# HP Select Audit Software

for the Windows®, HP-UX®, Linux®, and Solaris® operating systems

Software Version: 1.02

# Installation Guide

Document Release Date: July 2007
Software Release Date: July 2007

# Legal Notices

## Warranty

## Restricted Rights Legend

## Copyright Notices

## Trademark Notices

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

- 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.
- Microsoft SQL Server 2005 JDBC Driver
- OpenAdaptor from the Software Conservancy.
- Oracle JDBC Thin Driver
- Quartz, Copyright 2004 - 2005 OpenSymphony
- spring-framework from the Apache Software Foundation.
- Tomahawk from the Apache Software Foundation.
- treeviewjavascript from GubuSoft.
- Xalan-Java from the Apache Software Foundation.
- Xerces-Java version from the Apache Software Foundation.

Please check the `<install_dir>/3rd_party_license` folder for expanded copyright notices from such third party suppliers.

## Documentation Updates

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

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

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

**http://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 software support web site at:

**www.hp.com/go/hpsoftwaresupport**

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

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

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels and HP Passport, go to:

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

To find more information about HP Passport, go to:

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

# Contents

# 1 About the Select Audit Installation

HP Select Audit software is part of HP's 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 HP products and third-party applications.

## Audience

This document is intended for system administrators mandated to install and configure HP Select Audit 1.02 to suit their business and industry environment. This guide assumes a working knowledge of the following:

- WebLogic application server administration and configuration
- WebSphere application server administration and configuration
- Oracle database administration
- MSSQL database administration
- J2EE environments

## The Select Audit Documentation Set

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

- *HP Select Audit 1.02 Administration Guide*, © Copyright 2006 - 2007 Hewlett-Packard Development Company, L.P. (`administration_guide.pdf`).
- *HP Select Audit 1.02 Installation Guide*, © Copyright 2006 - 2007 Hewlett-Packard Development Company, L.P. (`installation_guide.pdf`).
- *HP Select Audit 1.02 User's Guide*, © Copyright 2006 - 2007 Hewlett-Packard Development Company, L.P. (`user_guide.pdf`).
- *HP Select Audit 1.02 Sarbanes-Oxley Model Guide*, © Copyright 2006 - 2007 Hewlett-Packard Development Company, L.P. (`sb_model_guide.pdf`)
- *HP Select Audit 1.02 Concepts Guide*, © Copyright 2006 - 2007 Hewlett-Packard Development Company, L.P. (`concepts_guide.pdf`)
- *HP Select Audit 1.02 Report Center User's Guide*, © Copyright 2006 - 2007 Hewlett-Packard Development Company, L.P. (`rpt_center_guide.pdf`)
- *HP Select Audit 1.02 Report Designer's Guide*, © Copyright 2006 - 2007 Hewlett-Packard Development Company, L.P. (`rpt_design_guide.pdf`)

- *HP Select Audit 1.02 Report Developer's Guide*, © Copyright 2006 - 2007 Hewlett-Packard Development Company, L.P. (`rpt_devel_guide.pdf`)

Online help is available with the Audit Portal.

# Installation Environment

Select Audit has three installers: a Connector installer and two Server installers, one for WebLogic and one for WebSphere. The Connector installer installs the Audit Connector on client machines running one or more of the HP 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 11
- Platform Availability on page 11

## Supported Platforms

The Select Audit Connector installer supports the following platforms:

- Select Identity 4.0, 4.11 and 4.12
- 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** | • Microsoft Windows 2003<br>• HP-UX 11.23, 11.23 Itanium, 11.31 Itanium<br>• Red Hat Linux AS 3.0, AS 4.0<br>• Solaris 9 and Solaris 10 |
| **Application and portal servers** | • BEA WebLogic Application Server 8.1 SP5 or SP6<br>• IBM WebSphere 6.0.2 fixpack 17 |
| **Audit connectors** | • HP Select Identity 4.0, 4.11 and 4.12<br>• HP Select Access 6.1 P3 and 6.2<br>• HP Select Federation 6.5 and 6.6 |
| **Audit storage and databases** | • Oracle 9i, 10g<br>• Microsoft SQL Server 2000 |
| **Compliance report packs** | • 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<br>For HP-UX: 220 MB |
| Video card | 256 colors | 256 colors |
| Operating systems | Windows 2003 Server Service Pack 2 | Red Hat Enterprise Linux 3<br>HP-UX 11.B.11.23 64 bit with all required patches |

➤ The specified memory requirements are per managed server. If you choose to run more than one Audit Server on the same machine, for example, if a WebLogic cluster installation has two or more managed servers on one machine, that machine should have a minimum of 1 GB of memory and 2 GB for improved performance, for each managed server.

➤ The recommended memory is 2 GB for improved performance to reduce the use of swap space.

## Platform Availability

The Select Audit Server is available for the Windows 2003 and UNIX (Linux, Solaris 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 Select Audit 1.02 Release Notes* (`SAudit_release_notes_1.02.html`) on the Select Audit installation CD for known installation issues at the time of this release.

**Table 3 Chapter Summary**

| Chapter | Description |
|---|---|
| Chapter 1, About the Select Audit Installation | This chapter describes the installation environment needed for Select Audit. |
| Chapter 2, Pre-Installation Information | This chapter describes the pre-installation steps for the Select Audit installers |
| Chapter 3, Installing Select Audit on WebLogic | This chapter describes how to install and uninstall the Select Audit components on your network with WebLogic. |
| Chapter 4, Installing Select Audit on WebSphere | This chapter describes how to install and uninstall the Select Audit components on your network with WebSphere. |
| Chapter 5, Installing the Select Audit Connector | This chapter describes how to install the Select Audit Connector. |
| Chapter 6, Using Self-Healing Services | HP Self-Healing Services (SHS) are part of HP's built-in support. This chapter describes SHS and how to use it in Select Audit. |
| Appendix A, Installer Configurations | This appendix describes the actions the WebLogic and WebSphere installers perform when installing Select Audit. |

# 2 Pre-Installation Information

This chapter describes the Select Audit installers, the required pre-installation steps and the recommended installation order.

## Select Audit Installers

Because HP employs InstallAnywhere installers, Select Audit is as simple to install as it is to configure. There are two main modules to install for Select Audit:

- the Audit Server
- the Audit Connector

### Audit Server

The Server installers install the Audit Server, reporting, and Self-Healing Services components on WebLogic or WebSphere. For information about Self-Healing Services, see Chapter 6, Using Self-Healing Services. The Server installer copies the necessary files to your system. This application is then deployed to the application server using the Deployment Wizard.

➤ The Audit Server requires a previously-installed J2EE server and database for deployment. Before installing the Audit Server, create a database and set up an application server for deployment. The Select Audit installer will not install an application server or database instance.

The Deployment Wizard prompts you for information about your J2EE server in order to automatically deploy the Audit Server. The files are copied to the main installation directory (`/SelectAudit/auditserver/dist`) at installation time. Post-installation, the wizard configures and deploys the application on the application 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.

### Audit Connector

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 Audit Connector relies on a configuration file that is created by the Connector installer and can be modified using 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 `jre` 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.

## The Impact of Running Control Panel Applications

If you are installing, uninstalling 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 is used to run the application server. 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`.

# Before Installing Select Audit

Before Select Audit is installed, you must do the following:

1. Install WebLogic 8.1 SP5 or SP6, or WebSphere 6.0.2 fixpack 17.
2. Create a new domain, and configure the server or cluster that the Audit Server will be deployed on.
3. Create a new database instance.
4. Setup the database schema.

➤ The application server the Audit Server is deployed on should be setup according to the vendor's recommendations.

## Creating a New Database Instance

Create a new database instance for the database you will use with Select Audit.

### Oracle

Before you start the Select Audit installation process, have the database server name, the new database instance port number and SID information available. A new database user will be created during installation; the user name and password of a DBA user is required for this step. You must have a DBA user name and password in order to install the Select Audit database tables and complete all the database-level setup needed by the application.

The Oracle Database server must have the Java option installed.

The Audit Server installer scripts create 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.

### MSSQL

To use JDBC distributed transactions through JTA, your system administrator should use the procedure described in the following link to install Microsoft SQL Server JDBC XA procedures.

➤ These instructions are only for MSSQL on WebLogic. No additional configuration is needed for WebSphere.

```
http://e-docs.bea.com/wls/docs81/jdbc_drivers/mssqlserver.html"
```

1. Copy the `sqljdbc.dll` and `instjdbc.sql` files from the `WL_HOME\server\lib` directory to the `SQL_Server_Root/bin` directory of the MS SQL Server database server, where `WL_HOME` is the directory in which WebLogic server is installed, typically `C:\bea\weblogic81`.

   ➤ If you are installing stored procedures on a database server with multiple Microsoft SQL Server instances, each running SQL Server instance must be able to locate the `sqljdbc.dll` file. Therefore the `sqljdbc.dll` file must be anywhere on the global PATH or on the application-specific path. For the application-specific path, place the `sqljdbc.dll` file into the `<drive>:\Program Files\Microsoft SQL Server\MSSQL$<Instance 1 Name>\Binn` directory for each instance.

2. Use SQL Query Analyzer to run the `instjdbc.sql` script.

   The system administrator should back up the master database before running `instjdbc.sql`. The `instjdbc.sql` script generates many messages. In general, these messages can be ignored; however, the system administrator should scan the output for any messages that may indicate an execution error. The last message should indicate that `instjdbc.sql` ran successfully. The script fails when there is insufficient space available in the master database to store the JDBC XA procedures or to log changes to existing procedures.

3. Start the DTC (Distributed Transaction Coordinator) service for the Microsoft SQL Server database.

This procedure must be repeated for each MS SQL Server installation that will be involved in a distributed transaction.

## Setting Up The Database Schemas

Select Audit supports the following databases:

- Oracle 9i and 10g
- Microsoft SQL 2000

### To configure the Oracle database server

Run the following scripts provided with Select Audit:

- `CREATE_DB_USER.SQL`
- `CREATE_ALL.SQL`
- `INIT_ALL.SQL`

1. In the `CREATE_DB_USER.SQL` script, replace the following variables with their own value:

   `$USER_NAME$`: The name of the database user to be created.

   `$USER_PSWD$`: The password of the database user to be created.

   ➤ The script uses default settings that can be customized before it is run.

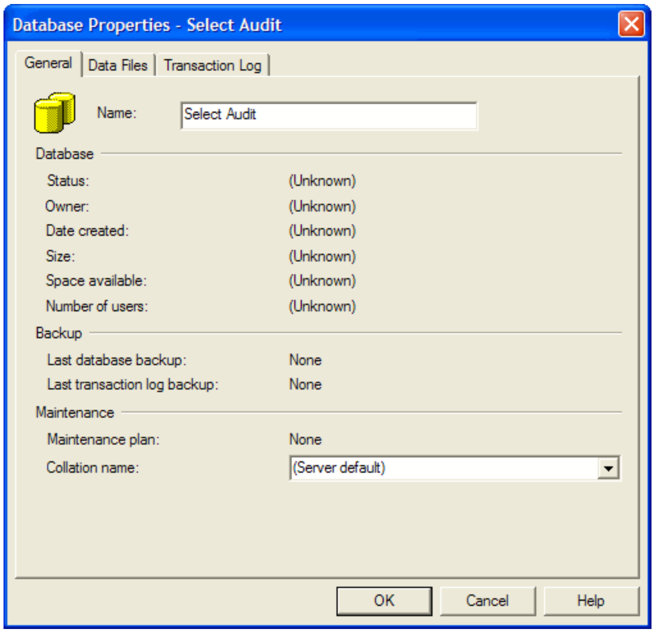
2. Log on to SQL Plus as the DBA (usually `system`) and run the `CREATE_DB_USER.SQL` script.
3. Log on to SQL Plus as the newly-created database user and run the `CREATE_ALL.SQL` script.
4. Next, run the `INIT_ALL.SQL` script.

## To configure the MSSQL database server

Before you install Select Audit, configure the MSSQL database using the Microsoft SQL Server Enterprise Manager interface.

1. Log in to the Microsoft SQL Server Enterprise Manager interface.
2. Click **Microsoft SQL Server** → **SQL Server Group** → **<server>** where **<server>** is the name of the SQL Server instance.
3. Right-click **Databases** and select **New Database**.

   The **Database Properties** dialog opens.



Database Properties - Select Audit

Name: Select Audit

Database

Status: (Unknown)

Owner: (Unknown)

Date created: (Unknown)

Size: (Unknown)

Space available: (Unknown)

Number of users: (Unknown)

Backup

Last database backup: None

Last transaction log backup: None

Maintenance

Maintenance plan: None

Collation name: (Server default)

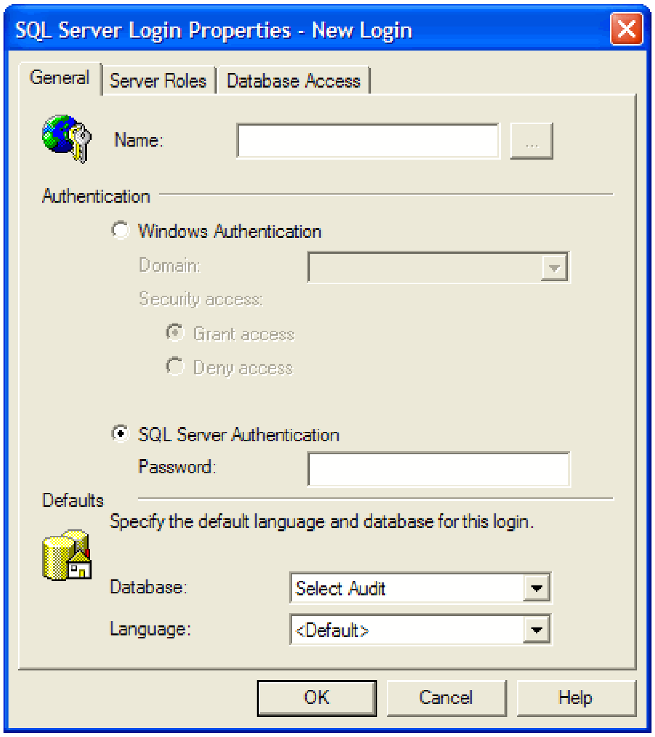
4. Type a name for the database, such as Select_Audit.
5. Click **OK** to finish creating the database.

