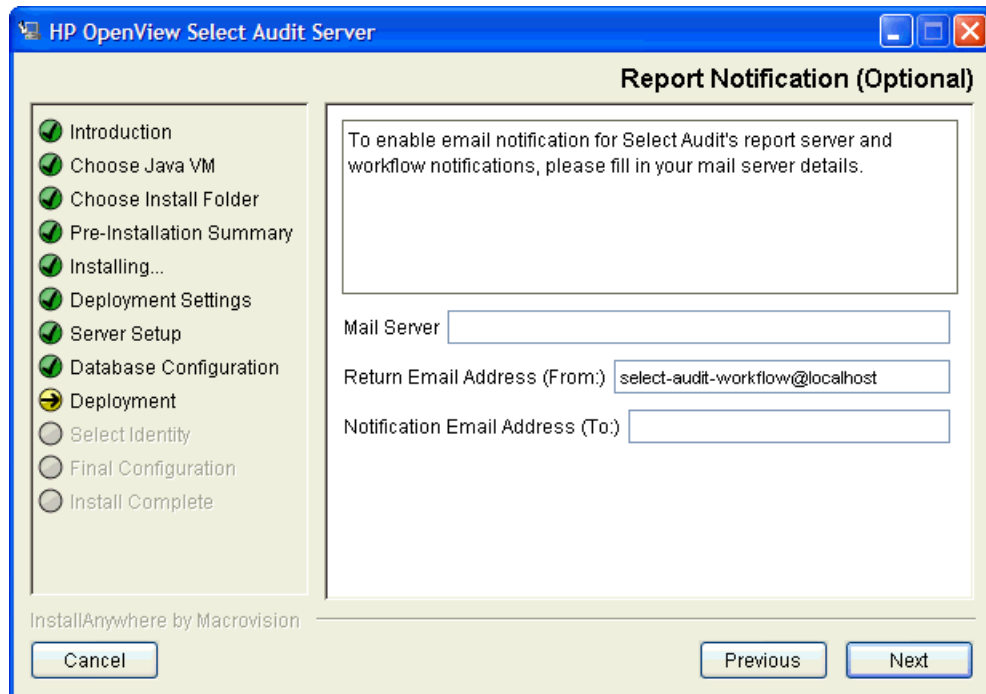


Figure 20 Report Notification Screen

23 Complete the following:

- Enter the mail server name in the **Mail Server** field.
- Enter a valid address the email is sent from in the **Return Email Address (From)** field.
- ▶ If you leave the default address in the **Return Email Address (From)** field, you must change the address to a valid email address using the WebLogic console after installation. See [Configuring a Mail Session in WebLogic](#) on page 43 for more information.
- Enter the address you want to send the email to in the **Notification Email Address (To)** field.

24 Click **Next**. The **Please Wait** screen appears while installer deploys Select Audit, as shown in [Figure 21](#).

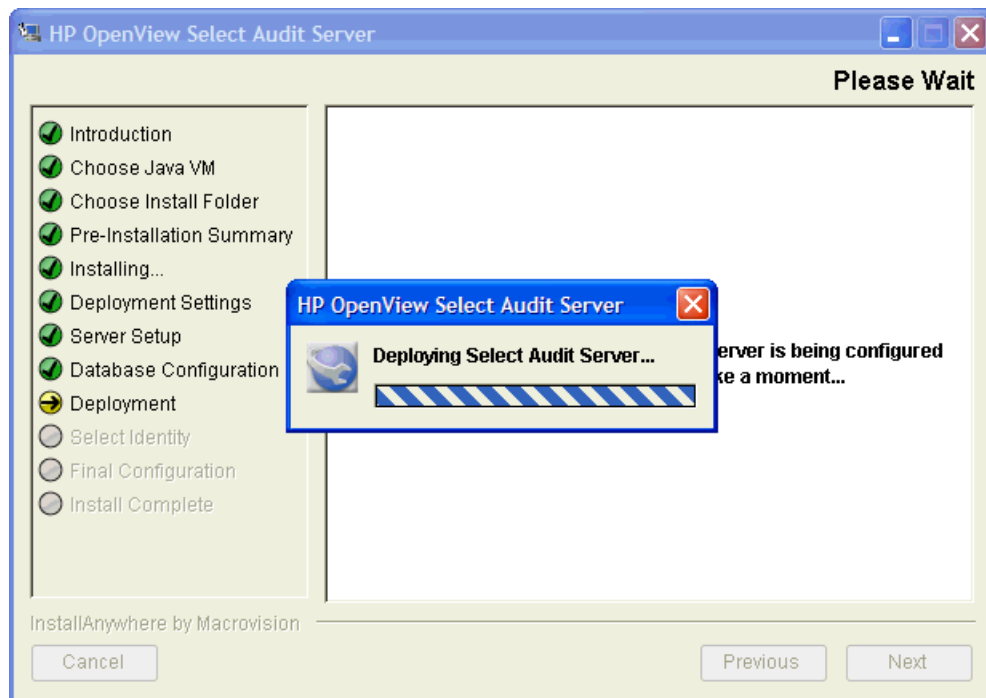


Figure 21 Please Wait Screen

On completion, the **Log4J Setup** screen appears, as shown in [Figure 22](#).

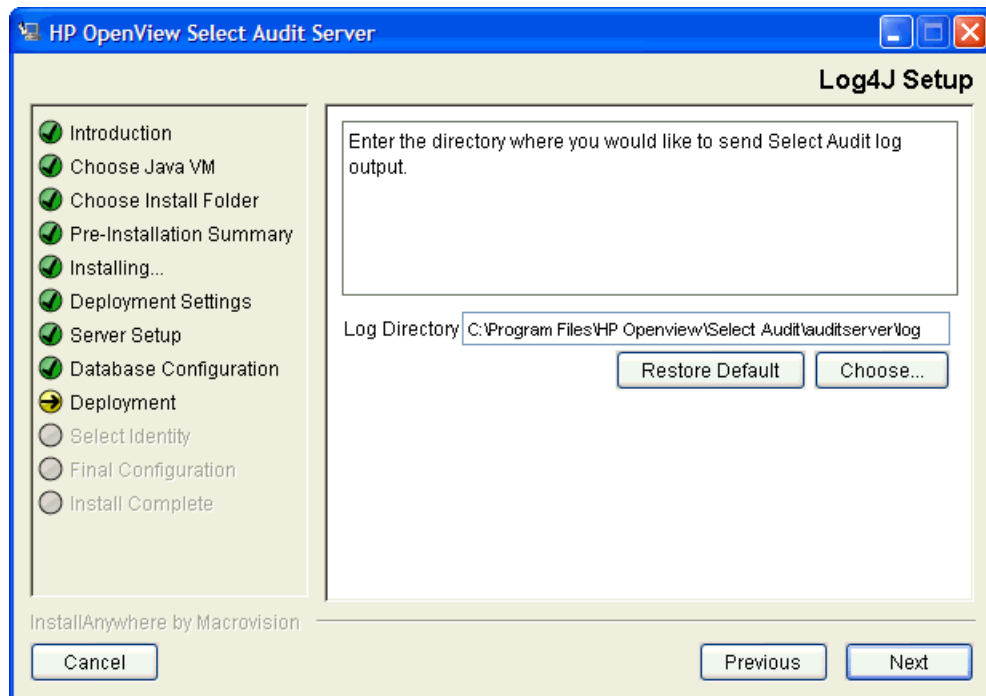


Figure 22 Log4J Setup Screen

- 25 Click **Choose** or enter the directory where you would like Select Audit log output stored in the **Log Directory** field.
 - ▶ Click **Restore Default** to restore the Select Audit defaults.
- 26 Click **Next**. The **Select Identity Integration** screen appears, as shown in [Figure 23](#).

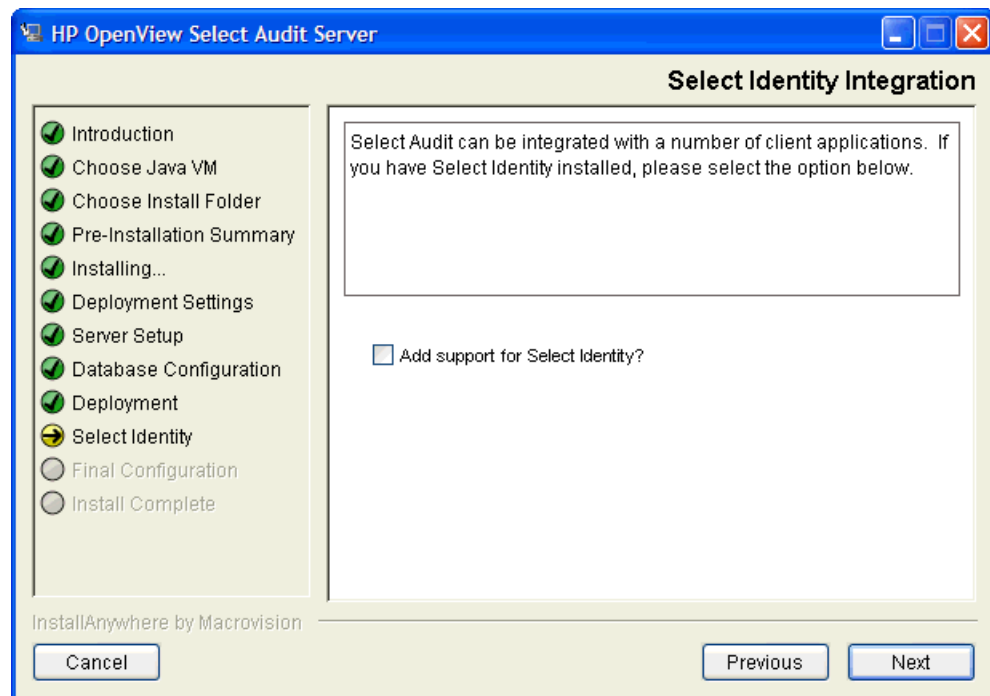


Figure 23 Select Identity Integration Screen

- 27 Select the **Add support for Select Identity?** check box to integrate Select Identity with Select Audit. Refer to the *HP OpenView Select Audit 1.01 Administration Guide* for more information about integrating Select Audit with Select Identity.
- 28 Click **Next**. If you chose to integrate with Select Identity, the **SI Server Info** screen appears, as shown in [Figure 24](#). If you chose not to integrate with Select Identity, the **Shutdown WebLogic** screen appears. Go to [Step 35](#).

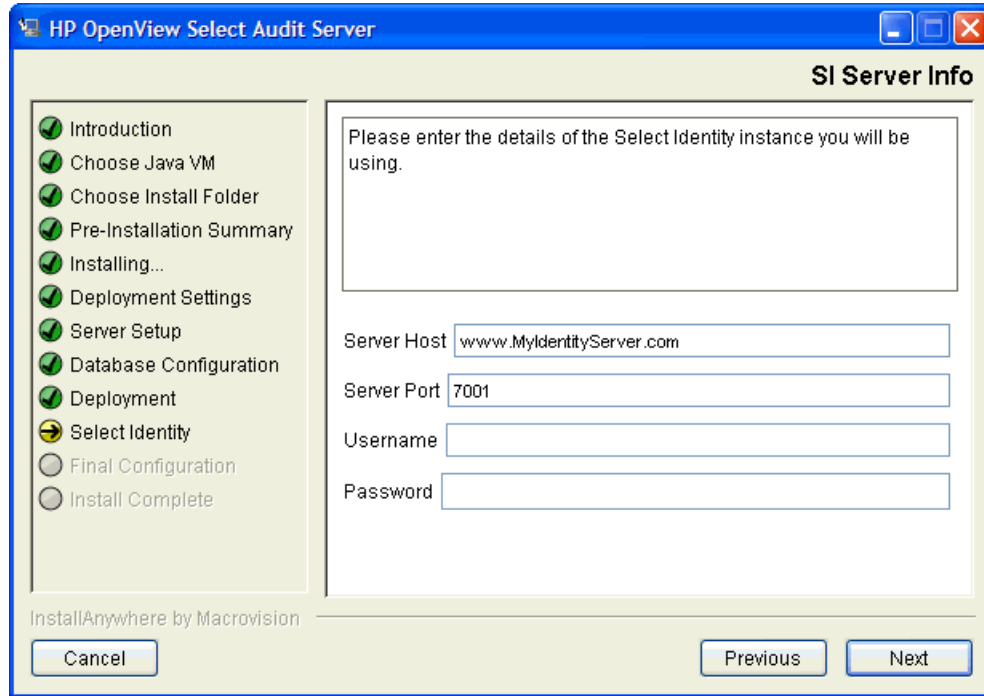


Figure 24 SI Server Info Screen

- 29 Complete the screen as follows:
 - Enter the SI server host name in the **Server Host** field.
 - Enter the SI port number in the **Server Port** field.
 - Enter the SI username in the **Username** field.
 - Enter the SI password in the **Password** field.
- 30 Click **Next**. The **Database Configuration: JDBC Services** screen appears, as shown in [Figure 25](#).