6 Create a user account to manage the Select Audit database by completing the following steps:

   a Select the `Microsoft SQL Server\SQL Server Group\server\Security` folder in the Enterprise Manager tree.

   b Create a new login for the new database by right-clicking **Logins** and selecting **New Login**.

   The **SQL Server Login Properties - New Login** dialog opens.



● SQL Server Authentication

Database: Select Audit

Language: <Default>

   c On the **General** tab, type a user name such as SAud, type a password, and select the **SQL Server Authentication** radio button as the authentication type.

   d Select the new database (Select_Audit) from the **Database** drop-down list. Keep the remaining default settings.

   e Click **OK**.

   f Confirm your password when prompted.

   g Click the **Database Access** tab.

   h Select the **Permit** check box next to the Select Audit database user.

   i Assign the `db_owner` and `public` permissions to the new user.

   j Click **OK** to save your settings.

7 Create the Select Audit database schema by performing the following steps:

   a Launch the **SQL Query Analyzer** by clicking **Tools** → **SQL Query Analyzer**.

   b Select the new database (Select Audit) from the **Database** drop-down list.

8 Load the `create_all.sql` script from the Select Audit database home directory.

   a Edit the `create_all` script by doing the following:

      — Replace all occurrences of `$USER_NAME$` with your database user name.

— Replace `$DB_NAME$` with the name of the database you created in step 3.

b Click the **Open** icon. Locate the Select Audit home directory.

c Select the `create_all.sql` file.

d Click **Open**.

e Run the script by clicking **Query** → **Execute** or **Play**.

➤ Ignore the warnings that are generated after running the script. These warnings can be safely ignored and will not cause any issues. The maximum size of the data being stored in the tables listed in the warning messages will not be exceeded.

f Verify that no error message is shown.

9 Insert the required default data into the Select Audit database by performing the following steps:

a Edit the `init_all` script by replacing all occurrences of `$DB_NAME$` with your database user name.

b Clear the previous script by clicking **Edit** → **Clear Window**.

c Load the `init_all.sql` script from the Select Audit database home directory.

d Click **Query** → **Execute**.

Messages in the console indicate that rows are being created.

e Verify that no error message is shown.

f Close the **SQL Query Analyzer** and the **Microsoft SQL Server Enterprise Manager**.

## Adding Users to Roles

The Audit Server installer creates the following roles:

- Select Audit Administrator
- Select Audit User
- Select Audit Auditor

As part of the pre-installation procedures, you should create the corresponding groups in your LDAP (Select Audit Administrators, Select Audit Auditors and Select Audit Users). The installer maps the roles to those groups. You must add users to the groups before the users can log on to Select Audit.

➤ The user that will be used in deployment should be added to the Select Audit Administrators group. If you are using a WebLogic embedded LDAP, this is taken care of by the installer.

An additional group, Select Audit Report Developers, must also be added to LDAP. This group is for report developers. Report developers need additional rights. They have access to the Developer Center and to error output from reports.

# 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 the LDAP repository used by the application server.

You may have to create the GLOBALUSER correlation table. See Correlating Users Between Applications in the *HP Select Audit 1.02 Administration Guide* for more information about the GLOBALUSERS table. Ensure the GUID used is the same as the login name in Select Identity.

Make sure you have the following information available before beginning.

- For the Select Identity server:
  - host name
  - port number
  - super administrator name
  - super administrator password
- For the Select Identity database:
  - host name
  - port number
  - database name (SID)
  - log-on user name
  - log-on user password

## Installing Select Audit and Select Identity on the Same Domain

If you want to install Select Identity and Select Audit in the same domain, they must be installed on separate servers. In most cases, this will mean having two clusters on the domain; one for Select Audit servers and another for Select Identity servers. This will ensure you can still achieve proper load balancing. If you do not want to run clusters, you can install two managed servers.

# Installing on HP-UX

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.

### Itanium Installation

The WebLogic 8.1 sp5 Itanium installer does not install any JDKs when it installs WebLogic. You must download the JDK 1.4.2_13 from HP at the following web site if you are using WebLogic 8.1.5:

```
http://www.hp.com/products1/unix/java/java2/sdkrte14/downloads/
license_sdk_1.4.2.13_itanium.html
```

For more information, refer to `http://e-docs.bea.com/platform/suppconfigs/configs81/hpux11_itanium/81sp5.html`.

## Installing in a Clustered Environment

When you run the Audit Server installer, you are given the option of installing in a single server or clustered environment. If you want to run Select Audit in a clustered environment, you must follow the appropriate steps for your application server before running the Audit Server installer.

➤ When installing on a cluster, ensure that there is at least 130 Mb of free space on the machine for each managed server, to account for application staging.

### Installing in a Clustered Environment on WebLogic

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.

   ➤ For Windows, you must create a shared directory and map that shared directory to a drive letter. The drive letter must be the same on all the machines that form the cluster.

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.

   ⚠ Make sure the mounted filesystem has read/write permissions on each managed server.

### Installing in a Clustered Environment on WebSphere

1. Create a WebSphere Deployment Manager and application server profiles on each server that will host a cluster member.
2. Federate the application server profiles with the Deployment Manager and create a cluster.

3 Start all the application servers in the cluster.

4 Create a shared directory on the Deployment server machine.

5 Mount the shared filesystem on the WebSphere Deployment Manager 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.

  ⚠ Make sure the mounted filesystem has read/write permissions on each managed server.

## 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 user name 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 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.

# 3 Installing Select Audit on WebLogic

This chapter describes how to install and uninstall the Audit Server on WebLogic.

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.

## Installing 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 `SelectAuditServerWLInstall.exe`.

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

  ⚠ If you are installing, uninstalling 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

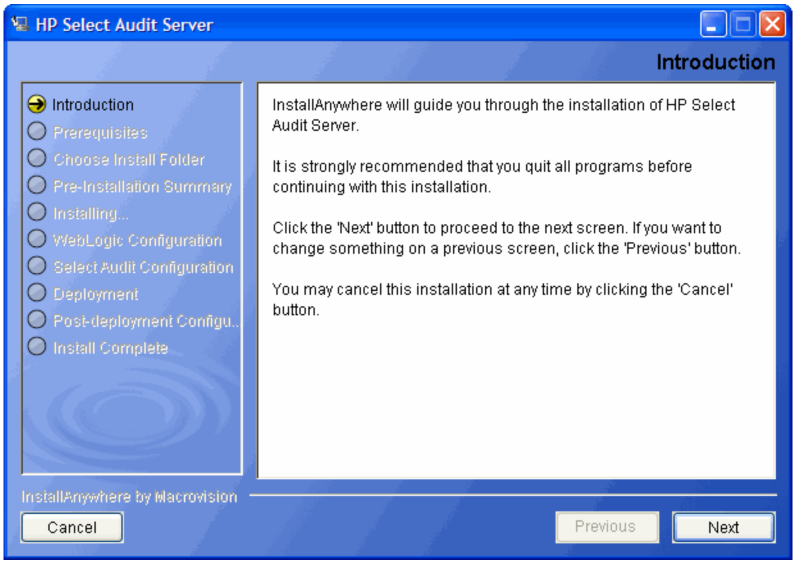
- **On HP-UX, Linux or Solaris:**

  Type the following command:

  `./SelectAuditServerWLInstall.bin`.

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

The installer extracts the installation files and then prepares the Select Audit Install wizard. When it has finished loading, the **Server Installer Introduction** screen opens.



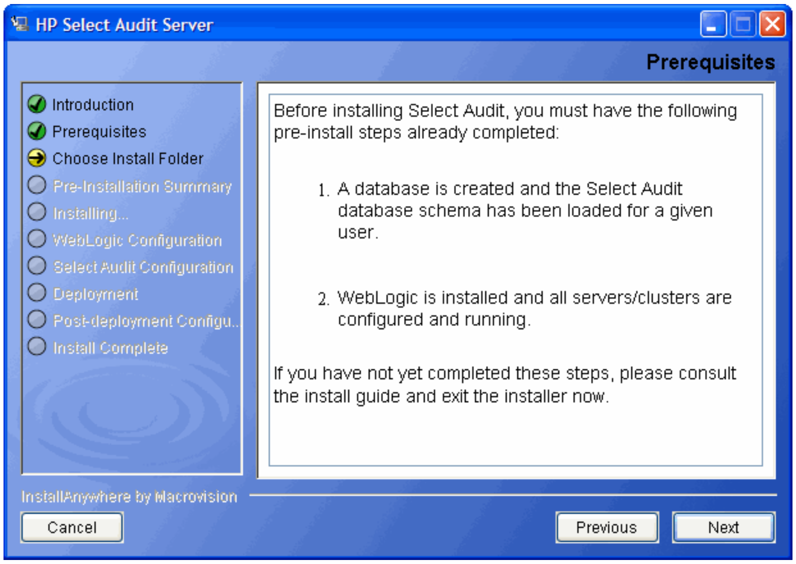
InstallAnywhere will guide you through the installation of HP Select Audit Server.

It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

2 Click **Next**. The **Prerequisites** screen opens.



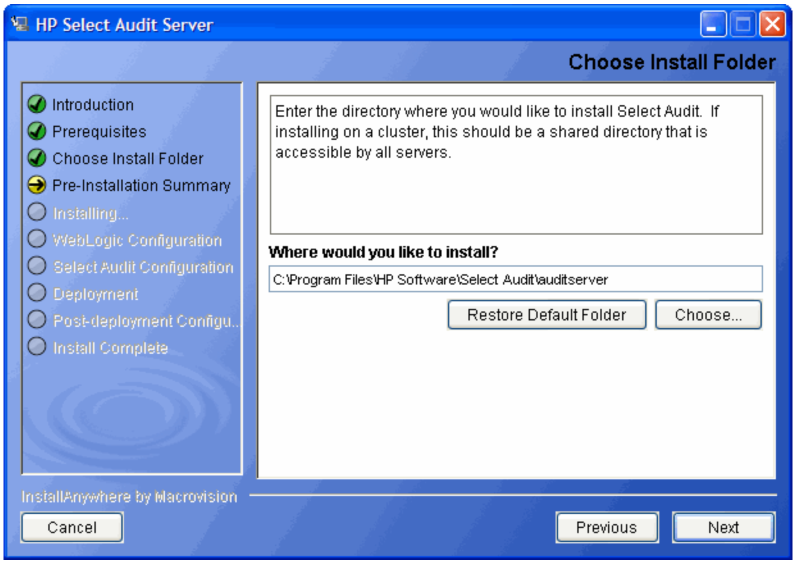
Before installing Select Audit, you must have the following pre-install steps already completed:

1. A database is created and the Select Audit database schema has been loaded for a given user.
2. WebLogic is installed and all servers/clusters are configured and running.

If you have not yet completed these steps, please consult the install guide and exit the installer now.

3 Review the listed prerequisites and confirm they have been met before proceeding.

4 Click **Next**. The **Choose Install Folder** screen opens.



Enter the directory where you would like to install Select Audit. If installing on a cluster, this should be a shared directory that is accessible by all servers.

**Where would you like to install?**

C:\Program Files\HP Software\Select Audit\auditserver

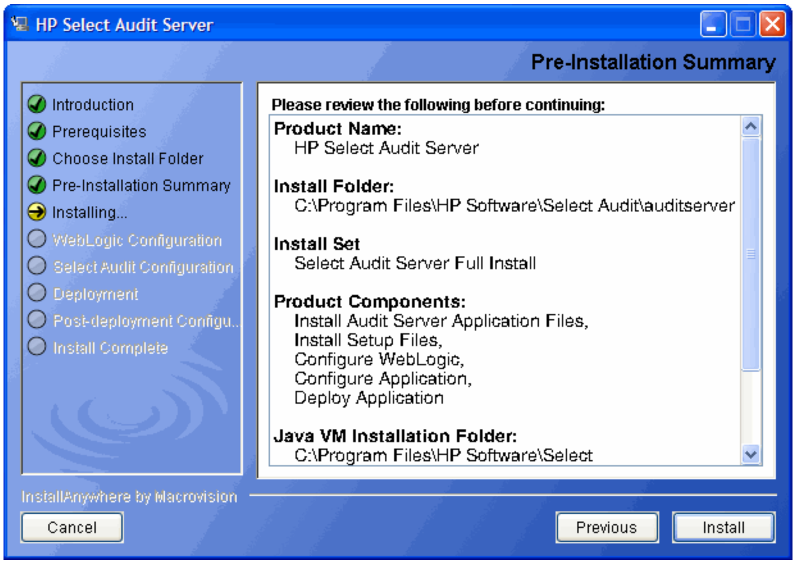
5 Select the location where you wish to install the Audit Server.

➤ 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.

6 Click **Next**. The **Pre-Installation Summary** screen opens.

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

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



**Please review the following before continuing:**

**Product Name:**
HP Select Audit Server

**Install Folder:**
C:\Program Files\HP Software\Select Audit\auditserver

**Install Set**
Select Audit Server Full Install

**Product Components:**
Install Audit Server Application Files,
Install Setup Files,
Configure WebLogic,
Configure Application,
Deploy Application

**Java VM Installation Folder:**
C:\Program Files\HP Software\Select

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

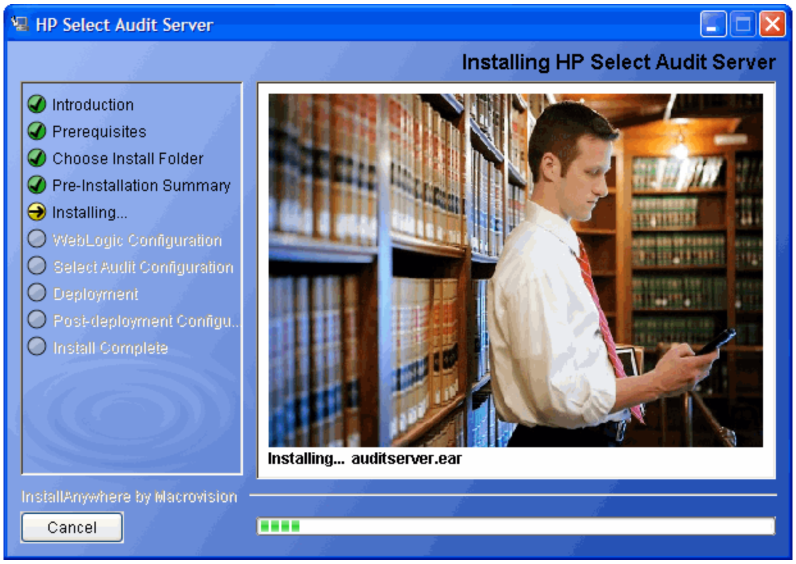
- The installation folder you chose to install the Audit Server in.
- The installation set.
- The components that will be installed.

- 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 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.

7 Review the information on the **Pre-Installation Summary** screen. If the information is correct, click **Install**.

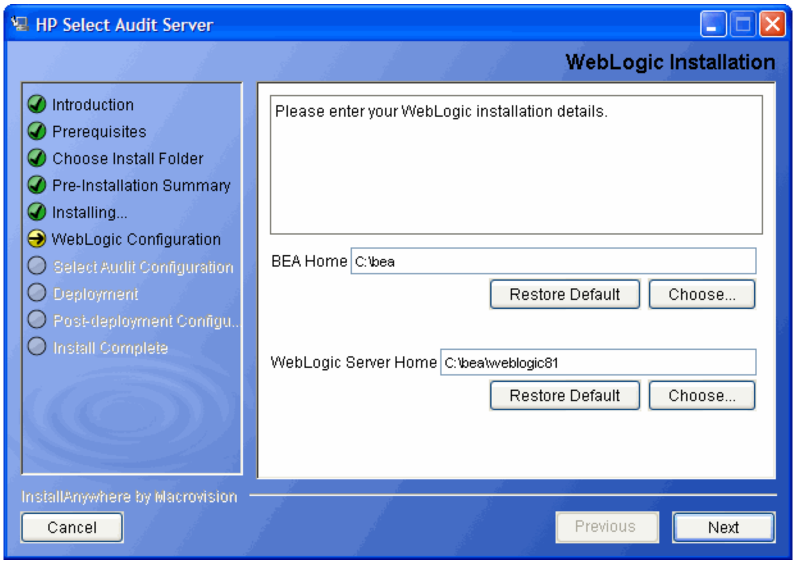
> To change any of the installation settings, click **Previous** to return to the screen containing the settings you want to change.

The Audit Server begins to install and the **Server Installation Progress** screen opens.



Installing... auditserver.ear

When the Audit Server installer is finished, the **WebLogic Installation** screen opens.



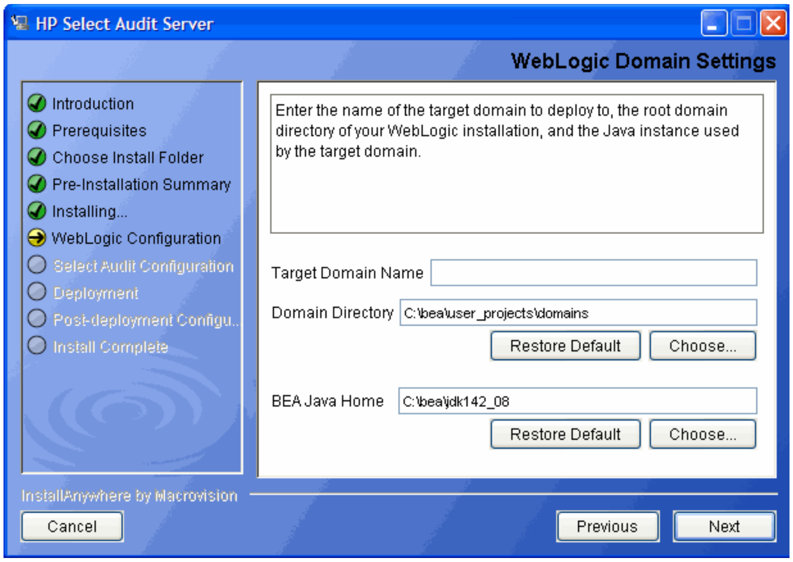
Please enter your WebLogic installation details.

BEA Home C:\bea

WebLogic Server Home C:\bea\weblogic81

8 If the default locations are incorrect, select your WebLogic home directory and WebLogic Server directory by clicking **Choose** beside each field.

9 Click **Next**. The **WebLogic Domain Settings** screen opens.



WebLogic Domain Settings

Enter the name of the target domain to deploy to, the root domain directory of your WebLogic installation, and the Java instance used by the target domain.

Target Domain Name

Domain Directory C:\bea\user_projects\domains

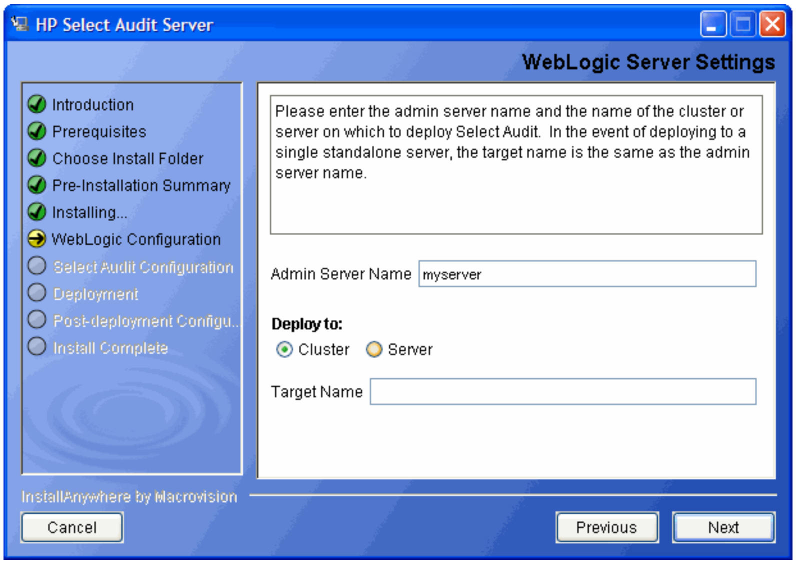
BEA Java Home C:\bea\jdk142_08

10 Do the following:

- Type the target domain in the **Target Domain Name** field.
- Type the root domain directory in the **Domain Directory** field.
- Type the location of the JDK used by the target domain in the **BEA Java Home** field.

➤ Click **Restore Default** to restore the Select Audit defaults.

11 Click **Next**. The **WebLogic Server Settings** screen opens.



WebLogic Server Settings

Please enter the admin server name and the name of the cluster or server on which to deploy Select Audit. In the event of deploying to a single standalone server, the target name is the same as the admin server name.

Admin Server Name myserver

**Deploy to:**

● Cluster ○ Server

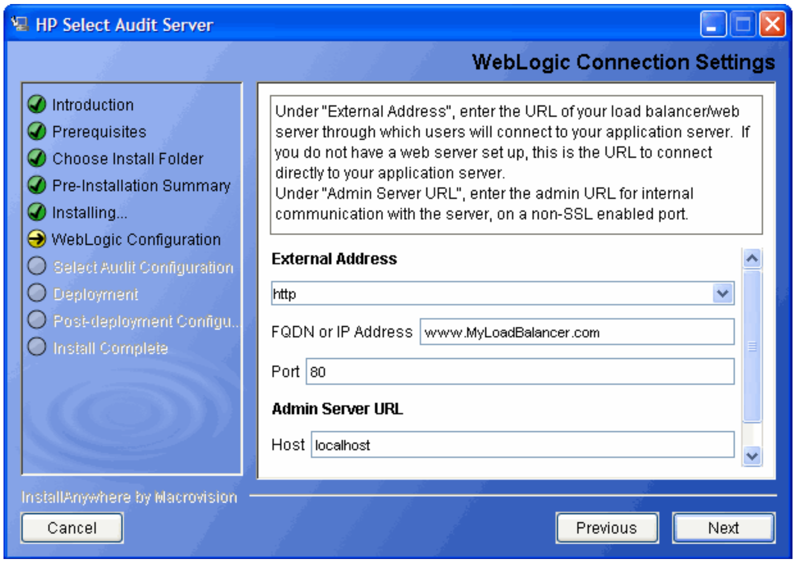
Target Name

12 Do the following:

- Select whether to deploy Select Audit as a stand-alone server or on a cluster.
- Type the Administration server name in the **Admin Server Name** field.
- Type the server name in the **Target Name** field.

➤ For stand-alone servers, this name will be the same as the Administration server name.

13 Click **Next**. The **WebLogic Connections Settings** screen opens.



Under "External Address", enter the URL of your load balancer/web server through which users will connect to your application server. If you do not have a web server set up, this is the URL to connect directly to your application server.
Under "Admin Server URL", enter the admin URL for internal communication with the server, on a non-SSL enabled port.

**External Address**

http

FQDN or IP Address: www.MyLoadBalancer.com

Port: 80

**Admin Server URL**

Host: localhost

14 Do the following:

- Select an address type from the **External Address** drop-down list.
- Type the URL that external 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.

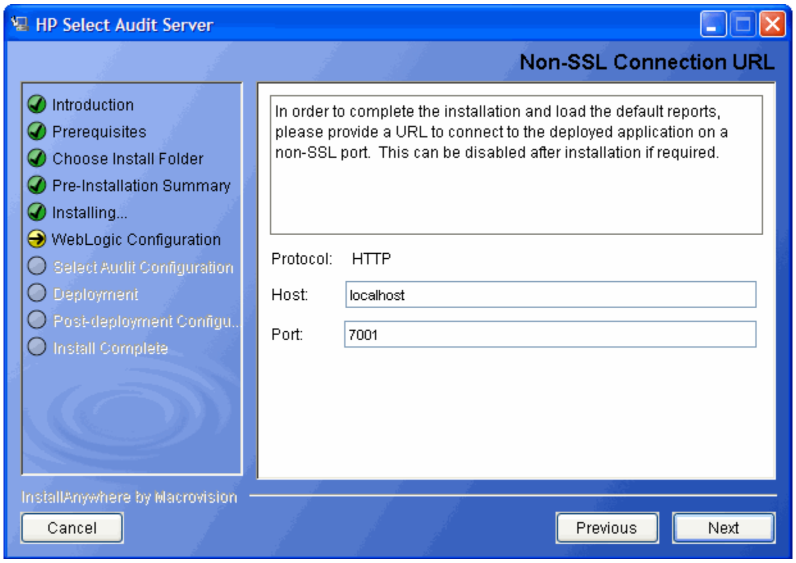
- Type the port number of the external address in the **Port** field.
- Type the administration URL that users will use for internal communication to the system in the **Host** field.
- Type the Administration server port number of the in the **Port** field.

15 If you selected `https` for the **External Address** type, the **Non-SSL Connection URL** screen opens.

Reports must be loaded through an `http://` SOAP call. A non-SSL connection is required to complete the installation. The `http` connection URL is not used again once the installation is complete.

> Import the CA certificate to the `cacerts` file used as the trust store for your Java Virtual machine. You can often use the keytool utility to do this:

```
keytool -import -alias <CA_Alias> -file <path/to/ca.der>
-keystore <path/to/cacerts_file> -storepass <password>
```



Non-SSL Connection URL

In order to complete the installation and load the default reports, please provide a URL to connect to the deployed application on a non-SSL port. This can be disabled after installation if required.

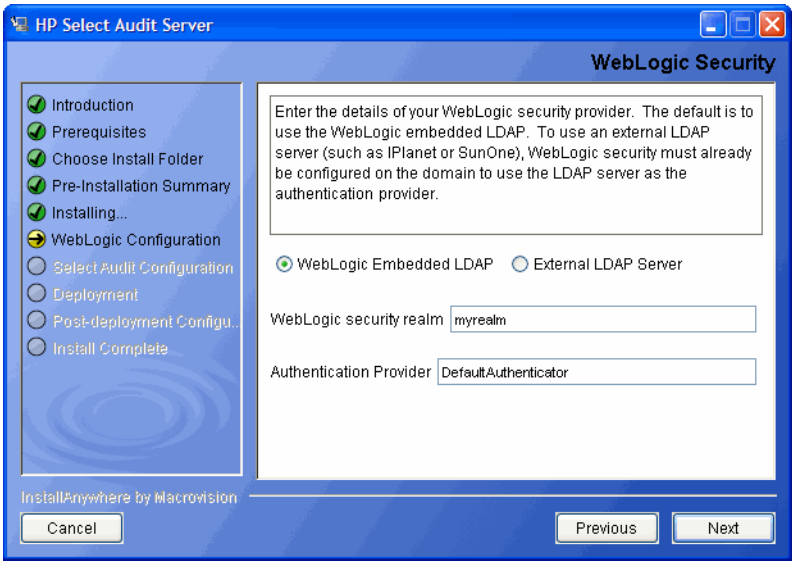
Protocol: HTTP

Host: localhost

Port: 7001

16 Type the non-SSL host name in the **Host** field and the non-SSL port number in the **Port** field.

17 Click **Next**. The **WebLogic Security** screen opens.



WebLogic Security

Enter the details of your WebLogic security provider. The default is to use the WebLogic embedded LDAP. To use an external LDAP server (such as IPlanet or SunOne), WebLogic security must already be configured on the domain to use the LDAP server as the authentication provider.