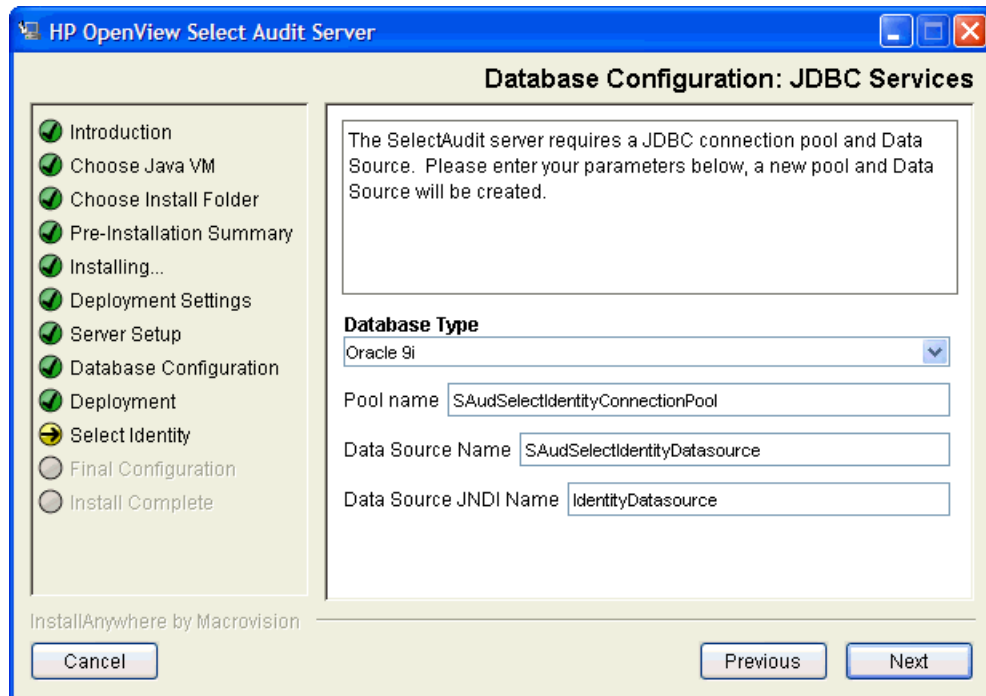


Figure 25 Database Configuration: JDBC Services Screen

- 31 Complete the screen as follows:
 - Select a database type from the **Database Type** drop-down list.
 - Enter the SI connection pool name in the **Pool name** field.
 - Enter the SI data source name in the **Data Source Name** field.
 - Enter the SI JNDI name in the **Data Source JNDI Name** field.
- 32 Click **Next**. The **Database Configuration: Connection Details** screen appears, as shown in [Figure 26](#).

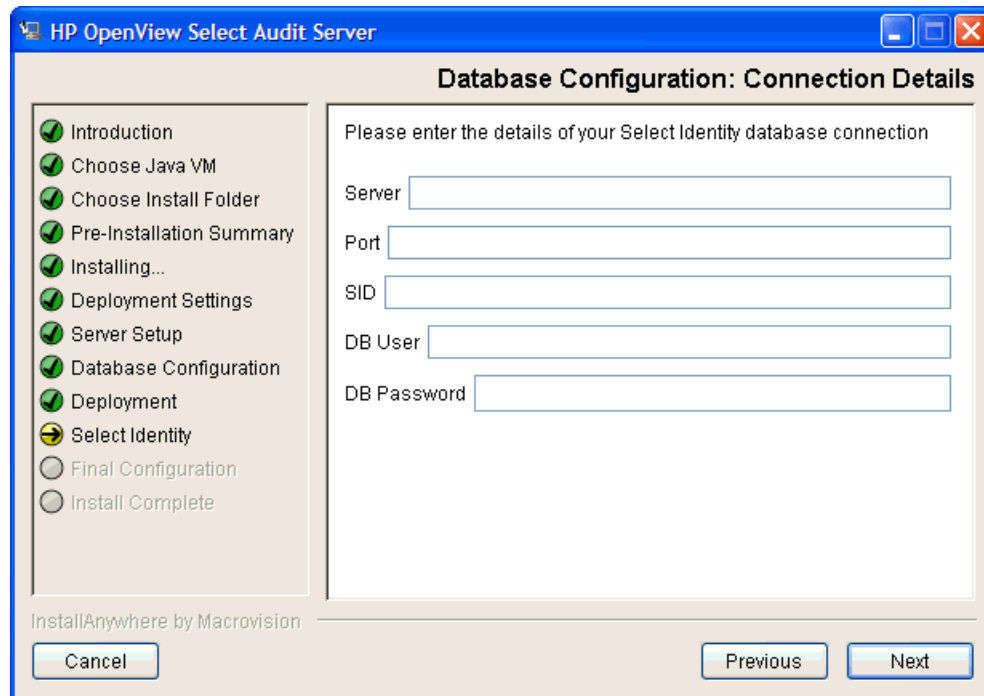


Figure 26 Database Configuration: Connection Details Screen

33 Complete the required information as follows:

- Enter the SI database server address in the **Server** field.
- Enter the SI database listener port number in the **Port** field.
- Enter the SI Oracle database SID in the **SID** field.
- Enter the SI database username in the **DB User** field.
- Enter the SI database password in the **DB Password** field.

▶ If you need to modify the database connection pool or data source information after installation, use the WebLogic console to do so. See [To create or modify database information in the WebLogic console](#) in the *HP OpenView Select Audit 1.01 Administration Guide* for more information.

If you need to turn SI integration off or on after installation, or to modify the integration information, use the Audit Portal **Select Identity Integration** screen. See [To configure Select Identity integration](#) in the *HP OpenView Select Audit 1.01 Administration Guide* for more information.

34 Click **Next**. The **Please Wait** screen appears.

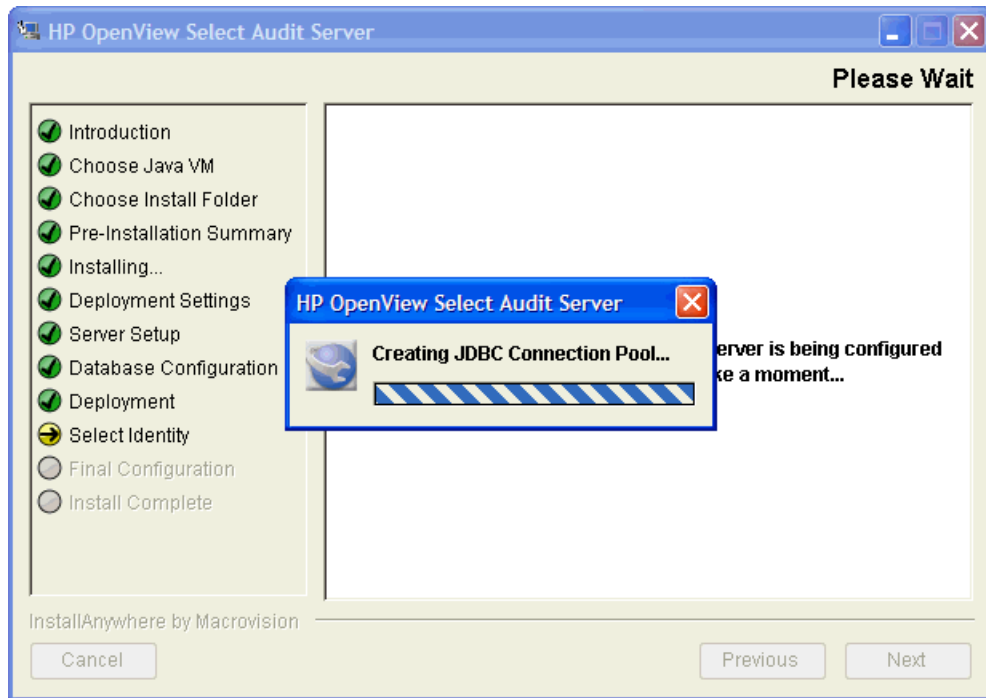


Figure 27 Please Wait Screen

When the installer has created the Select Identity connections, the **Shutdown WebLogic** screen appears, as shown in [Figure 28](#).

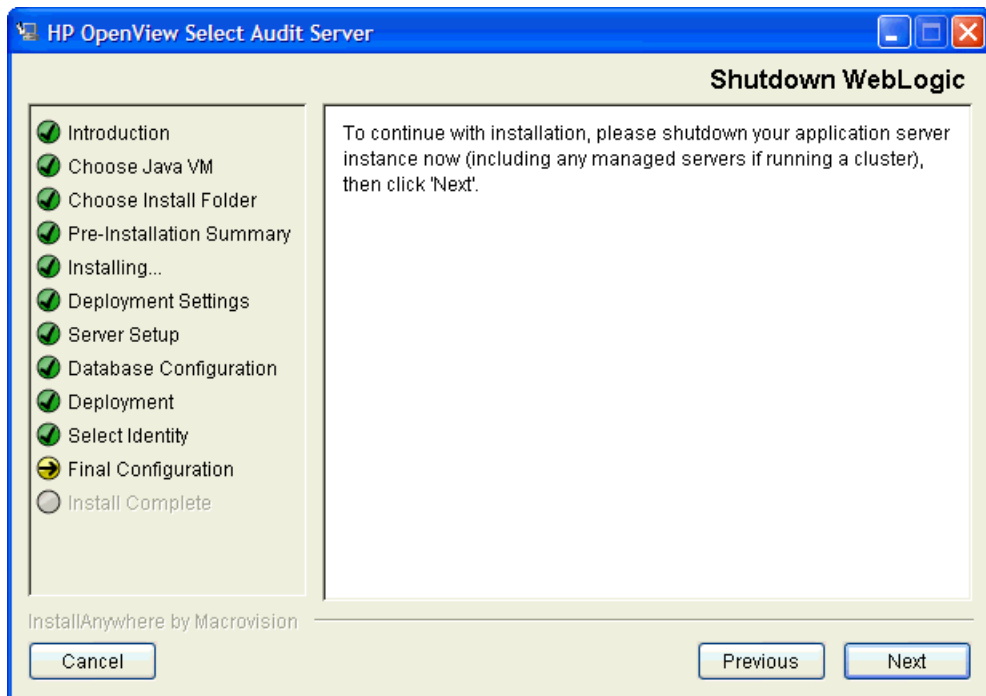


Figure 28 Shutdown WebLogic Screen

35 Stop WebLogic and click **Next**.

- ▶ If you are running a cluster, stop all managed servers first and then stop the Administration server.

The installer then configures the Audit Server. When the installer has configured the Audit Server, the **Start WebLogic** screen appears, as shown in [Figure 29](#).

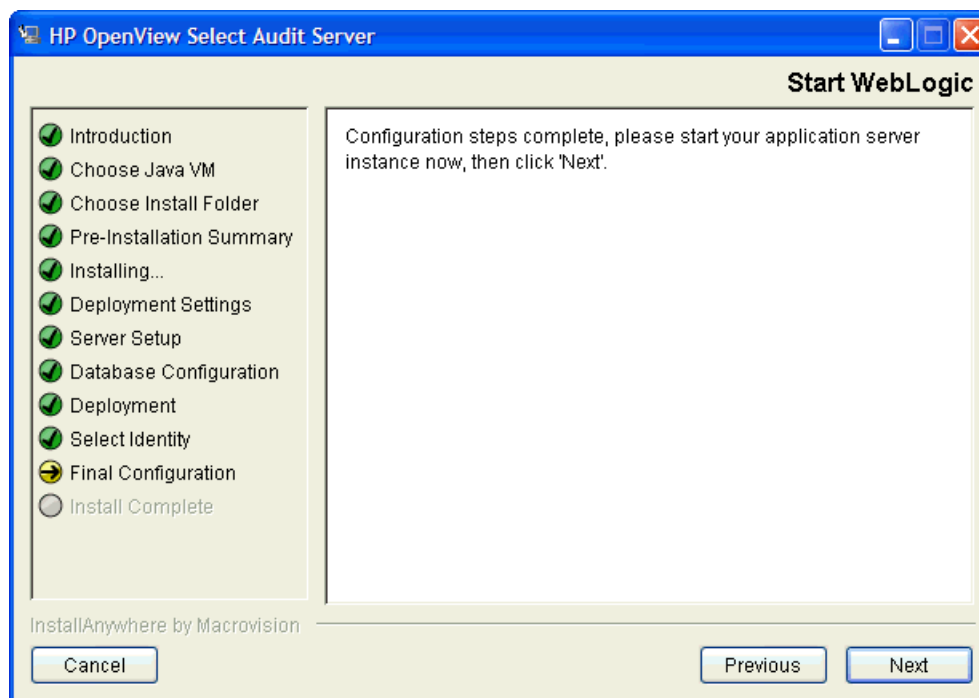


Figure 29 Start WebLogic Screen

For clustered environments

For proper functioning in clustered environments, remote start attributes need to be set for each managed server.