● WebLogic Embedded LDAP ○ External LDAP Server

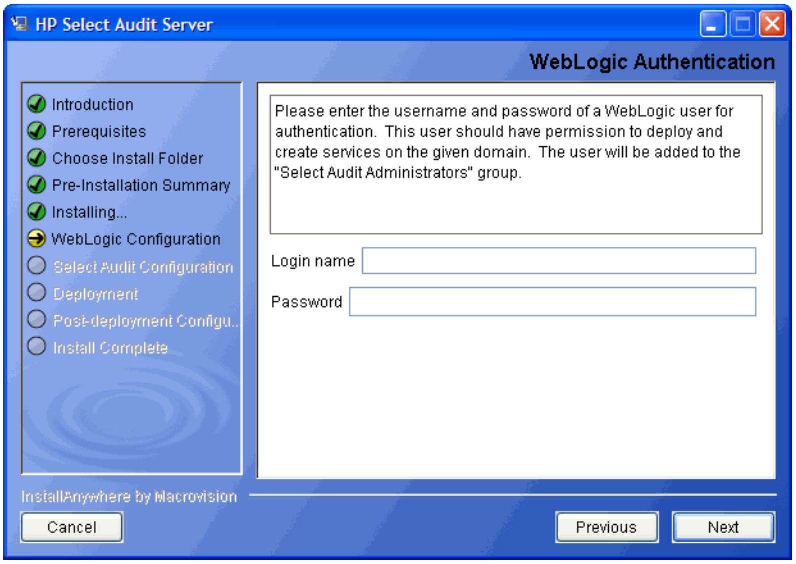
WebLogic security realm myrealm

Authentication Provider DefaultAuthenticator

18 Do the following:

- Select the type of LDAP server you want to use.
- Type your security realm in the **WebLogic security realm** field.
- Type the name of the authentication provider in the **Authentication Provider** field.

19 Click **Next**. The **WebLogic Authentication** screen opens.



WebLogic Authentication

Please enter the username and password of a WebLogic user for authentication. This user should have permission to deploy and create services on the given domain. The user will be added to the "Select Audit Administrators" group.

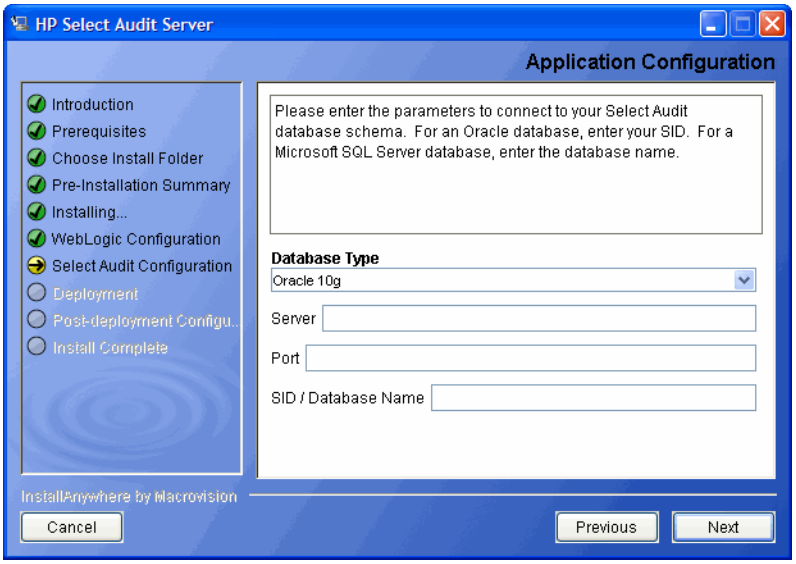
Login name

Password

20 Type the user name and password of a user with permission to deploy and create services on the domain.

> This user will be added to the Select Audit Administrators group if you are using an embedded LDAP. For external LDAP, manually add the user to the Select Audit Administrators group.

21 Click **Next**. The **Application Configuration** screen opens.



Application Configuration

Please enter the parameters to connect to your Select Audit database schema. For an Oracle database, enter your SID. For a Microsoft SQL Server database, enter the database name.

Database Type: Oracle 10g

Server

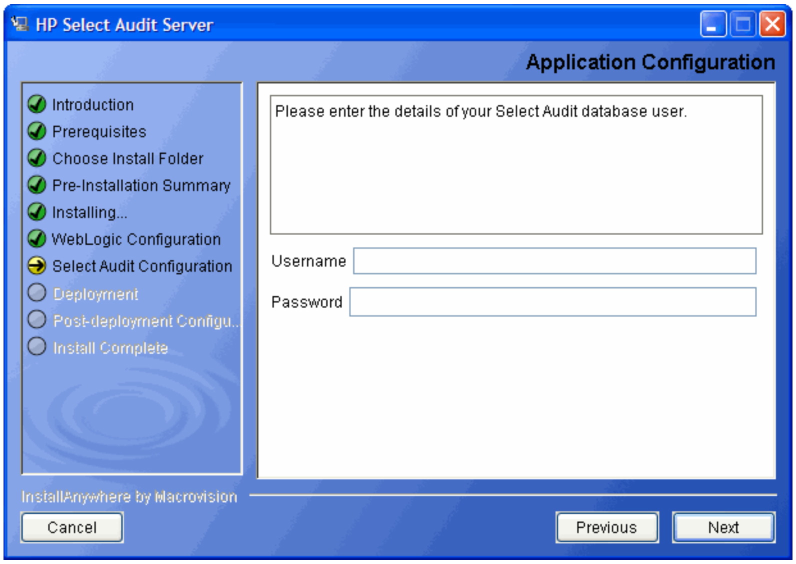
Port

SID / Database Name

22 Enter the database connection parameters as follows:

- Select your database type from the **Database Type** drop-down list.
- Type the database server address in the **Server** field.
- Type the database listener port number in the **Port** field.
- If you are using an Oracle database, type the SID in the **SID/Database Name** field.
- If you are using an MSSQL database, type the database name in the **SID/Database Name** field.

23 Click **Next**. The **Application Configuration** log-on information screen opens.



Please enter the details of your Select Audit database user.

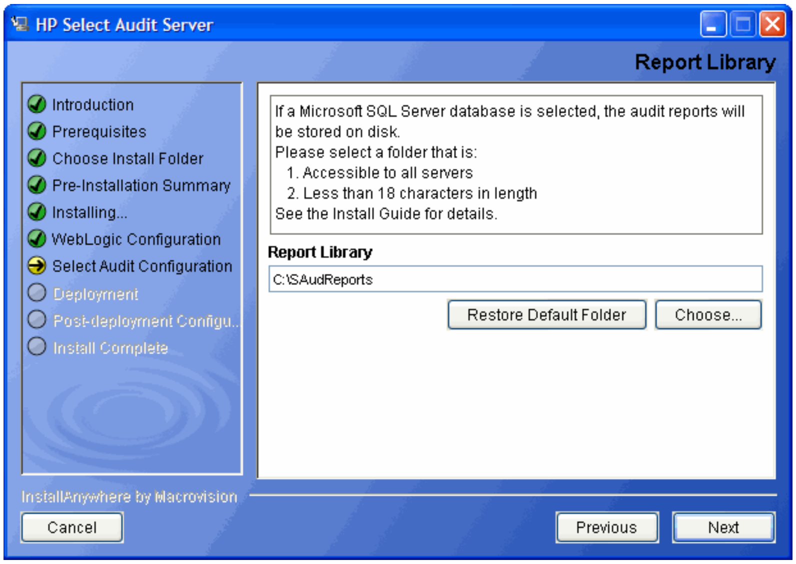
Username

Password

24 Type your database user name in the **Username** field and your database password in the **Password** field.

25 Click **Next**. The installer tests the database connection.

- If you are using Oracle, go to step 27.
- If you are using MSSQL, the **Report Library** screen opens.

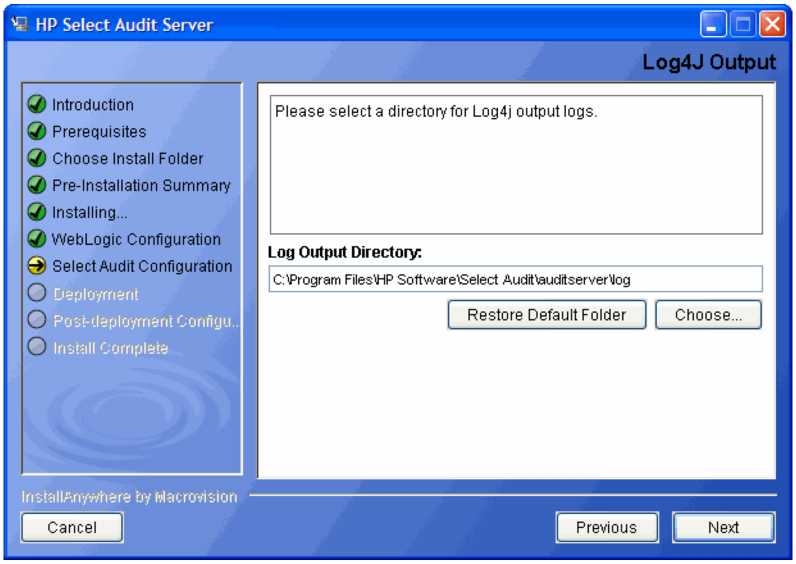


If a Microsoft SQL Server database is selected, the audit reports will be stored on disk.
Please select a folder that is:
1. Accessible to all servers
2. Less than 18 characters in length
See the Install Guide for details.

**Report Library**

C:\SAudReports

26 Select a location for the audit reports and click **Next**. The **Log4J Output** screen opens.



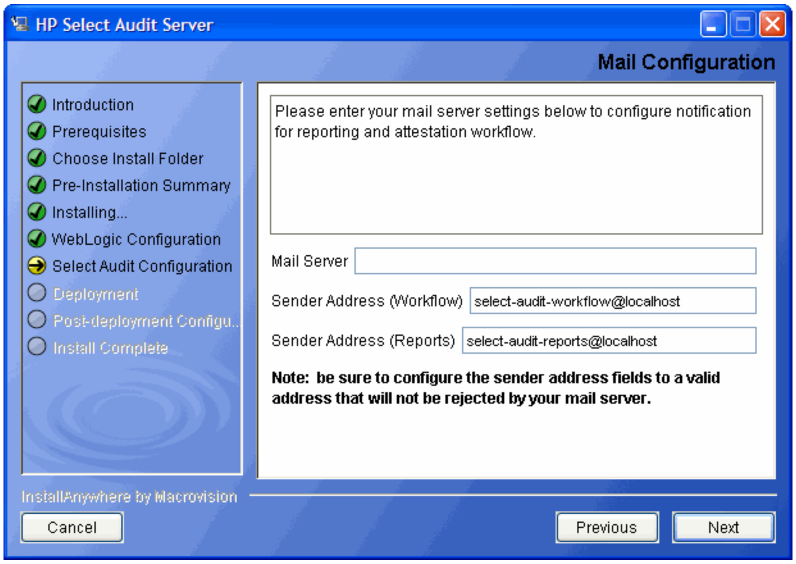
Please select a directory for Log4j output logs.

Log Output Directory: C:\Program Files\HP Software\Select Audit\auditserver\log

27 Click **Choose** or type the directory location where you would like Select Audit log output stored in the **Log Output Directory** field.

Click **Restore Default** to restore the Select Audit defaults.

28 Click **Next**. The **Mail Configuration** screen opens.



Please enter your mail server settings below to configure notification for reporting and attestation workflow.

Mail Server

Sender Address (Workflow) select-audit-workflow@localhost

Sender Address (Reports) select-audit-reports@localhost

**Note: be sure to configure the sender address fields to a valid address that will not be rejected by your mail server.**

29 Complete the screen as follows:

- Type your mail server name in the **Mail Server** field.
- Type a valid email address for where workflows are sent from in the **Sender Address (Workflow)** field.

- Type a valid email address for where report notifications are sent from in the **Sender Address (Reports)** field.

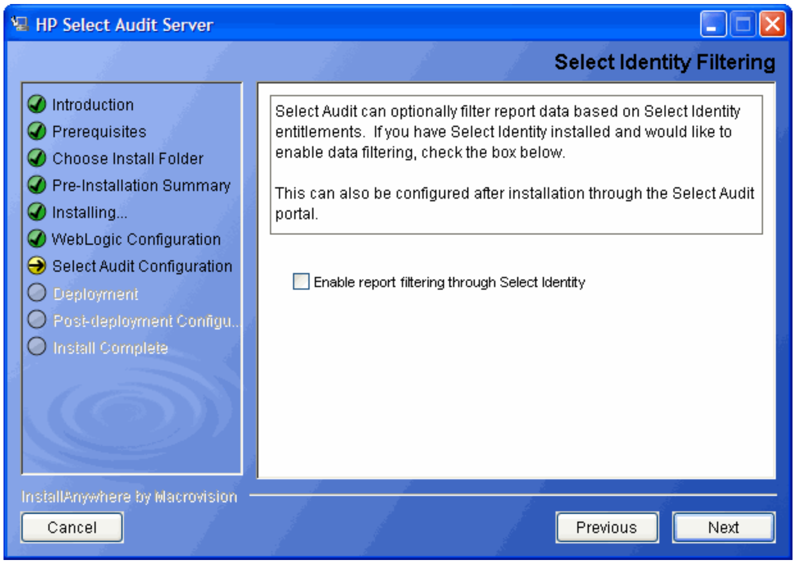
**Mail Server** and **Sender Address (Workflow)** entries are stored in a `workflow.properties` file as:

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

`workflow.properties` is located in `<install_dir>/dist/config/properties`.

An invalid **Sender** address may be rejected by your SMTP server which will lead to a workflow email notification failure. To change the SMTP server and/or the **Sender** address, update these entries manually and restart the application server.

30 Click **Next**. The **Application Configuration** Select Identity filtering screen opens.



Select Audit can optionally filter report data based on Select Identity entitlements. If you have Select Identity installed and would like to enable data filtering, check the box below.

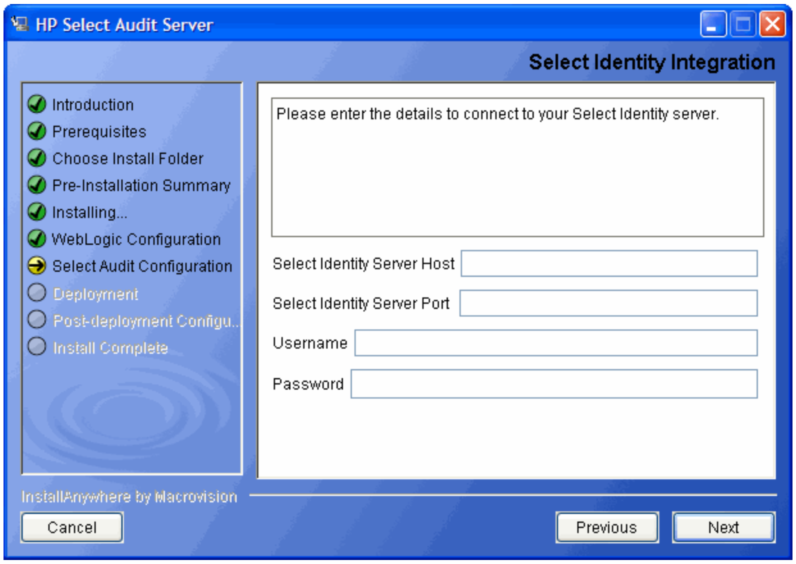
This can also be configured after installation through the Select Audit portal.

□ Enable report filtering through Select Identity

31 Select the **Enable report filtering through Select Identity** check box to filter report data based on Select Identity entitlements. Refer to the *HP Select Audit 1.02 Administration Guide* for more information about integrating Select Audit with Select Identity.

32 Do one of the following:

- Click **Next** if you chose to integrate with Select Identity. The **Select Identity Integration** screen opens.
- If you chose not to integrate with Select Identity, go to step 36.

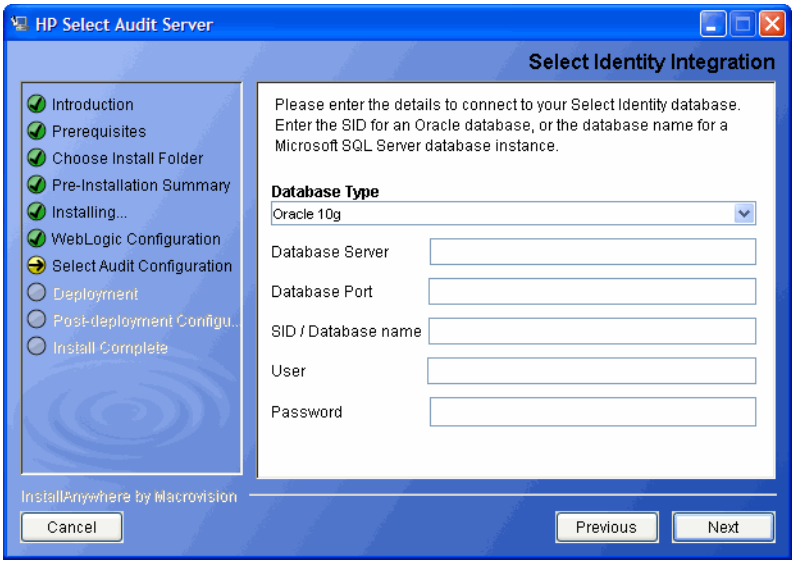


Please enter the details to connect to your Select Identity server.

33 Complete the screen as follows:

- Type the Select Identity server host name in the **Select Identity Server Host** field.
- Type the Select Identity port number in the **Select Identity Server Port** field.
- Type the Select Identity server user name in the **Username** field.
- Type the Select Identity server password in the **Password** field.

34 Click **Next**. The **Select Identity Integration** database configuration screen opens.



Please enter the details to connect to your Select Identity database. Enter the SID for an Oracle database, or the database name for a Microsoft SQL Server database instance.

Database Type: Oracle 10g

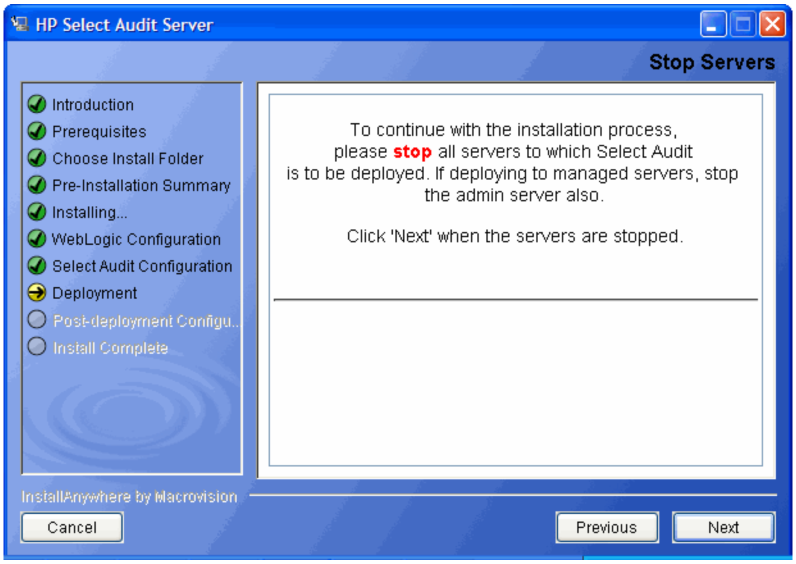
35 Complete the screen as follows:

- Select a database type from the **Database Type** drop-down list.
- Type the Select Identity database server address in the **Database Server** field.
- Type the Select Identity database listener port number in the **Database Port** field.
- If you are using an Oracle database, type the SID in the **SID/Database name** field.
- If you are using an MSSQL database, type the database name in the **SID/Database Name** field.

- Type the Select Identity user name in the **User** field.
- Type the Select Identity password in the **Password** field.

36 Click **Next**. The installer then configures the Audit Server.

When the installer has configured the Audit Server, the **Stop Servers** screen opens.



To continue with the installation process, please **stop** all servers to which Select Audit is to be deployed. If deploying to managed servers, stop the admin server also.

Click 'Next' when the servers are stopped.

### Clustered Environments

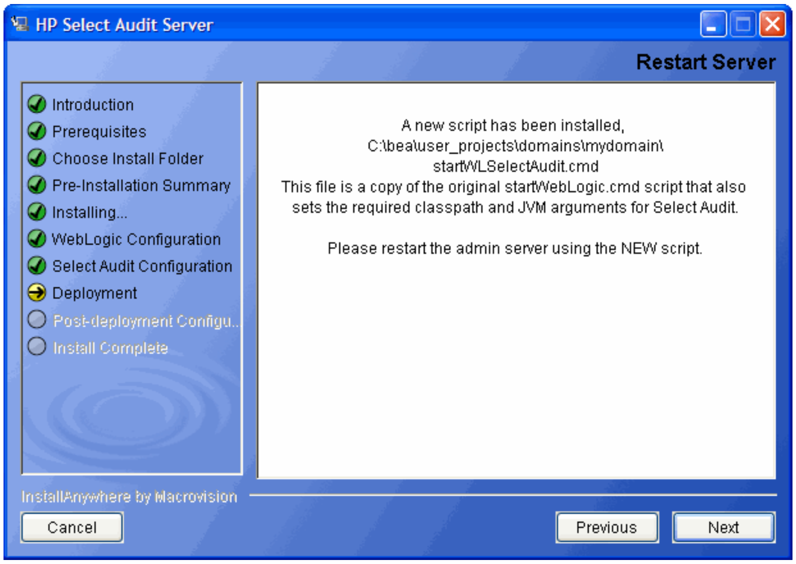
For proper functioning in clustered environments, remote start attributes need to be set for each managed server.

Change the `vde.aclcheck` 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.

37 Stop the WebLogic server.

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

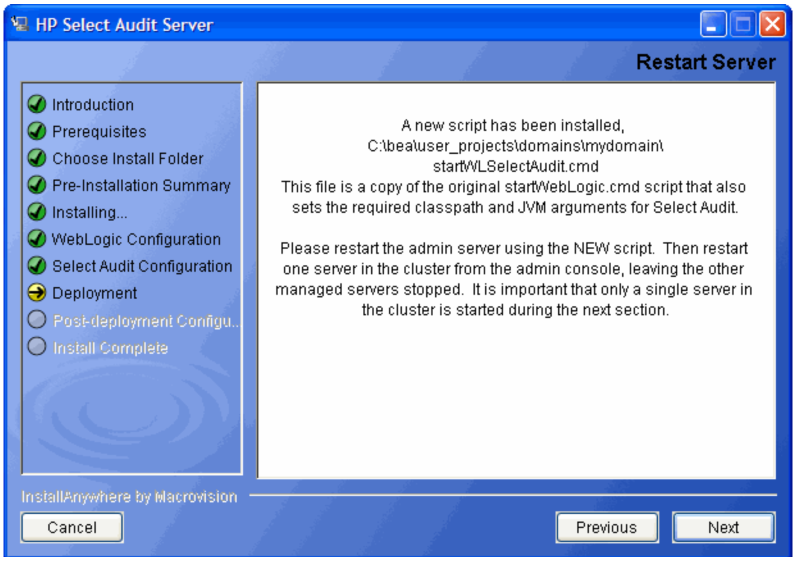
38 Click **Next**. When the installer confirms the server has stopped and it has performed offline processing, the **Restart Server** screen opens.



A new script has been installed,
C:\bea\user_projects\domains\mydomain\
startWLSelectAudit.cmd
This file is a copy of the original startWebLogic.cmd script that also sets the required classpath and JVM arguments for Select Audit.

Please restart the admin server using the NEW script.

If you are running a cluster, when the installer confirms the servers in the cluster have stopped, the **Restart Server Cluster** screen opens.



A new script has been installed,
C:\bea\user_projects\domains\mydomain\
startWLSelectAudit.cmd
This file is a copy of the original startWebLogic.cmd script that also sets the required classpath and JVM arguments for Select Audit.

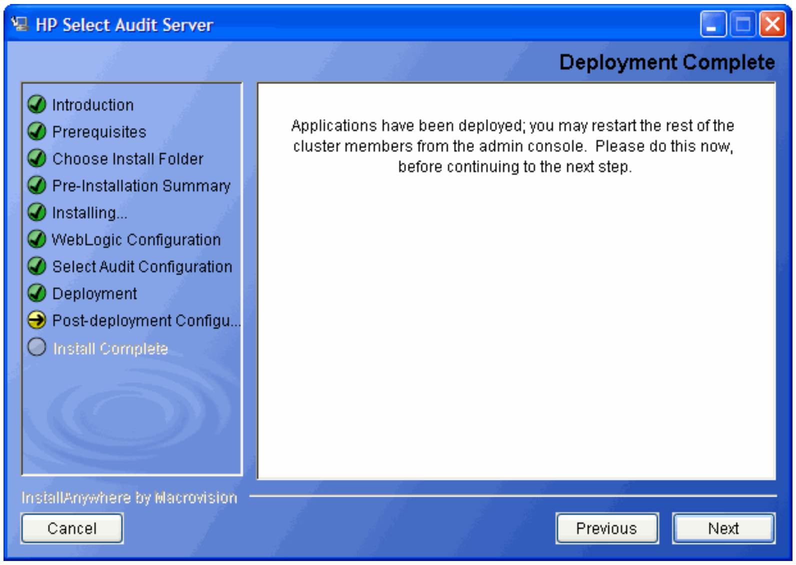
Please restart the admin server using the NEW script. Then restart one server in the cluster from the admin console, leaving the other managed servers stopped. It is important that only a single server in the cluster is started during the next section.

39 Restart the WebLogic server using `startWLSelectAudit.cmd`.

A new script, `startWLSelectAudit.cmd`, is installed under the `bea\user_projects\domains\<your domain>` directory. This script sets the required classpath and JVM arguments. The script is a copy of the original `startWebLogic.cmd` startup script with the new values added.

### Clustered Environments

If you are running a cluster, start the Administration server first and then a single managed server in the cluster, leaving the rest of the cluster members stopped. After deployment, the **Deployment Complete** screens opens.

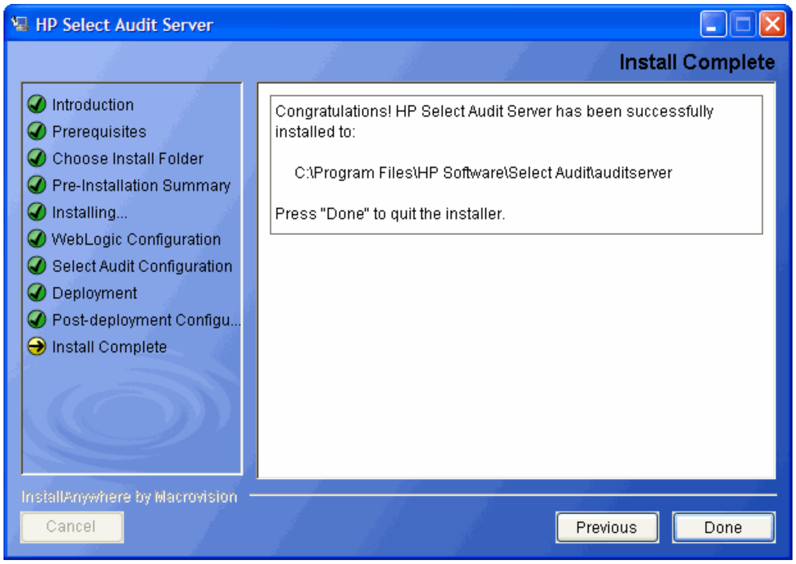


Applications have been deployed; you may restart the rest of the cluster members from the admin console. Please do this now, before continuing to the next step.