- a Login to the WebLogic console.
- b Expand the servers on the left pane.
- c For each of the managed servers in the cluster, excluding the Administration server instance, do the following:
 - i Click the server name.
 - ii Select the **Configuration** tab in the right pane.
 - iii Select the **Remote Start** sub-tab in the right pane.
 - iv Enter the path to the BEA home.
 - v Enter the following in the **Arguments** field to register the WebLogic JAAS login module with the Java VM running the managed server:

```
 ${REPORT_SEC} ${HEADLESS_OPT} ${MEM_ARGS}
```

These three parameters can be derived from the `startWebLogic` script on the WebLogic Administration server that starts the cluster domain.
- d Specify an appropriate classpath that includes both Select Audit and WebLogic require jar files. The appropriate classpath may be derived from the `startWeblogic` start script for the WebLogic domain.

- e Change the `vde.ac1check` parameter to 0 (the default is 1) in the `$WL_HOME/common/nodemanager/<server name>/ldap/conf/vde.prop` file on each of the managed server machines.
 - f Restart all managed server instances.
 - g Login to the Report Center to validate successful authentication.
- 36 Start WebLogic and click **Next** once the server has restarted.
- ▶ If you are running a cluster, start the Administration server first and then all managed servers.

The Please Wait screen appears while the installer performs the final Audit Server configuration.

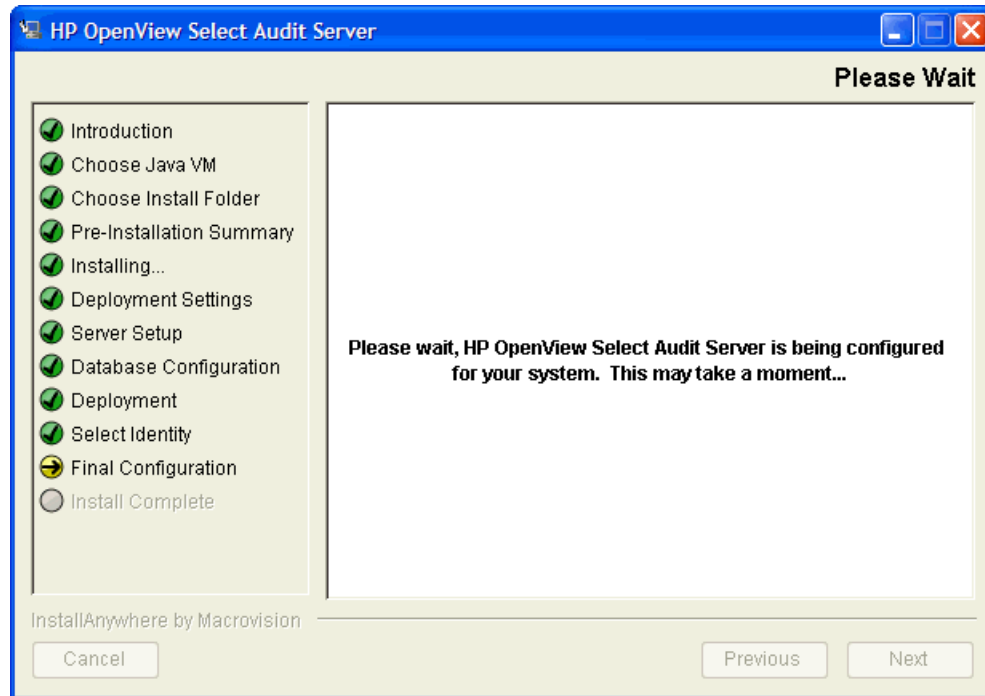


Figure 30 Please Wait Screen

When the installer has configured the Audit Server, the **Install Complete** screen appears.

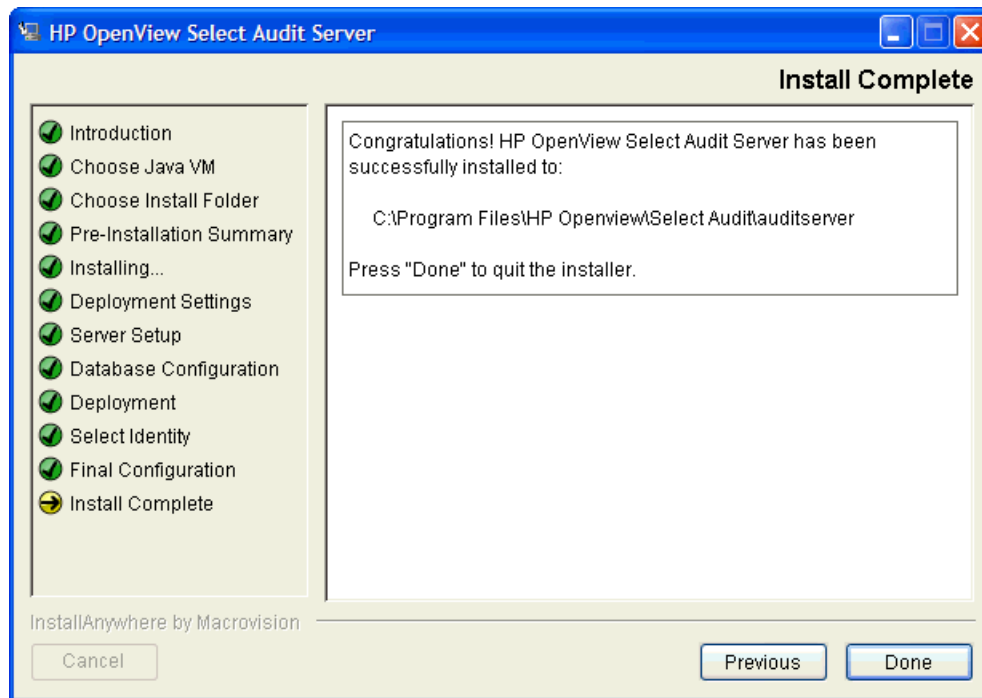


Figure 31 Install Complete Screen

- 37 Click **Done** to complete the installation of the Audit Server. The installer then cleans up all temporary installation files.

When the server installation has completed, the Audit Server administration UI is available at `http://<server>:<port>/auditportal`.



Redeploying the Audit Server when it is already deployed can cause problems with the data signature. You must undeploy the Audit Server, restart WebLogic (or the cluster), and then deploy the Audit Server again. This is because the Normalizer threads started by the undeployed instance of the Audit Server are still running, there is more than one instance of the signer, and the old instance of the signer may corrupt the signature of the data signed by the new instance of Audit Server.

Post-Installation Steps

Once the Audit Server installer is finished, there are some post-installation steps required. These are described below.

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 descendants 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

```

Redirecting WebLogic Server Output

You may optionally redirect logging on the WebLogic server by configuring log4J.

- 1 Add the following code before `JAVA_OPTIONS` in `startWebLogic.sh` or `startWebLogic.cmd`:

```

REDIRECT_OUT=-Dweblogic.Stdout="myserver/stdout.log"
REDIRECT_ERR=-Dweblogic.Stderr="myserver/stderr.log"

```



You can name your log files any name you want.

- 2 Add the following to `JAVA_OPTIONS`:

- For UNIX:
Add `${REDIRECT_OUT}` and `${REDIRECT_ERR}`.
- For Windows:
Add `%REDIRECT_OUT%` and `%REDIRECT_ERR%`.

Adding Users to WebLogic Roles

The Select Audit installers create global roles and the corresponding associated groups in WebLogic. After you have installed Select Audit, you must use the WebLogic console to create your users and add them to the associated groups (Select Audit Administrators, Select Audit Users, and Select Audit Auditors) before those users can log in to Select Audit. There is an additional group, just for the Jasper developers, `SelectAuditReportDevelopers`. This group is used to give additional rights to regular users who are also Jasper developers. Jasper developers have access to the Jasper Developer Center and error output.

To add users

- 1 Open the WebLogic console.
- 2 Click `Security/Realms/myrealm` in the left console pane.
- 3 Add new users for users with auditor and user functions by doing the following:
 - a Click **Users** → **Configure a new User** to add a user.
 - b Enter the user information and click **Apply**.
 - c Click the **Groups** tab.
 - d Select the group you want to associate the user with and click the arrow to move the group to **Current Groups**.
 - e Click **Apply**.

Configuring a Mail Session in WebLogic

The Audit Server installer uses a default return address on the **Report Notification** screen. If you accept the default setting in the installer, an exception will be thrown by the SMTP server when it tries to send a message that has in the default value `select-audit-workflow@localhost` in the **From** field. You must change this setting in the WebLogic console if you did not configure it in the installer.

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 `mail.TruAccess` for the JNDI.
- 5 Enter the properties for the mail session.
- 6 Click **Apply**.

Setting a Default Time Zone for Database Connection Pools

If you are using Oracle 9i and BEA WebLogic Sever 8.1 SP5, a default time zone has to be setup on each database connection pool used by Select Audit. This configuration has to be done right after installation and before sending any audit message to Select Audit. The default time zone has to be set to be the as same as your WebLogic server time zone.

To setup the default time zone

- 1 Login as a WebLogic administrator in the WebLogic Server console.
- 2 In the left pane, expand the **Services** node.
- 3 Expand **JDBC/Connection Pools**.
- 4 Click **SelectAuditConnectionPool**.
- 5 In the right pane, click the **Connections** tab.
- 6 Click the **Show** link near the bottom of the page and expand the **Advanced Options** section.
- 7 Enter `SQL ALTER SESSION SET TIME_ZONE = '<your time zone>'` in the **Init SQL** field. Replace the `<your time zone>` with your default time zone name. For example EST, GMT, etc. For information about all valid time zone name, please refer to Oracle documentation.
- 8 Click **Apply**.
- 9 Click **SelectAuditReportPool** in left pane and repeat [Step 5](#) to [Step 8](#).
- 10 If there is a **SAudSelectIdentityConnectionPool** node in left pane, select it and repeat [Step 5](#) to [Step 8](#).
 - ▶ This connection pool is listed if you enabled Select Identity integration during Select Audit installation.
- 11 Restart the WebLogic server.

Configuring UTF-8 Fonts in PDF Channel Reports

In order to view international text in PDF channel reports, you must configure the Report server to send an appropriate font in the PDF file. The following procedure is an example of how to do this in a Windows XP environment.

- 1 Create TrueType Font Metrics.
 - a Locate a suitable TTF font file, e.g `C:\WINDOWS\Fonts\ArialUni.ttf`.
 - b Create a new folder, e.g. `c:\fop` and `cd` into it.
 - c Create a metrics file in Windows from the TrueType font. The following example will create `ttfarialuni.xml` in `c:\fop`.

```
SET SAUD_INSTALL_DIR=Your Select Audit install folder
SET LIB_DIR=%SAUD_INSTALL_DIR%\dist\reporting\ReportServer\WEB-INF\lib
java -cp
%LIB_DIR%\fop.jar;lib\avalon-framework.jar;%LIB_DIR%\xml-apis.jar;
%LIB_DIR%\xercesImpl.jar;lib\xalan.jar org.apache.fop.fonts.
apps.TTFReader C:\WINDOWS\Fonts\ArialUni.ttf ttfarialuni.xml
```

2 Register the fonts with FOP.

- a Create a new file in `c:\fop` and call it `userconfig.xml`.
- b Add the following content to the file:

```
<!-- <!DOCTYPE configuration SYSTEM "config.dtd"> -->
<configuration>
  <entry>
    <key>fontBaseDir</key>
    <value>C:\fop</value>
  </entry>
  <font>
    <font metrics-file="ttfarialuni.xml"
    embed-file="C:\WINDOWS\Fonts\ArialUni.ttf" kerning="yes">
      <font-triplet name="ArialUni" style="normal" weight="normal" />
      <font-triplet name="ArialUni" style="normal" weight="bold" />
      <font-triplet name="ArialUni" style="italic" weight="normal" />
      <font-triplet name="ArialUni" style="italic" weight="bold" />
    </font>
  </font>
</configuration>
```

- ▶ Since the configuration file is XML, be sure to keep it well-formed. In font-triplets, “ArialUni” is the name of the font. You can call it anything you want. Just make sure that you are consistent.

3 Modify `defaultscope.xml` by editing the properties `fopConfigFile` and `fopFont`.

- ▶ The `defaultscope.xml` file is located at
`%SAUD_INSTALL_DIR%\dist\reporting\ReportServer\WEB-INF\conf`.

- a For `fopConfigFile`, enter the location of your config file created in Register Fonts with FOP, e.g:

```
<Property name="fopConfigFile">C:\\fop\\userconfig.xml</Property>
```
- b For `fopFont`, enter the name of the font you specified in that config file, e.g:

- ▶ The name is case-sensitive and it must match the case specified in the config file.