Restart the other servers in the cluster.

40 Click **Next**. The installer performs the final Audit Server configuration.

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



Congratulations! HP Select Audit Server has been successfully installed to:

C:\Program Files\HP Software\Select Audit\auditserver

Press "Done" to quit the installer.

42 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 `WARN`, except for the custom `SA_AUDITOR` loggers, which should remain set to `INFO`. To enable logging to the Console or a file, change the appropriate logger 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.

## 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, for example, `C:\WINDOWS\Fonts\ArialUni.ttf`.

   b. Create a new folder, for example, `c:\fop` and change directories to 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 code to the file:

```
<!-- <!DOCTYPE configuration SYSTEM "config.dtd"> -->
<configuration>
  <entry>
  <key>fontBaseDir</key>
  <value>C:\fop</value>
  </entry>
  <fonts>
    <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>
  </fonts>
</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`, type the location of your `config` file created in Register Fonts with FOP, for example:

```
<Property name="fopConfigFile">C:\\fop\\userconfig.xml</Property>
```

b For `fopFont`, type the name of the font you specified in that `config` file, for example:

➤ 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.

# Uninstalling the Audit Server

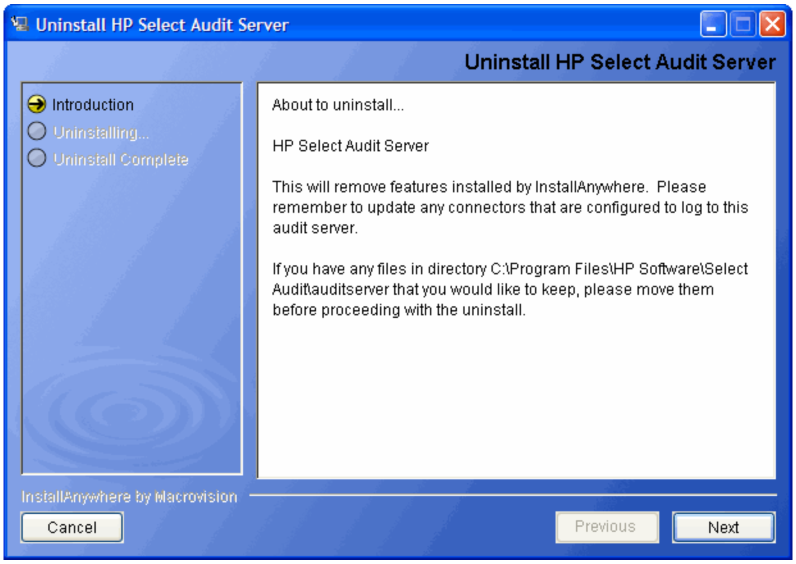
Audit Server uninstaller executables are created on the machine where the Audit Server is installed during the Server installation. After installing the Audit Server on Windows, there is an `Uninstall_Select_Audit` folder under the `C:\Program Files\HP Software\Select Audit` directory. This folder contains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

⚠ If you are installing, uninstalling 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 `/HP Software/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 Software\Select Audit\auditserver\Uninstall_Select_Audit` directory. The **Select Audit Uninstall Introduction** screen opens.


Uninstall HP Select Audit Server
Uninstall HP Select Audit Server
Introduction
Uninstalling...
Uninstall Complete
InstallAnywhere by Macrovision
Cancel
Previous
Next

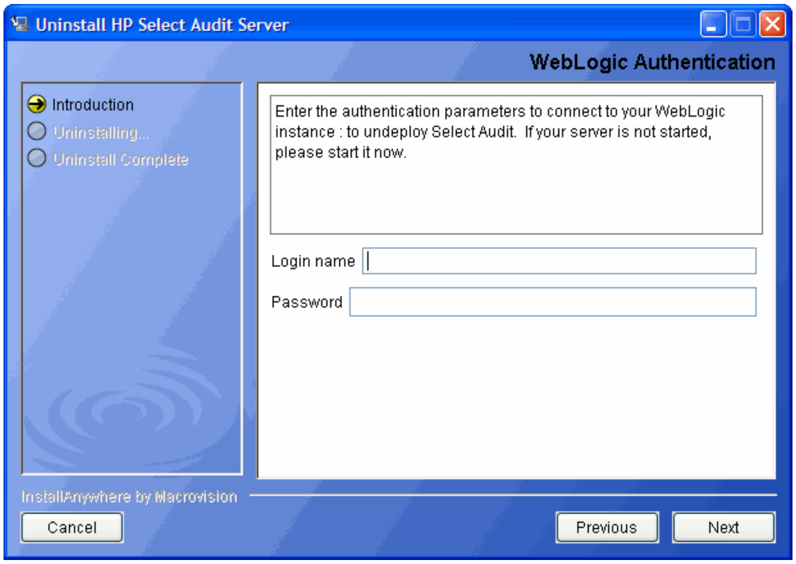
About to uninstall...

HP Select Audit Server

This will remove features installed by InstallAnywhere. Please remember to update any connectors that are configured to log to this audit server.

If you have any files in directory C:\Program Files\HP Software\Select Audit\auditserver that you would like to keep, please move them before proceeding with the uninstall.

2 Click **Next**. The **WebLogic Authentication** screen opens.



Enter the authentication parameters to connect to your WebLogic instance : to undeploy Select Audit. If your server is not started, please start it now.

Login name

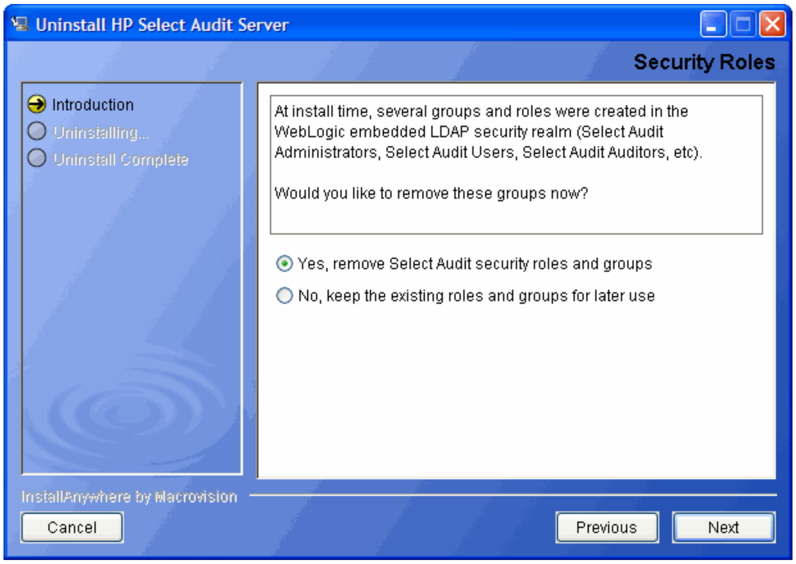
Password

3 Type the Server administrator name in the **Login name** field and Server administrator password in the **Password** field in the corresponding fields. This user must have privileges to undeploy and remove services on the domain.

The WebLogic server must be running to properly uninstall Select Audit.

4 Click **Next**. The **Stop Servers** screen opens.

5 Stop all servers and click **Uninstall**. The **Security Roles** screen opens.



At install time, several groups and roles were created in the WebLogic embedded LDAP security realm (Select Audit Administrators, Select Audit Users, Select Audit Auditors, etc).

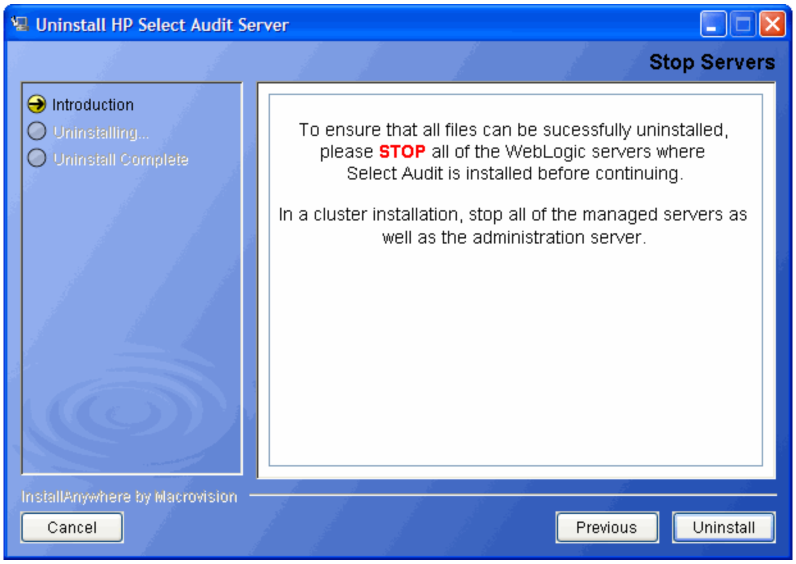
Would you like to remove these groups now?

● Yes, remove Select Audit security roles and groups

○ No, keep the existing roles and groups for later use

6 Select whether to remove the groups and roles created by the installer or to keep them for later use.

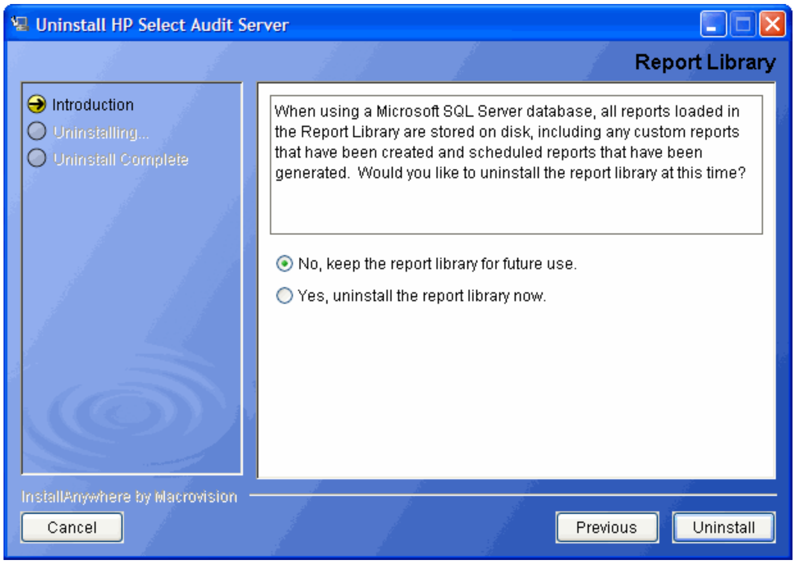
7 Click **Next**. The **Stop Servers** screen opens.



To ensure that all files can be sucessfully uninstalled, please **STOP** all of the WebLogic servers where Select Audit is installed before continuing.

In a cluster installation, stop all of the managed servers as well as the administration server.

8 Stop the servers and click **Uninstall**. If you are using MSSQL, the **Report Library** screen opens, otherwise, go to step 10.



When using a Microsoft SQL Server database, all reports loaded in the Report Library are stored on disk, including any custom reports that have been created and scheduled reports that have been generated. Would you like to uninstall the report library at this time?

● No, keep the report library for future use.

○ Yes, uninstall the report library now.

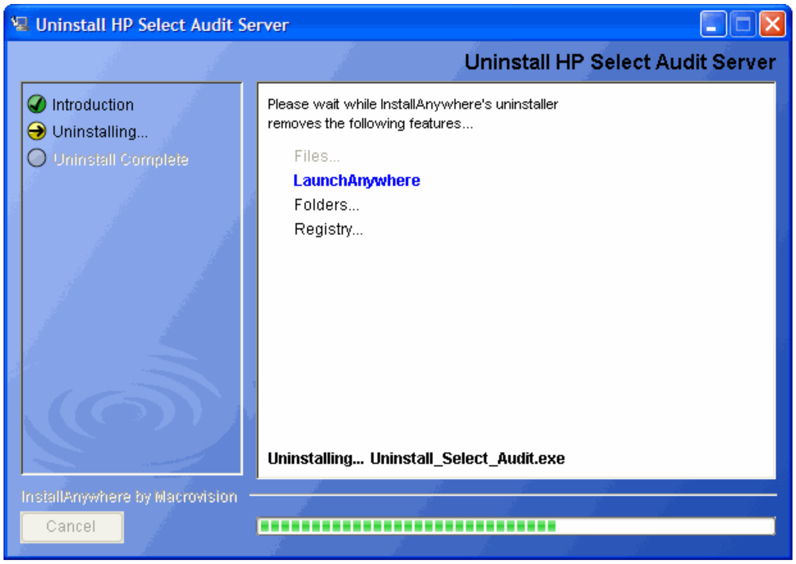
When using a Microsoft SQL Server database, all reports loaded in the Report Library are stored on disk, including any custom reports that have been created and scheduled reports that have been generated.

9 Do one of the following:

- Click **Yes** to uninstall the Report Library, including all custom reports and schedules permanently.
- Click **No** to leave any custom reports on disk to be restored later.

10 Click **Uninstall**. The **Uninstall HP Select Audit Server** screen opens.

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

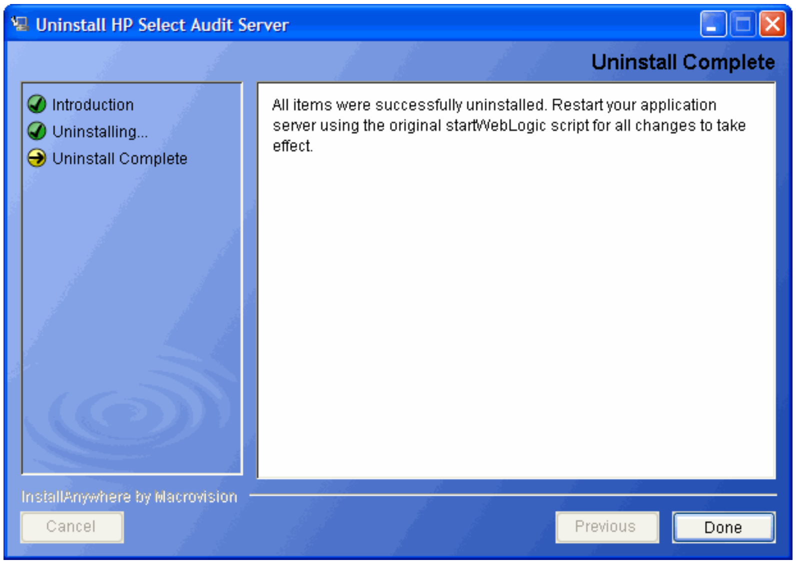

Uninstall HP Select Audit Server
Uninstall HP Select Audit Server
Introduction
Uninstalling...
Uninstall Complete
InstallAnywhere by Macrovision
Cancel

Please wait while InstallAnywhere's uninstaller removes the following features...

Files...
LaunchAnywhere
Folders...
Registry...

Uninstalling... Uninstall_Select_Audit.exe

The uninstaller removes the Select Audit features. When the Audit Server is uninstalled, the **Uninstall Complete** screen opens.



All items were successfully uninstalled. Restart your application server using the original startWebLogic script for all changes to take effect.

11 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.

12 Restart the application server using the original `startWebLogic` script so that the changes take effect.

# 4 Installing Select Audit on WebSphere

This chapter provides an overview of how to install and uninstall the Select Audit components on WebSphere.

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.

## WebSphere Installer Prerequisites

Before you run the WebSphere Audit Server installer, ensure that you have completed the prerequisites listed in this section.

### Database Setup

Set up your database using the steps described in Setting Up The Database Schemas on page 15 for your Oracle or MSSQL database

### Server Setup

For the WebSphere application server, HP recommends that you make sure there is enough permanent memory allocated on the system. The `MaxPermSize` parameter should be set at 25% from the JVM's heap size.

1. Create a new WebSphere profile by launching `IBM/WebSphere/AppServer/firststeps/firststeps.bat` and following the directions to create a new application server profile.
2. Copy the `soap.jar` and `js.jar` files from the Select Audit CD to the WebSphere `lib` directory: `<WebSphere_Install_Dir>/IBM/WebSphere/AppServer/lib`.

   ➤ If you are installing Select Audit on a WebSphere cluster, copy the `soap.jar` file to every server in the cluster.

3. Start the server.
4. Open the WebSphere Administration console at `http://localhost:9060/ibm/console`.

5 Click **Security** → **Global Security**.

6 Click **User registries** → **LDAP** and configure an LDAP user registry using the following settings for your LDAP server:

- Server user ID
- Server user password
- Type
- Host
- Port
- Base distinguished name (DN)
- Bind distinguished name (DN)
- Bind password

7 For SunOne LDAP setup, do the following:

a Click **Advanced Lightweight Directory Access Protocol (LDAP) user registry setting**.

b Change the value in the **Group member ID map** field to `groupofuniquenames:uniquemember`.

c Change the value in the **Group Filter** field to `(&(cn=%v)(objectclass=groupofuniquenames))`.

8 Click **OK** and then **Save** to save your changes.

9 Click **Authentication** → **Authentication mechanisms** → **LTPA**.

10 Type the LTPA password and retype it to confirm the entry. This password is used to generate a key.

11 Change the **Timeout** from 120 minutes to 20 minutes. This means that redirecting to the Report server from the Audit Portal will be timed out after 20 minutes.

> If you are not using fixpack 17, you may need to do the below step, otherwise you can ignore it. Under **Global Security** → **Authentication** → **Authentication mechanisms** → **LTPA** → **Trust Association**, select the **Enable trust association** check box.

12 Click **OK** and then **Save**.

13 Click **Security** → **Global Security**.

14 Select the **Enable global security** check box. Selecting this check box automatically selects **Enforce Java 2 Security**.

15 Select **LTPA** from the **Active Authentication mechanism** drop-down list.

16 Select LDAP from the **Active user registry** drop-down list.

17 Click **OK** and then **Save**.

18 When installing Select Audit in a cluster, make sure you restart the node on each application server profile with the proper credentials, once global security has been enabled.

> These credentials are the user name and password specified in the **Server user ID** and **Server user password** fields in step 6.

### Create Groups in LDAP

Create the following groups in your LDAP directory:

- Select Audit Administrators
- Select Audit Users
- Select Audit Auditors

These groups are required by the Audit Server installer to map the corresponding roles to the groups.

### Edit the server.policy File

When Java 2 Security is enabled as described above, you must also edit the `<profile>/properties/server.policy` file. This can be done manually or through the Policy Tool.

1. Append these lines to the end of the file configured with the location where you will install Select Audit:

```
//grant permissions for custom service

grant codeBase "file:/<install_directory>/HP Software/Select Audit/
auditserver/dist/lib/-" {

  permission java.security.AllPermission;

};
```

2. Save the file and restart your server.

You are now ready to install Select Audit to the directory specified in `server.policy`.

#### Clustered Environments

The `server.policy` file for each application server profile that is part of the cluster needs to be updated.

Once the file has been saved, all application server profiles and the Deployment Manager profile need to be restarted.

## Installing 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 `SelectAuditServerInstallWS.exe`.

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

     ⚠ If you are installing, uninstalling 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

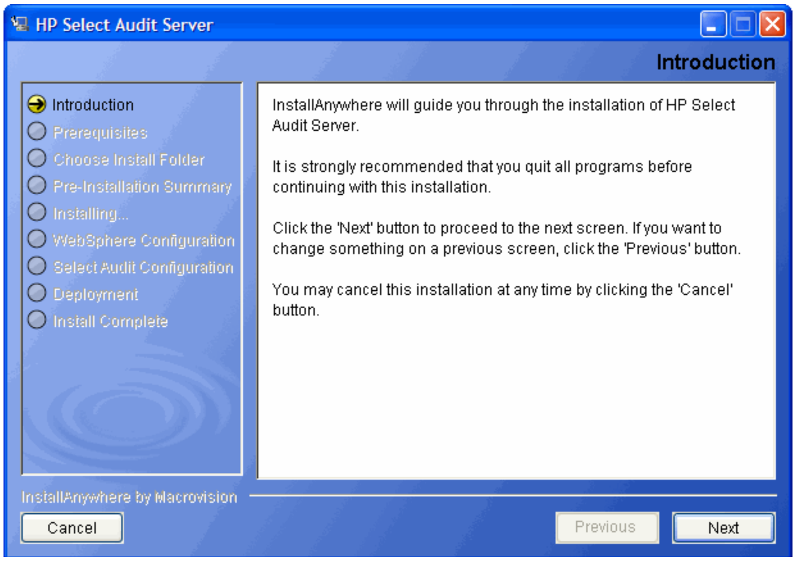
- **On HP-UX, Linux or Solaris:**

  Type the following command:

  `./SelectAuditServerInstallWS.bin.`

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

The installer extracts the installation files and then prepares the Select Audit Install wizard. When it has finished loading, the **Server Installer Introduction** screen opens.



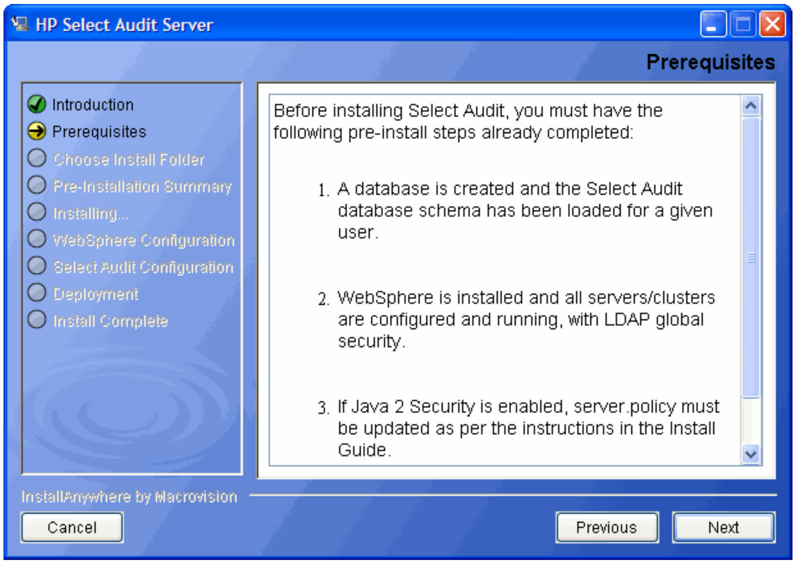
InstallAnywhere will guide you through the installation of HP Select Audit Server.

It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

2 Click **Next**. The **Prerequisites** screen opens.

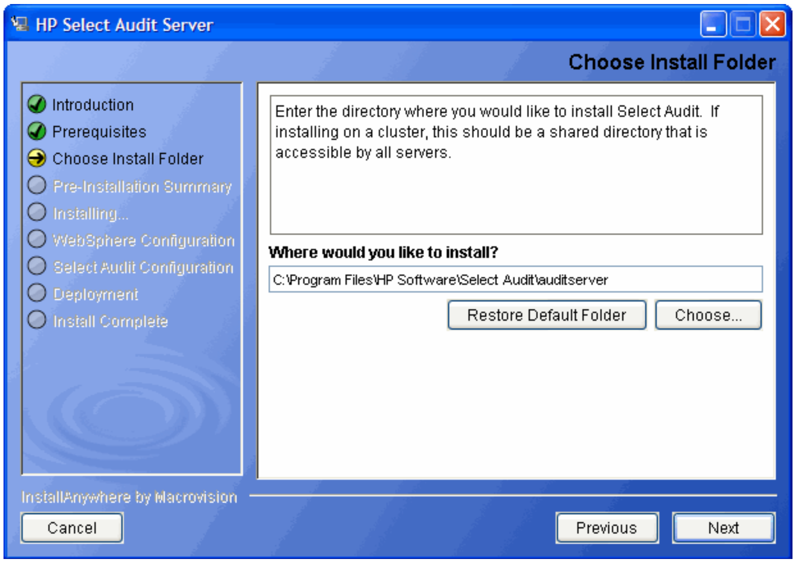


Before installing Select Audit, you must have the following pre-install steps already completed:

1. A database is created and the Select Audit database schema has been loaded for a given user.
2. WebSphere is installed and all servers/clusters are configured and running, with LDAP global security.
3. If Java 2 Security is enabled, server.policy must be updated as per the instructions in the Install Guide.

3 Review the listed prerequisites and confirm they have been met before proceeding.

4 Click **Next**. The **Choose Install Folder** screen opens.



Choose Install Folder

Enter the directory where you would like to install Select Audit. If installing on a cluster, this should be a shared directory that is accessible by all servers.

**Where would you like to install?**

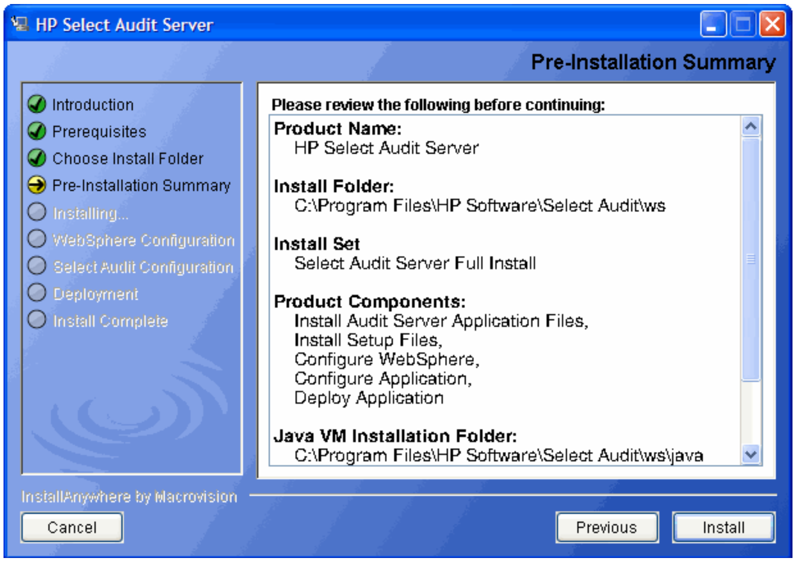
C:\Program Files\HP Software\Select Audit\auditserver

5 Select the location where you wish to install the Audit Server. If you are installing on a cluster, use a directory that is accessible by all servers.

> When specifying Select Audit installation path, make sure to specify the mounted filesystem to ensure consistent paths on both the WebSphere Administration server as well as managed servers.

6 Click **Next**. The **Pre-Installation Summary** screen opens.

> The following characters are not valid in file or folder names when specifying where to install the Audit Server:
>
> `( ) { } [ ] / \ : ; " ' < > | $ * ? # &,`



Pre-Installation Summary

**Please review the following before continuing:**

**Product Name:**
HP Select Audit Server

**Install Folder:**
C:\Program Files\HP Software\Select Audit\ws

**Install Set**
Select Audit Server Full Install

**Product Components:**
Install Audit Server Application Files,
Install Setup Files,
Configure WebSphere,
Configure Application,
Deploy Application

**Java VM Installation Folder:**
C:\Program Files\HP Software\Select Audit\ws\java

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

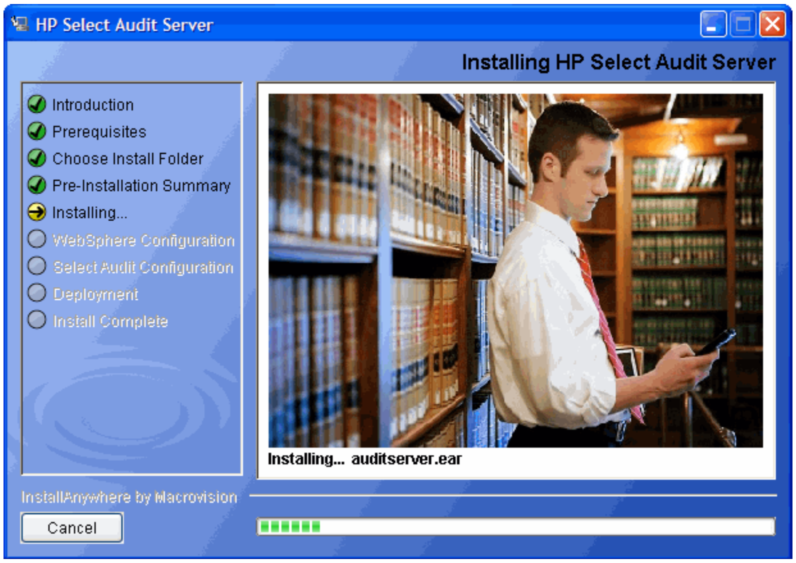
- The installation folder you chose to install the Audit Server in.
- The installation set.

- The components that will be installed.
- The installation location of the Java Virtual Machine that the Select Audit Install wizard has automatically installed.
- 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.

7 Review the information on the **Pre-Installation Summary** screen. If the information is correct, click **Install**.

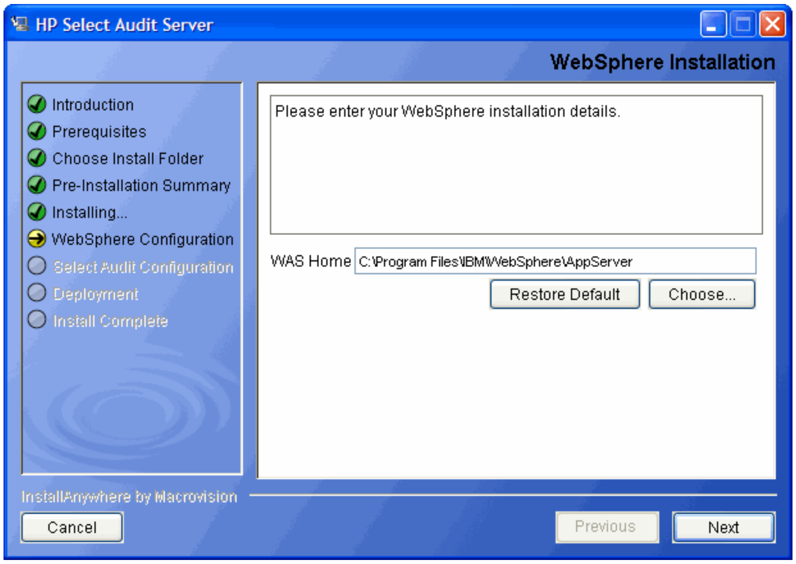
> To change any of the installation settings, click **Previous** to return to the screen containing the settings you want to change.