```
<Property name="fopFont">ArialUni</Property>
```

At this point, this font will be embedded into every PDF file generated by the server.

- ▶ `ArialUni.ttf` is used as an example. Make sure you have the distribution rights for the font you use.

Running the Audit Connector Installer

The Connector installer takes you through the following steps for installing and deploying the Audit Connector:

- entering Audit Connector installation information
- configuring the Audit Connector
- authenticating the Audit Connector

Select Application Configuration Requirements

The Select applications have specific configuration requirements in order to log to Select Audit. Unless the applications are configured properly, they will not log to Select Audit. Refer to the specific *HP OpenView Select** documentation for more information about configuring Select* applications.

Select Audit Connector Installer Mode Overview

HP allows you to run the Select Audit Connector installer in three modes: Default or GUI mode, Console interactive mode (on UNIX only), and Silent mode.

Table 4 Available Installation Modes

Mode	Description
Default	Graphical User Interface with wizard panels and dialog boxes.
Console	For remote installations over Telnet, or on systems without a graphical windowing environment. Also known as Command Line Interface.
Silent	These installers do not interact with the user at all and are suitable for distribution when all of the settings are already known or provided in a Response file.

The GUI mode is used for normal installations. Console mode can be used for installing many connectors on different machines. If you are installing Select Audit on a UNIX host, Console mode is particularly useful to UNIX end users who do not have X-Windows or VNC running on their system. Default settings can be specified.

Running the Connector Installer in Default Mode

- 1 Start the Select Audit setup program by running the corresponding setup file from the root of the Select Audit product CD:

- On Windows:

Double-click `SelectAuditConnectorInstall.exe`.



If you are uninstalling and/or installing, or configuring Select Audit components on a Windows host computer, ensure that you do not have the Services window or any other Control Panel application open. This open Control Panel application triggers conflicts that can cause the installer to behave abnormally.

OR

- On UNIX:

Enter the following command: `./SelectAuditConnectorInstall.bin`.



You should be logged in using the same user that WebLogic is running on to install the Audit Server or Audit Connector.

The installer extracts the installation files, then prepares the Select Audit Connector Install wizard. When it has finished loading, the **Introduction** screen appears, as shown in [Figure 32](#).

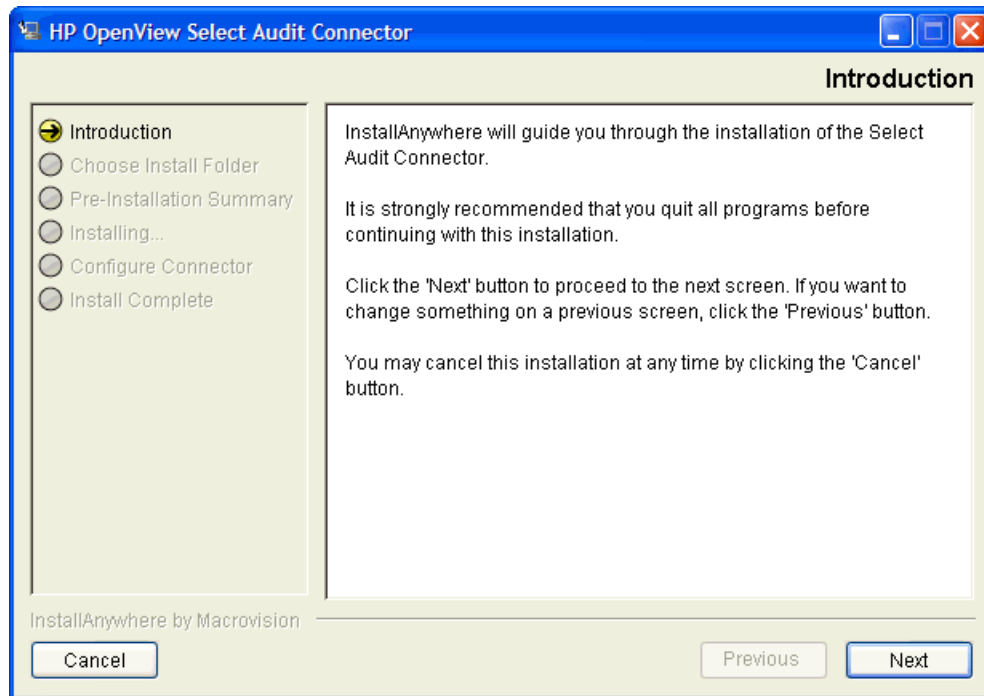


Figure 32 Introduction Screen

- 2 Click **Next**. The **Choose Install Folder** screen appears, as shown in [Figure 33](#).

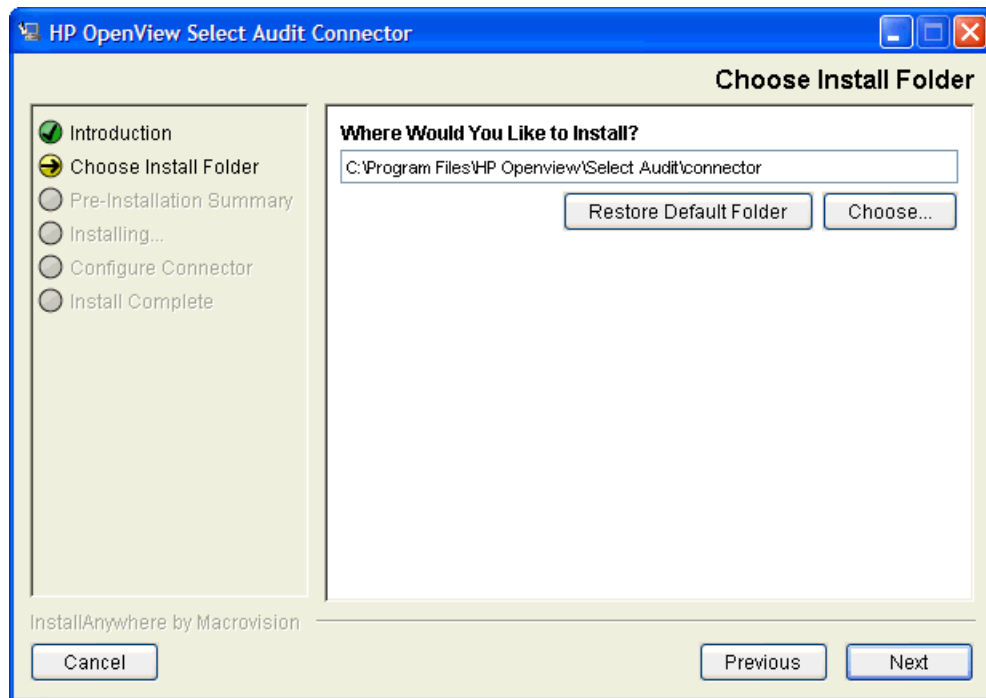


Figure 33 Choose Install Screen

- 3 Do one of the following:
 - If the default location is acceptable, proceed to [Step 4](#).
 - If you want to select a different installation folder, click **Choose**, select a folder, then click **OK**. The new folder appears in the **Where would you like to install Select Audit?** field.
 - If you choose the wrong folder, click **Restore Default** to restore the Select Audit defaults.
 - The following characters are not valid in file or folder names when specifying where to install the Audit Connector:
 () { } [] / \ : ; " ' < > | \$ * ? # & ,
- 4 Click **Next**. The **Log Directory** screen appears, as shown in [Figure 34](#). The Log Directory is where audit event logs are temporarily stored before being sent to the server.

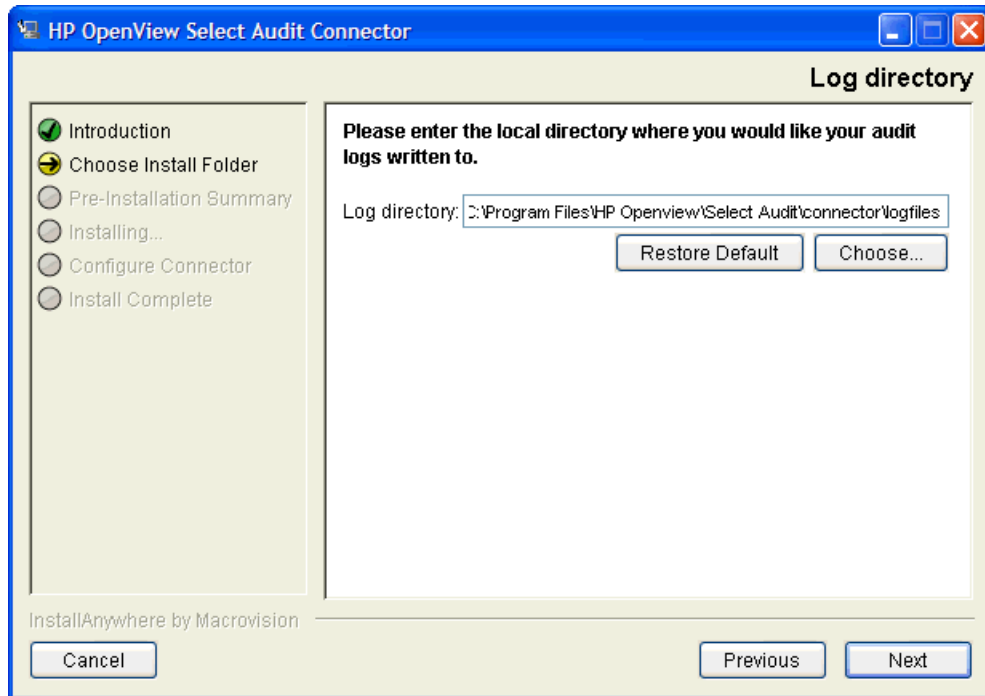


Figure 34 Log Directory Screen

- 5 Select the local directory that you want to write audit logs to and click **Next**. The **Pre-Installation Summary** screen appears, as shown in [Figure 35](#).

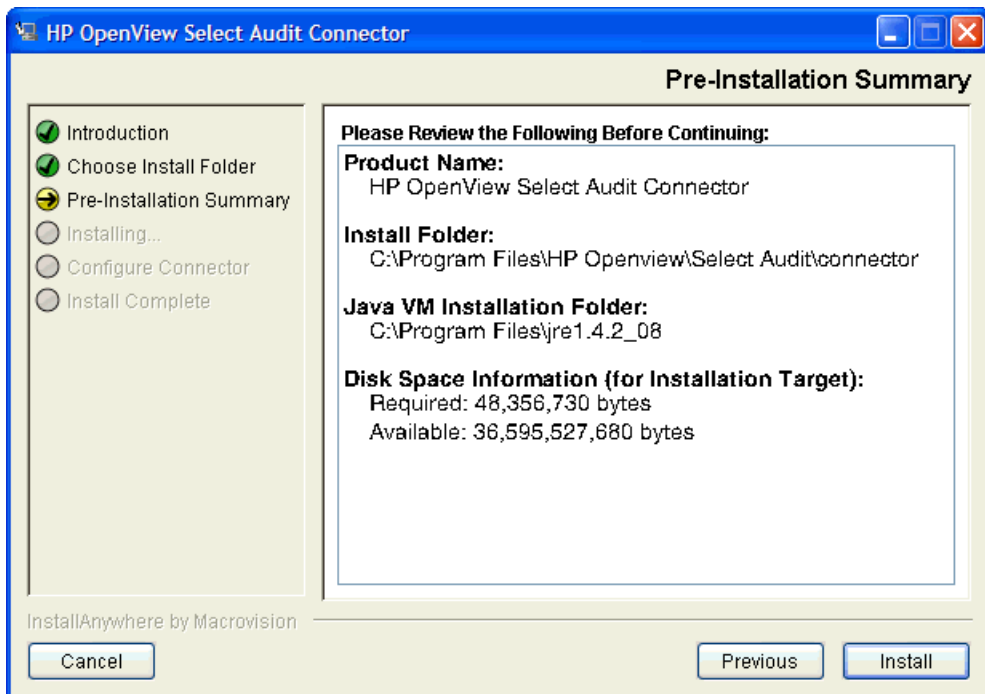


Figure 35 Pre-Installation Summary Screen

The **Pre-Installation Summary** screen creates a digest of the following installation information you provided to this point:

- The installation and shortcut folders you chose to install the Audit Connector in.
 - The installation location of the Java Virtual Machine that the Select Audit Install wizard has automatically installed. The Java Virtual Machine is required to run both the maintenance program as well as Select Audit components.
 - The amount of disk space required for the components you selected to install. If the disk space required exceeds what is available on this computer, free up space or adjust what you are currently intending to install.
- 6 Review the information on the **Pre-Installation Summary** screen. If the information is correct, click **Install**.
- To change any of the installation settings, click **Previous** to return to the screen containing the settings you want to change.

The Audit Connector begins to install and the **Connector Installation** screen appears, as shown in [Figure 36](#).



Figure 36 Connector Installation Screen

When the Connector installer is finished, the **Configure Connector** screen appears, as shown in [Figure 37](#).

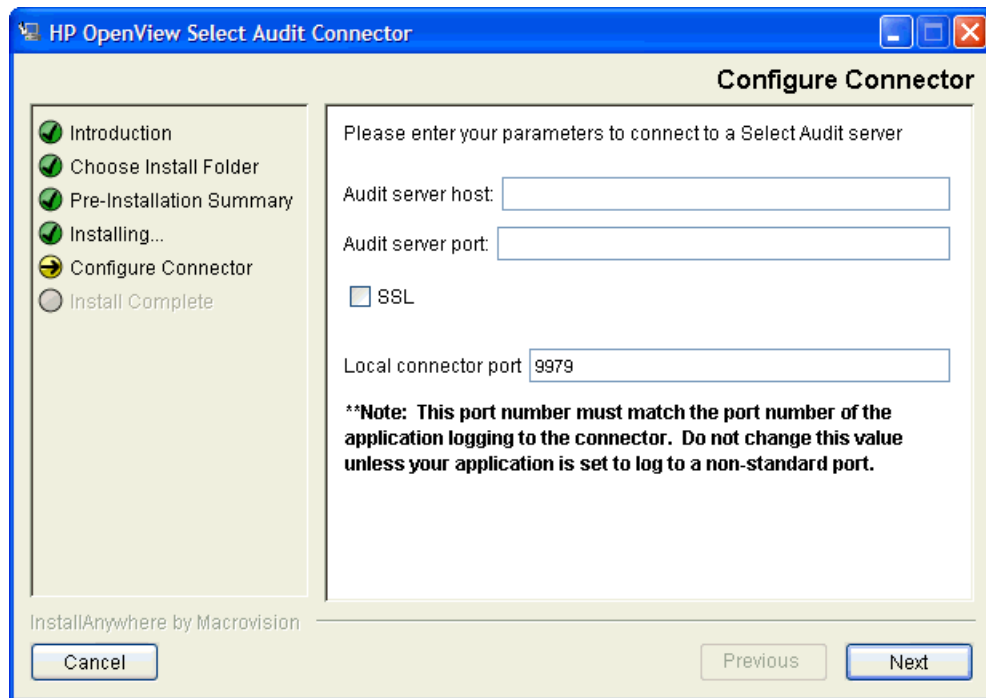



Figure 37 Configure Connector Screen

- 7 On the **Configure Connector** screen, do one of the following:
 - Accept the default values.
 - Customize your configuration:
 - Enter the server hostname in the **Audit server host** field.
 - Enter the server port number in the **Audit server port** field.
 - Enter the port number of the application logging to the Audit Connector in the **Local connector port** field.
-  The port number must match the port number of the application logging to the connector. Do not change the port number unless your application is set to log to a non-standard port.
- 8 If you want to use an SSL connection, select the **SSL** check box.
 - ▶ SSL must also be turned on in the Audit Server if you use it in the Audit Connector.
 - 9 Click **Next**. If you are not using SSL the **Connector Authentication** screen appears, as shown in [Figure 38](#).

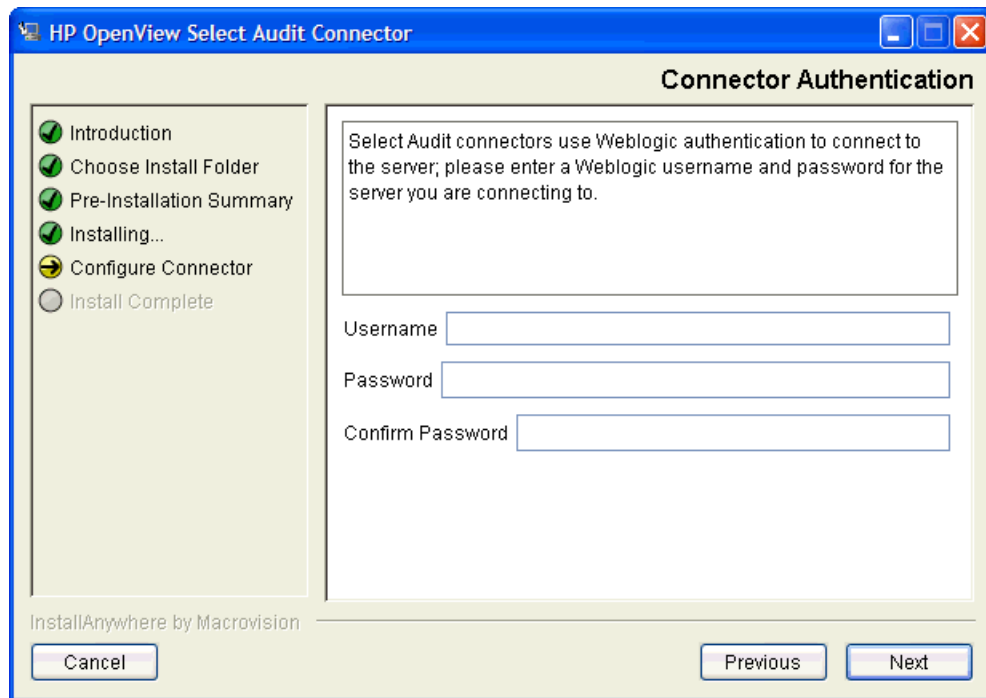


Figure 38 Connector Authentication Screen

If you are using SSL the **SLL Connector Authentication** screen appears, as shown in Figure 39.

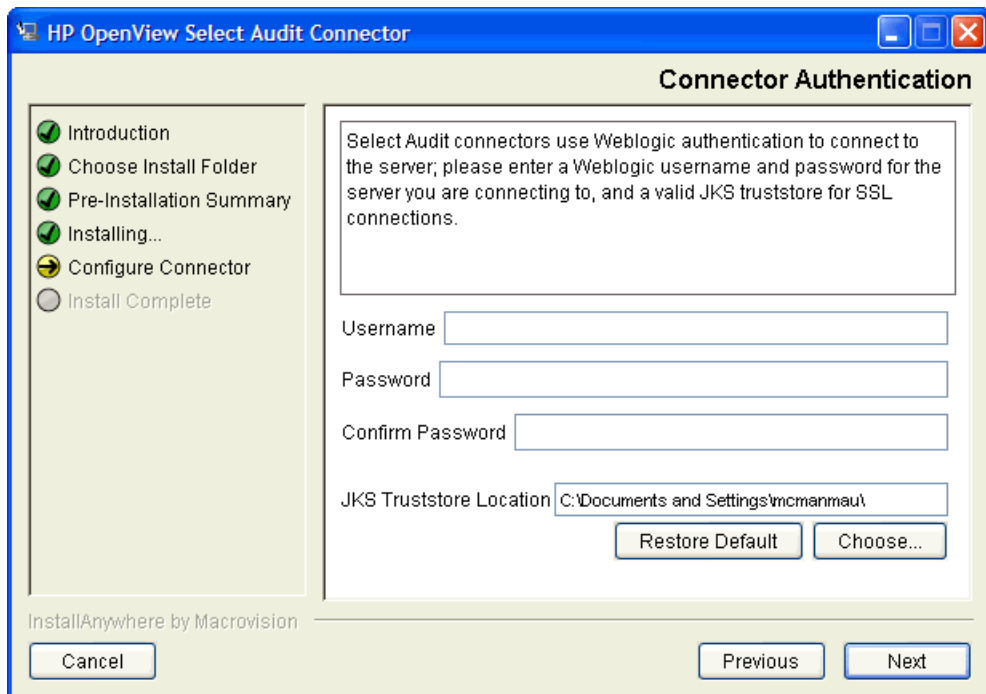


Figure 39 SSL Connector Authentication Screen

- 10 Enter the **Username** and **Password** required to authenticate to the Audit Server. Re-enter the password in the **Confirm Password** field.

The username and password are the credentials of a WebLogic user in the **Administrators** group. These credentials must be predefined on the WebLogic server before the Connector installation is attempted.

- For SSL connections, click **Choose** to select the location of a valid JKS Truststore in the **JKS Truststore Location** field.

11 Click **Next**. The **Please Wait** screen appears.

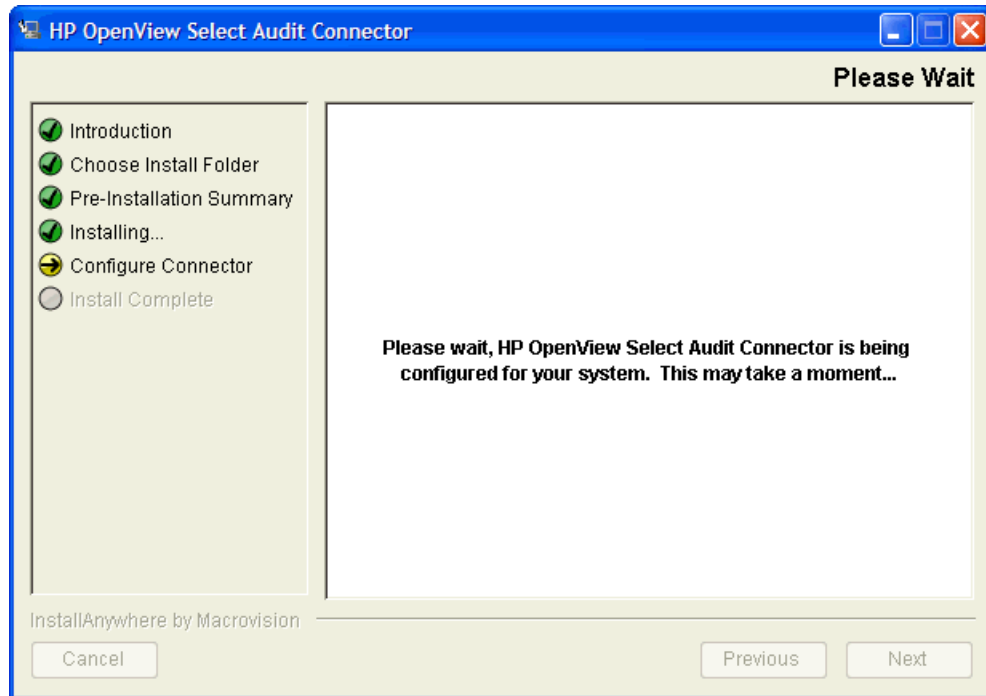


Figure 40 Please Wait Screen

When the Audit Connector has been configured, the **Install Complete** screen appears, as shown in [Figure 41](#).

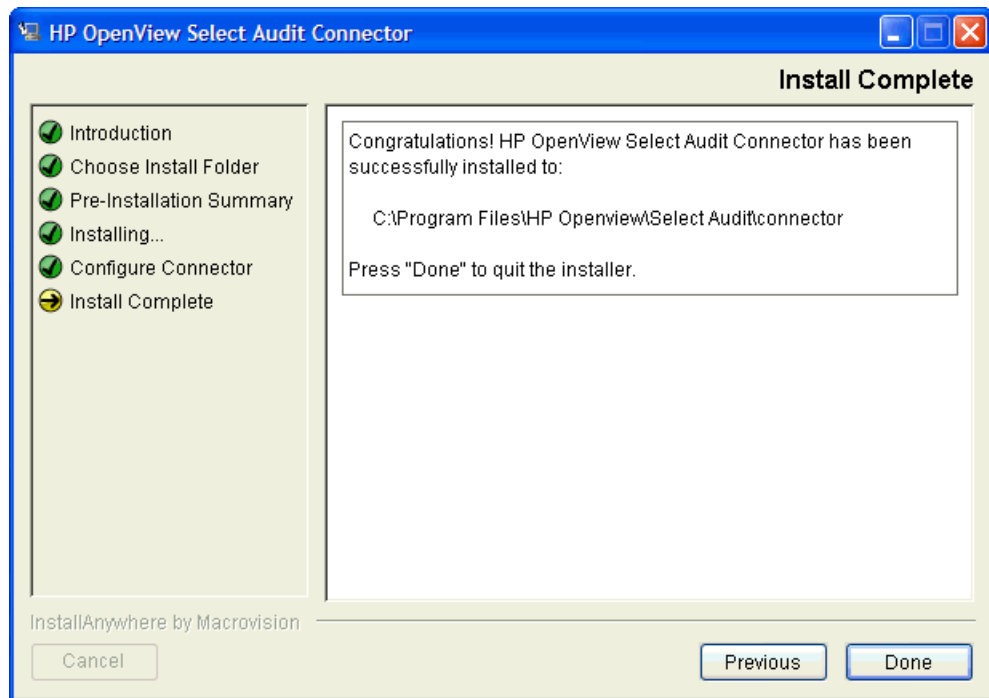



Figure 41 Install Complete Screen

- 12 Click **Done** to close the installer. The Audit Connector is now installed.

For Windows installations, the installer:

- Creates the Audit Connector's local configuration file `connector.props` in your installation directory root. (See [Chapter 3, Configuring Select Audit](#) in the *HP OpenView Select Audit 1.01 Administration Guide* for more information.) Once the Audit Connector has been started, it registers with the Audit Server, and downloads the default connector configuration values from the server's configuration module. If these values are different than the values configured by the Connector installer, they will be saved in local file, `connector.properties`. The values in `connector.properties` **overwrite** those in `connector.props`.

 Do not manually edit the `connector.props` file.

- Cleans up all temporary installation files.



On Windows platforms, the Connector installer always installs the Audit Connector as a service called `HP Select Audit Connector` and starts it automatically.

On UNIX platforms, a startup script is created with the name `SAudConn` in the `opt/ov/SelectAudit/connector` directory. It can be run with the options `start`, `stop` and `restart`.

Running the Connector Installer in Console Mode

The installer can run in an interactive, text-only mode.

- 1 From either the command line or command shell, change directories to your CD drive.
- 2 At the Command Prompt, run the following Console command line argument:

```
SelectAuditConnectorInstall.exe -i console
```

`-i console` tells the installer to run in Console mode.

▶ For UNIX, run installers using the same user that WebLogic is running on. This allows the installer to set up all the required symbolic links. These links are removed when you uninstall all or part of Select Audit.

3 Define Select Audit's installation folder by doing one of the following:

- Typing the *absolute* path to the folder you wish to use.

OR

- Pressing **Enter** to accept Select Audit's default folder. The default install path is:

```
/opt/OV/SelectAudit/connector
```

4 The installer gives you a pre-installation summary for the components you defined. This summary provides a digest of the following installation information:

- The install path of Select Audit.
- The installation location of the Java Virtual Machine that the Select Audit Installation wizard has automatically installed. The Java Virtual Machine is required to run both the maintenance program as well as Select Audit components.
- The amount of disk space that is required for the components you selected to install. If the disk space required exceeds what is available on this computer, free up space or adjust what you are currently intending to install.

5 If this information is correct, press **Enter** to continue installing these components. If the information is not correct, type **back** to redefine which components you want to install.

6 Configure the host, port, username and password.

7 When the installer is finished, an Installation Complete message appears. Click **Enter** to exit the installer.

Running the Connector Installer in Silent Mode

1 Before running the installer, create the file `installpropertiesfile.txt` in the folder where the installer runs from.

The `installpropertiesfile.txt` file includes:

```
INSTALLER_UI=silent
USER_INSTALL_DIR=C:\\Program Files\\HP Openview\\Select
Audit\\connector
CONN_LOGFILE=$USER_INSTALL_DIR$\\connector\\logfiles\\log.out
CONN_USERNAME=
CONN_PASS=
CONN_PASS2=
CONN_PORT=9979
SERVER_PROTOCOL=http
SERVER_HOST=
SERVER_PORT=7001
SSL=0
```

2 From either the command line or command shell, change directories to the folder where the installer runs from.

- 3 At the Command Prompt, run the following Console command line argument:
`SelectAuditConnectorInstall.exe -f installpropertiesfile.txt`

Uninstalling the Audit Server

Audit Server uninstaller executables are created on the machine where the Audit Server is installed during the Server installation. After installing the Audit Server on Windows, there is an `Uninstall_Select_Audit` folder under the `C:\Program Files\HP OpenView\Select Audit` directory. This folder contains the uninstaller executable `Uninstall_Select_Audit.exe`.



If you are uninstalling and/or installing, or configuring Select Audit components on a Windows host computer, ensure that you do not have the Services window or any other Control Panel application open. This open Control Panel application triggers conflicts that can cause the installer to behave abnormally.

On HP-UX and Linux, under the server installation directory `/opt/OV/SelectAudit`, there is a `Uninstall_Server` directory that contains the `Uninstall_Select_Audit` binary.

To uninstall the Audit Server on Windows

- 1 Double-click `Uninstall_Select_Audit.exe` under the `C:\Program Files\HP OpenView\Select Audit\auditserver\Uninstall_Select_Audit` directory. The **Select Audit Uninstall Introduction** screen appears, as shown in [Figure 42](#).

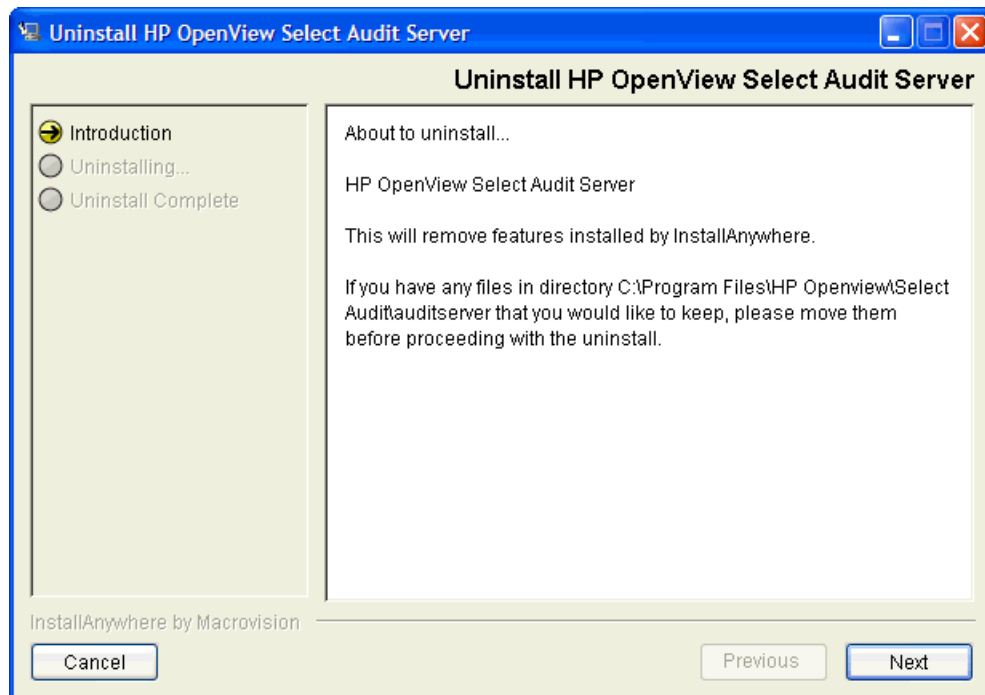


Figure 42 Server Uninstall Introduction Screen

- 2 Click **Next**. The **WebLogic Authentication** screen appears, as shown in [Figure 43](#).

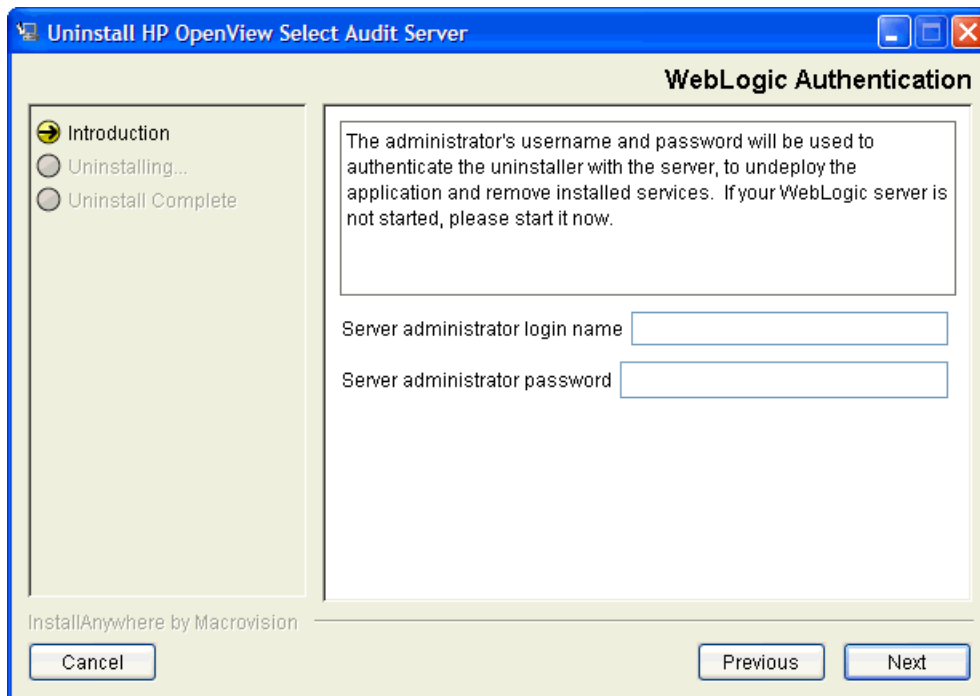


Figure 43 WebLogic Authentication Screen

- 3 Enter the **Server administrator login name** and **Server administrator password** in the corresponding fields.
 - ▶ The WebLogic server must be running to properly uninstall Select Audit.
- 4 Click **Next**. The **Start WebLogic** screen appears, as shown in [Figure 44](#).

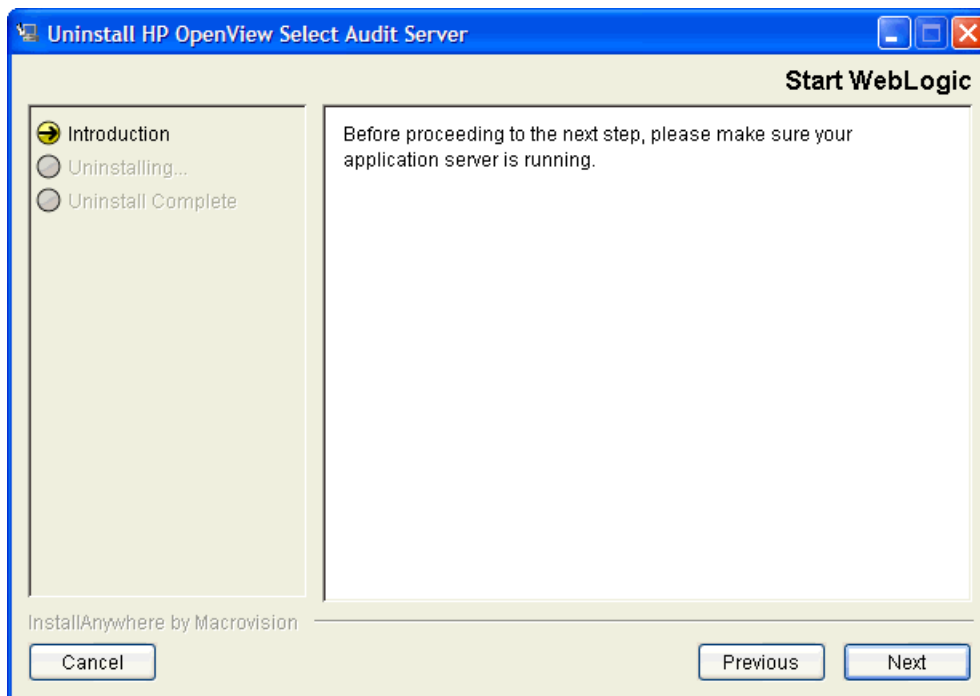


Figure 44 Start WebLogic Screen

- 5 Start WebLogic and click **Next** once the server has started.
 - ▶ If you are running a cluster, start the Administration server first and then all managed servers.

The **Please Wait** screen appears while uninstaller contacts WebLogic, deploys the database schema and configures Select Audit, as shown in [Figure 45](#).

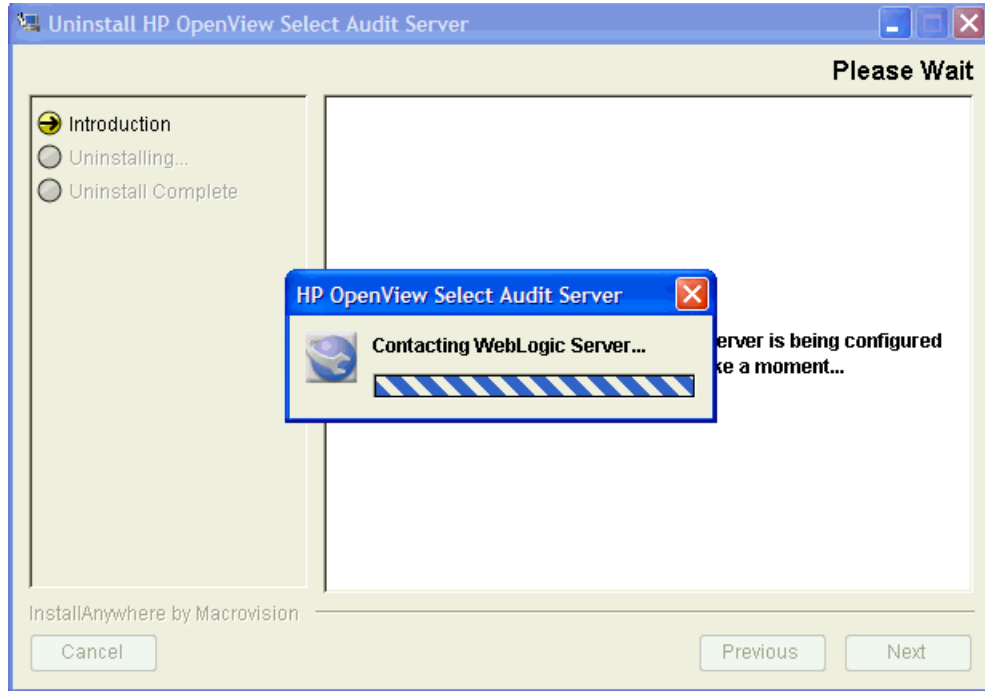


Figure 45 Please Wait Screen

On completion, the **Shutdown WebLogic** screen appears, as shown in [Figure 46](#).

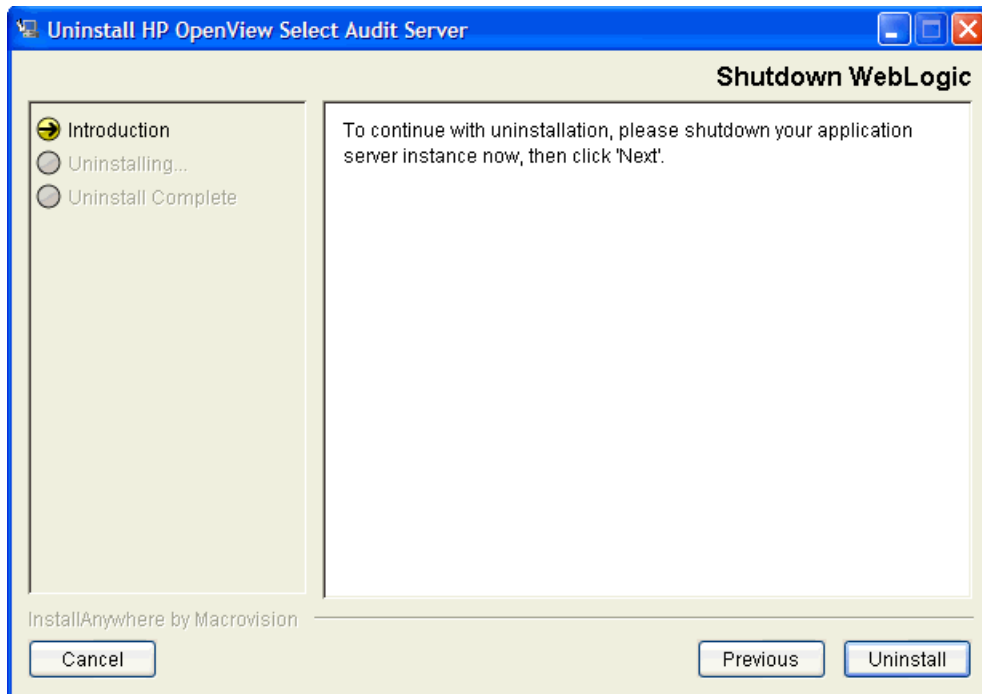


Figure 46 Shutdown WebLogic Screen

- 6 Stop WebLogic and click **Uninstall**. The **Uninstall HP OpenView Select Audit Server** screen appears as shown in [Figure 47](#).

▶ If you are running a cluster, stop all managed servers first and then stop the Administration server.

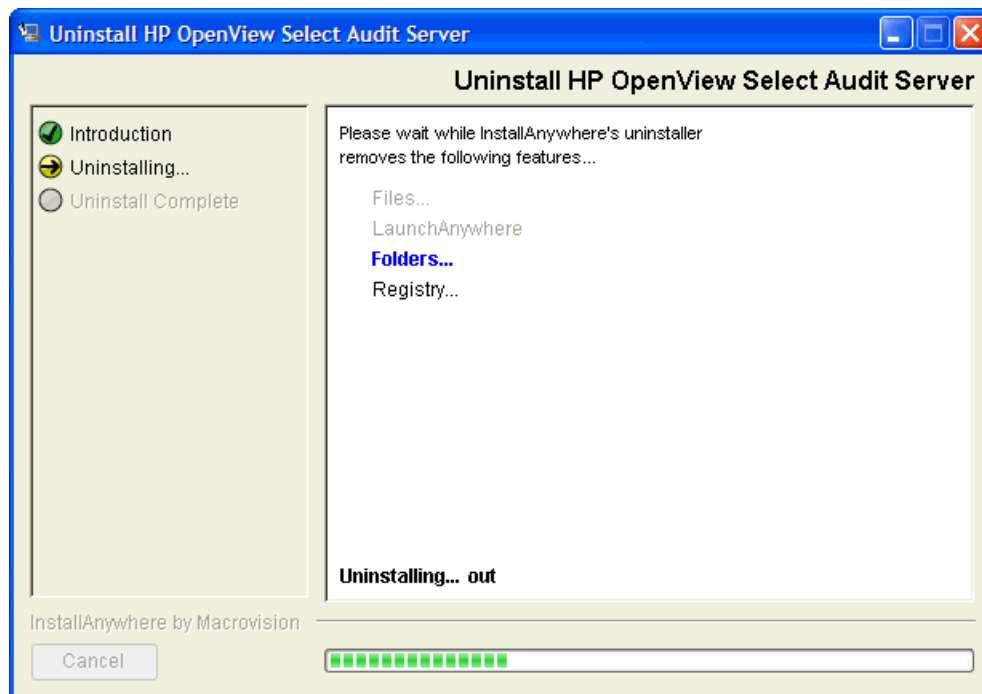


Figure 47 Uninstall HP OpenView Select Audit Server Screen

The uninstaller removes the Select Audit features. When the Audit Server is uninstalled, the **Uninstall Complete** screen appears, as shown in [Figure 48](#).

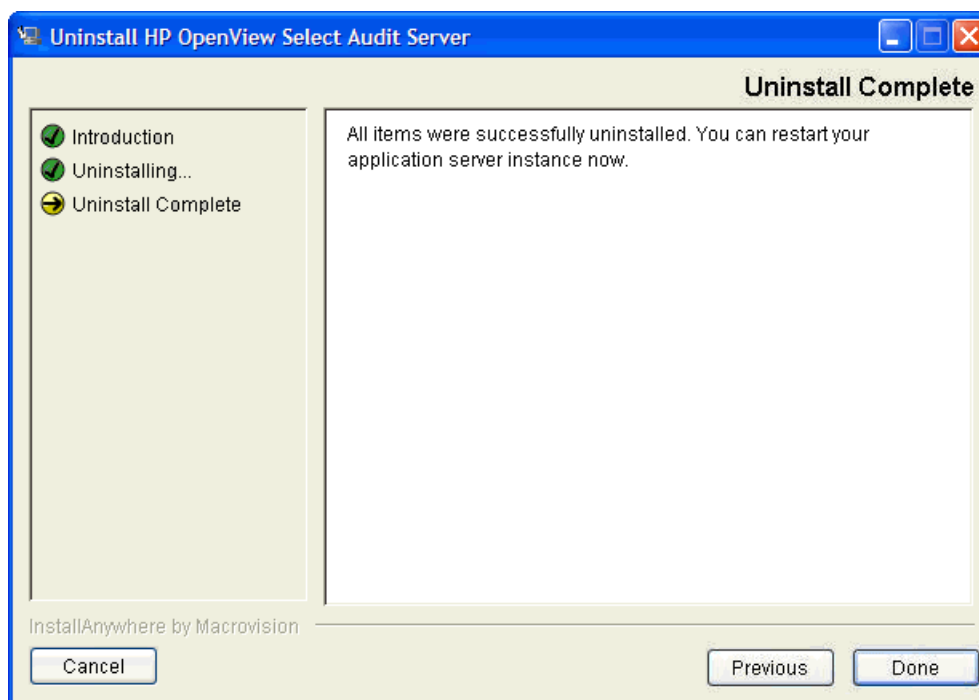


Figure 48 Server Uninstall Complete Screen

- 7 Click **Done** to exit the uninstaller.
 - ▶ The uninstaller does not remove any files or folders created after you installed Select Audit. You must remove these manually.

Uninstalling the Audit Connector

Audit Connector uninstaller executables are created on the machine where the Audit Connector is installed during the Connector installation. After installing the Audit Connector on Windows, there is an `Uninstall_Connector` folder under `C:\Program Files\HP OpenView\Select Audit` directory. This folder contains the uninstaller executable `Uninstall_Connector.exe`.

- ⚠ If you are uninstalling and/or installing, or configuring Select Audit components on a Windows host computer, ensure that you do not have the Services window or any other Control Panel application open. This open Control Panel application triggers conflicts that can cause the installer to behave abnormally.

On Linux, under the connector installation directory `/opt/OV/SelectAudit/connector`, there is a `Uninstall_Connector` directory that contains the `Uninstall_Connector` binary.

To uninstall the Audit Connector

- 1 Double-click `Uninstall_Connector.exe` under the `C:\Program Files\HP OpenView>Select Audit\connector\Uninstall_Connector` directory. The **Uninstall Select Audit Connector Introduction** screen appears, as shown in [Figure 49](#).

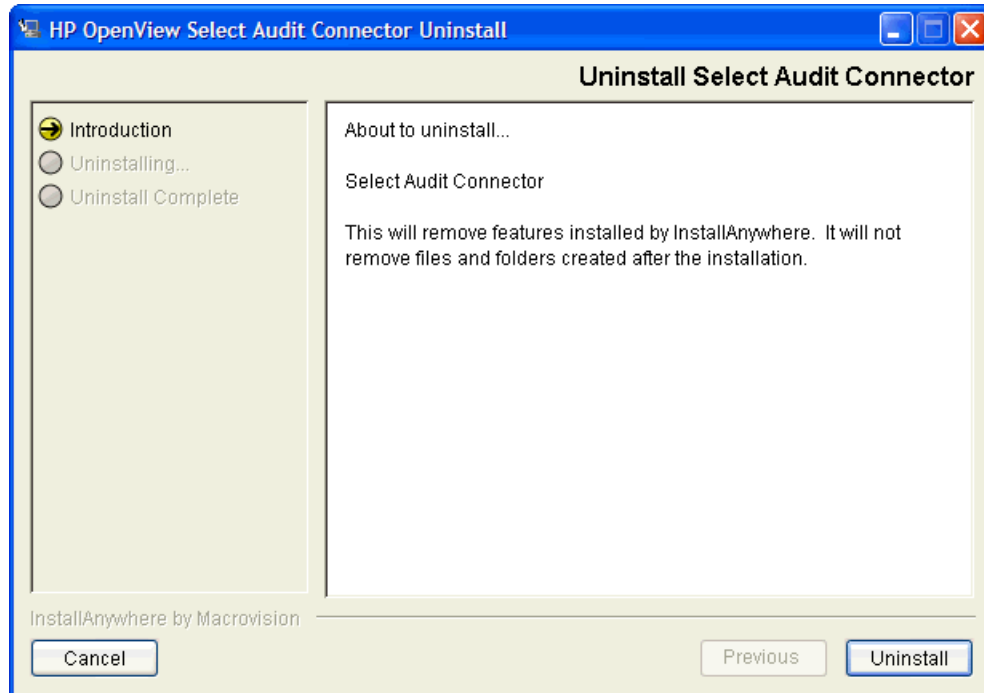


Figure 49 Uninstall Select Audit Connector Introduction Screen

- 2 Click **Uninstall**. The **Uninstall Select Audit Connector** screen appears, listing the features being uninstalled, as shown in [Figure 50](#).

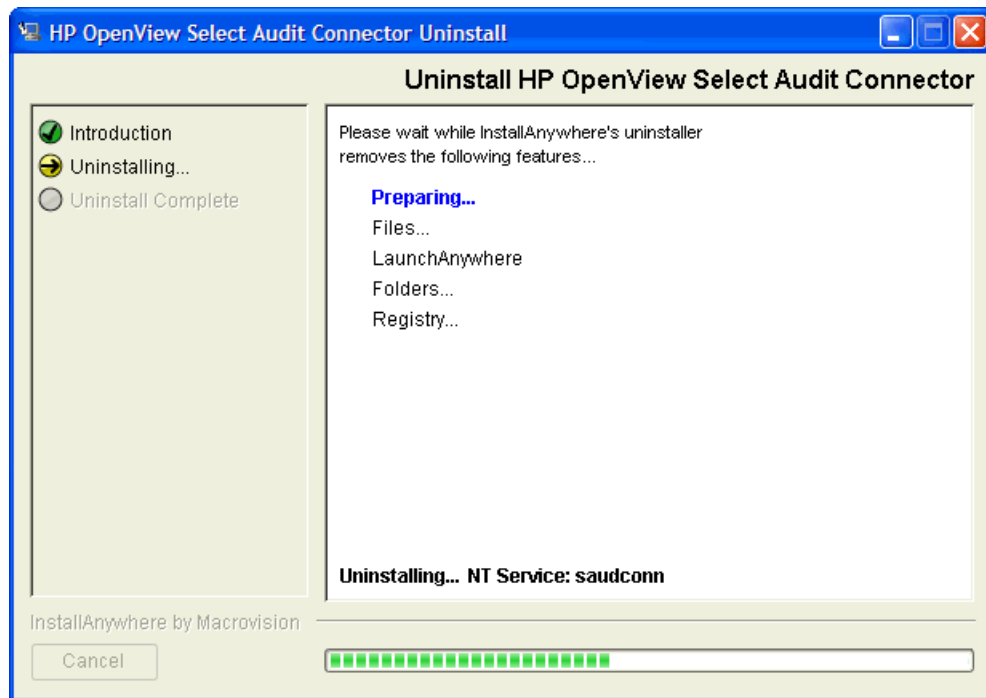


Figure 50 Uninstall Select Audit Connector Screen

When Select Audit is uninstalled, the **Uninstall Complete** screen appears, as shown in Figure 51.

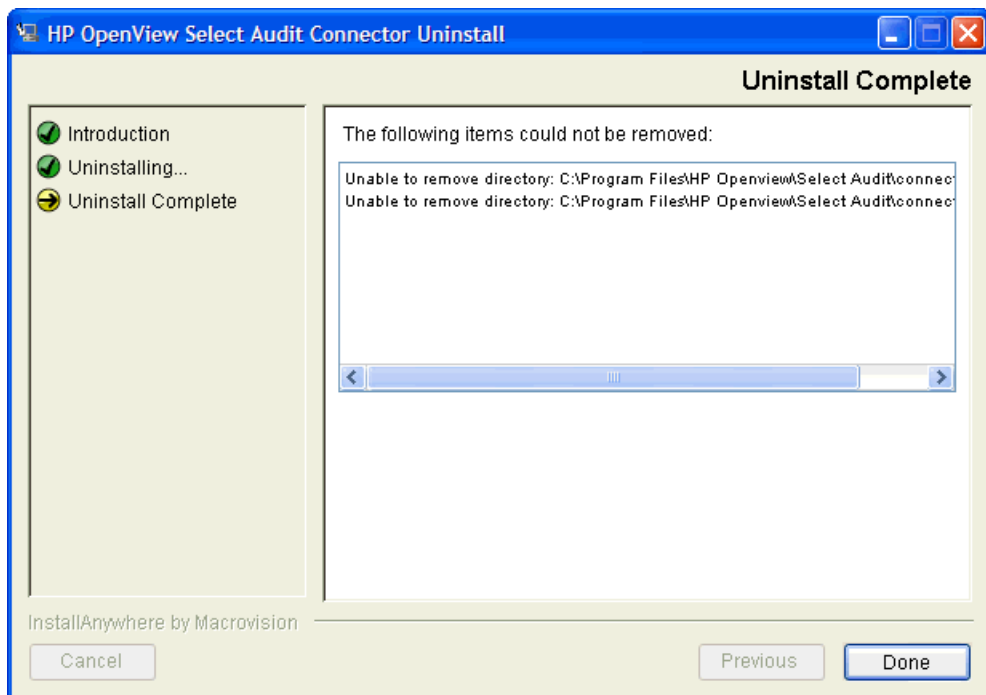


Figure 51 Uninstall Complete Screen

3 Click **Done** to exit the uninstaller.



The uninstaller does not remove any files or folders that are in use at uninstall time. You must remove these manually.

4 Using Self-Healing Services

HP OpenView Self-Healing Services (SHS) are part of HP's built-in support. SHS integrates with OpenView products to provide better support for clients. This chapter describes SHS and how to use it in Select Audit in the following topics:

- [Self-Healing Services](#) on page 65
- [Data Collector](#) on page 65
- [Using SHS](#) on page 67

Self-Healing Services

The typical support process is a cycle where the customer calls support, and is asked to gather a set of information about their system. The data is analyzed and if turns out to be incomplete, the customer is asked to collect more data (which may no longer be available). HP OpenView Self-Healing Services enable HP software to automatically detect problems and take steps to remedy them.

When HP software detects it has suffered a problem, information surrounding the problem is gathered. The gathered information consists of artifacts such as application configuration files, log files and system environmental settings. This information is sent securely to HP. When received, the information is analyzed and processed for possible solutions. A web page is published on eCare with the analysis results, knowledge base and discussion forum documents that relate to the detected problem. An email message is sent notifying you that a problem was detected and a web page has been prepared with information that will enable them to solve the problem. If you cannot solve the problem yourself, you can open a support case which will be handled like a traditional support case, except for one significant difference. The problem, the information surrounding it, and the informational web page are all available to the support engineer without any customer interaction, allowing the support engineer to have as much information about your environment.

Data Collector

A collector gathers whatever information is needed about a customer's environment to help a support engineer solve the problem. Select Audit implements a Data Collector using a Java framework that collects log files, configuration data, and any other information that is useful in debugging a problem.

The Data Collector runs on the Select Audit server side. It collects data when prompted, but does not perform pre-emptive evaluations or self-diagnosis. The SHS component is shown in [Figure 52](#).

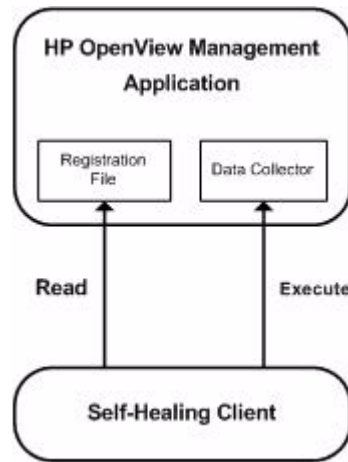


Figure 52 Self-Healing Services

The Data Collector must be registered with the OS via a signed registration file. You must create the registry key entry for SHS to register with the Self-Healing Client.

Data Collection Process

The data collection process can be launched after a customer experiences a problem by running the `run-data-collector.bat` or `run-data-collector.sh` file. See [Using SHS](#) on page 67 for more information about running SHS. The information is transferred to HP support, who diagnose the problem and contact you with a solution. The `saud-collector-task-file.xml` file describes the items to be collected. The Data Collector reads the task file to determine which information to collect, copies all relevant files into the specified output directory, and creates an XML file summarizing all data collected. The data collection process is shown in [Figure 53](#).

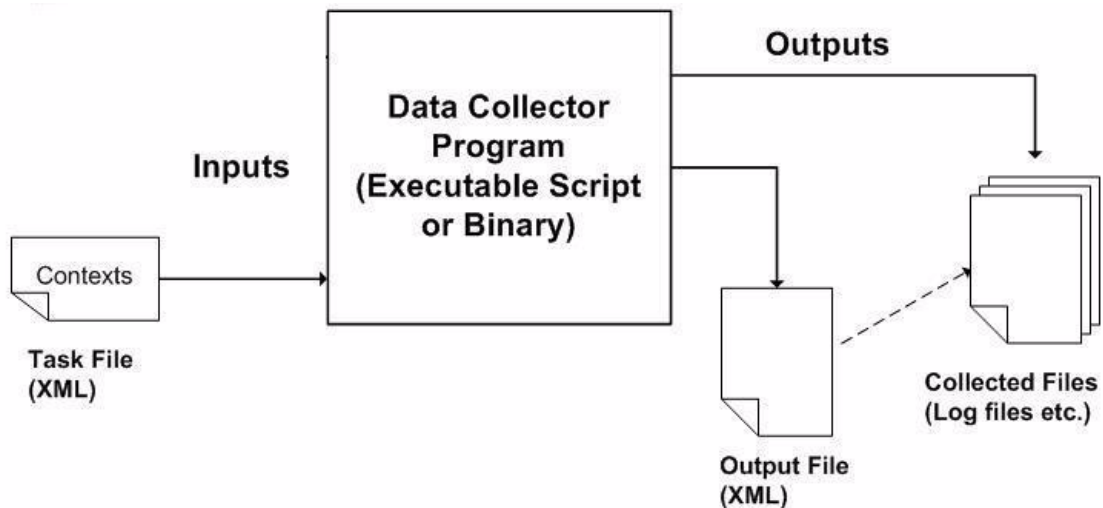


Figure 53 Data Collection Process

Data Collected

SHS collects Select Audit configuration details and log files, environment data, database configuration details, WebLogic configuration files, startup script etc. As more layers of implementation are added, the list of information collected will be updated accordingly.

A maximum of 30 files can be collected, with a maximum file size of 1Mb per file. The total data collected must not exceed 5Mb in total (ISEE).

Using the Data Collector in a Clustered Environment

Each managed server that is part of the cluster requires access to some files on disk, e.g. `audit_config.xml`, `scopeserver.xml`, etc. When installing on the cluster, the installer is only run once on the machine running the WebLogic Administration server.

To make sure all installed files are available to each managed servers, Select Audit is installed on a shared filesystem that is available to all managed servers.

Because SHS is installed in the same path as the Audit Server, there is no need to copy the SHS folder to different machines. Create a different directory for each managed server and modify the SHS script accordingly. You then need to manually change the following files for the specific host's environment (for example, `JRE_HOME`) and define which files to collect:

- `run-data-collector.bat`
- `sign-data-collector.bat`
- `saud-collector-config.xml`

Run the Data Collector on each system directly from the shared location. For continuous metrics you could schedule the appropriate script on each system.

Using SHS

SHS is installed by the Select Audit 1.01 installer at the following location:

```
\HP Openview\Select Audit\auditserver\shs
```

This folder contains the following files:

- `run-data-collector.bat` (or `run-data-collector.sh`) for collecting Select Audit data
- `sign-data-collector.bat` (or `sign-data-collector.sh`) for signing the collector registration file
- `saud-collector-config.xml` configuration file
- `saud-collector-task-file.xml`



You should not modify the `saud-collector-task-file.xml` file.

- `saud-collector.jar`

To start collecting data

- 1 In the **SHS** folder, double-click `run-data-collector.bat` or from the command line using the following command:


```
run-data-collector.bat -c <file> -d <directory> -t <file> -x  
<file>
```

The arguments used in the command are described in the following table:

Table 5 Command Line Arguments

Command	Description
-c	Collector configuration file.
-d	Output directory where collected files will be stored.
-t	Task file containing the collection tasks to be performed.
-x	XML output file to create with the collection information.

The collected files, as well as a summary file and collector log are saved in the HP Openview\Select Audit\auditserver\shs\out folder.

 You can specify another output directory using the `-d` argument.

You can edit the `saud-collector-config.xml` file to add or delete data files to be collected.

- 2 Send the collected files, summary file and collector log to HP Support.

Index

A

- appenders, setting for logging, 40
- Audit Connector
 - installation modes, 46
 - installing, 46
 - installing in Console mode, 54
 - installing in Default mode, 47
 - installing in Silent mode, 55
 - Select application configuration, 46
 - uninstalling, 60
- Audit Server
 - installing, 16
 - post-installation steps, 39
 - uninstalling, 56

C

- clustered environments
 - data collector, 67
 - pre-installation steps, 14
- configuration requirements, Select applications, 46

D

- Data Collector
 - clustered environments, 67
 - collection process, 66
 - data collected, 67
 - described, 65
- databases, default time zones, 44
- defaults
 - installation directory, Select Audit, 22, 48
 - restoring to, 22, 23, 32, 48
- disk space, minimum requirements for, 9

H

- hardware requirements, 9
- HP-UX
 - minimum requirements for, 9
 - platform availability for, 9
 - setting printev for, 15

I

- installation modes
 - Console, 54
 - Default, 47
 - overview, 46
 - Silent, 55
- installation order, 15
- installing Select Audit
 - Connector installer mode overview, 46
 - order, 15
 - pre-steps, 13
 - system requirements, 9
- integration, Select Identity, 13

J

- Java Virtual Machine
 - install location, 55
 - supported versions, 17

L

- links, symbolic, 15, 55
- Linux
 - minimum requirements for, 9
 - platform availability for, 9
 - setting printev for, 15
- log4j
 - appenders, setting, 40
 - configuring, 39
 - enabling, 40
 - properties file, 40
- log4j.properties, 40
- logging
 - configuring, 39
 - enabling, 40
 - redirecting on WebLogic, 42
 - setting appenders, 40

M

- mail sessions, configuring, 43
- memory, minimum requirements for, 9

O

operating systems
 minimum requirements for, 9
 platform availability for, 9

P

platforms. *See* operating systems

post-installation steps
 configuring log4j, 39
 configuring UTF-8 fonts, 44
 database connection pools, default time zones, 44
 WebLogic mail session configuration, 43
 WebLogic roles, adding, 43
 WebLogic server redirecting logging, 42

pre-installation
 clustered environments, 14
 DBA user, 14
 HP-UX, 14
 steps, 13

printenv, path to, 15

processor, minimum requirements for, 9

R

Red Hat Linux. *See* Linux

registry entries, creating, 15

requirements
 JVM, 55
 registry entries, 15
 system, summary of, 9

roles, WebLogic, adding, 43

S

Select Audit
 connector installation, 47, 54, 55
 connector installation modes, 46
 default installation directory, 22, 48
 installation order, 15
 installing, 15
 operating systems available for, 9
 platform availability, 9
 Select Identity integration, 13
 system requirements, 9

Self-Healing Services, 65 to 68
 data collected, 67
 data collection process, 66
 data collector, 65
 described, 65
 using, 67

software requirements, 9

Solaris

 minimum requirements for, 9
 platform availability for, 9
 setting printev for, 15

symbolic links, 15, 55

system requirements for installation, 9

U

UTF-8 fonts, configuring, 44

V

video card, minimum requirements for, 9

VNC, 46

W

WebLogic
 logging, redirecting, 42
 mail session, configuring, 43
 roles, adding, 43

Windows

 minimum requirements for, 9
 platform availability for, 9

X

X-Windows, 46