The Audit Server begins to install and the **Server Installation Progress** screen opens.



Installing... auditserver.ear

When the Audit Server installer is finished, the **WebSphere Installation** screen opens.

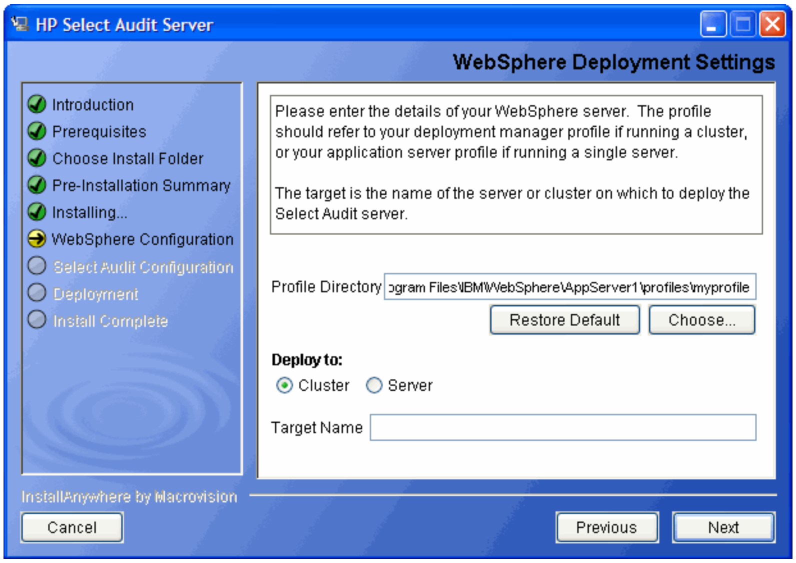


Please enter your WebSphere installation details.

WAS Home C:\Program Files\IBM\WebSphere\AppServer

8 If the default WAS location is incorrect, select your WebSphere home directory by clicking **Choose** below the **WAS Home** field.

9 Click **Next**. The **WebSphere Deployment Settings** screen opens.



Please enter the details of your WebSphere server. The profile should refer to your deployment manager profile if running a cluster, or your application server profile if running a single server.

The target is the name of the server or cluster on which to deploy the Select Audit server.

Profile Directory: ɔgram Files\IBM\WebSphere\AppServer1\profiles\myprofile

**Deploy to:**
● Cluster ○ Server

Target Name:

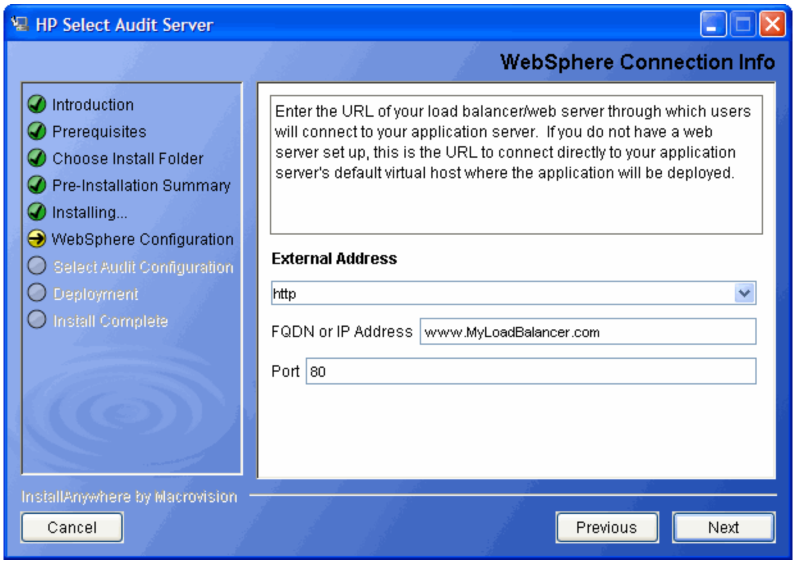
10 Do the following:

- In the **Profile Directory** field, type the application server profile if you are running a single server or the Deployment Manger profile if you are running a cluster.

  Click **Restore Default** to restore the Select Audit defaults.

- Select whether you want to deploy Select Audit to a cluster or single server under the **Deploy to:** section.
- Type the server or cluster name in the **Target Name** field.

11 Click **Next**. The **WebSphere Connections Info** screen opens.



Enter the URL of your load balancer/web server through which users will connect to your application server. If you do not have a web server set up, this is the URL to connect directly to your application server's default virtual host where the application will be deployed.

**External Address**

http

FQDN or IP Address: www.MyLoadBalancer.com

Port: 80

12 Do the following:

- Select an address type from the **External Address** drop-down list.

- Type the URL that external 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.

➤ If you are installing on a cluster, see Enabling Load Balancing for Clusters on page 61 for more information.

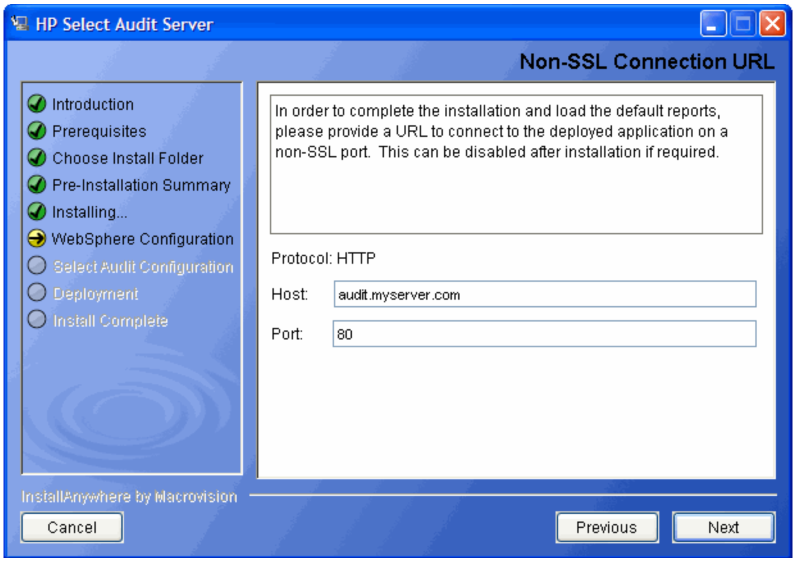
- Type the port number of the external address in the **Port** field.

13 If you selected `https` for the **External Address** type, the **Non-SSL Connection URL** screen opens.

Reports must be loaded through an `http://` SOAP call. A non-SSL connection is required to complete the installation. The `http` connection URL is not used again once the installation is complete.

➤ Import the CA certificate to the `cacerts` file used as the trust store for your Java Virtual machine. You can often use the keytool utility to do this:

```
keytool -import -alias <CA_Alias> -file <path/to/ca.der>
-keystore <path/to/cacerts_file> -storepass <password>
```



In order to complete the installation and load the default reports, please provide a URL to connect to the deployed application on a non-SSL port. This can be disabled after installation if required.

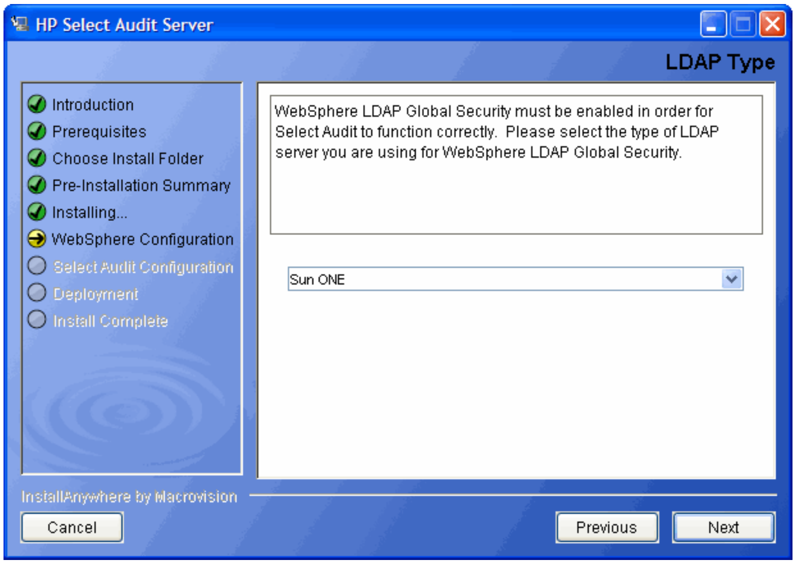
Protocol: HTTP

Host: audit.myserver.com

Port: 80

14 Type the non-SSL host name in the **Host** field and the non-SSL port number in the **Port** field.

15 Click **Next**. The **LDAP Type** screen opens.

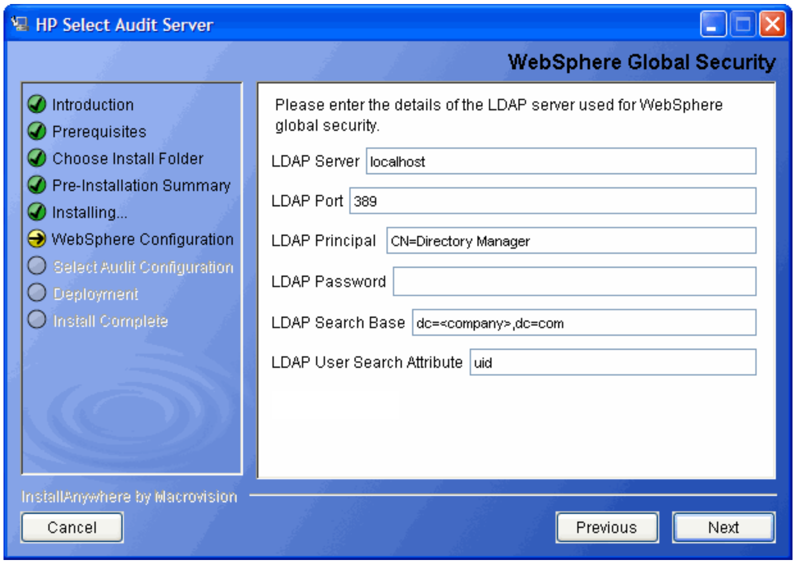


WebSphere LDAP Global Security must be enabled in order for Select Audit to function correctly. Please select the type of LDAP server you are using for WebSphere LDAP Global Security.

Sun ONE

16 Select your LDAP server type from the drop-down list.

17 Click **Next**. The **WebSphere Global Security** screen opens.



Please enter the details of the LDAP server used for WebSphere global security.

LDAP Server localhost

LDAP Port 389

LDAP Principal CN=Directory Manager

LDAP Password

LDAP Search Base dc=<company>,dc=com

LDAP User Search Attribute uid

18 Do the following:

a Type the name of the LDAP server in the **LDAP Server** field.

b Type the port number of the LDAP server in the **LDAP Port** field.

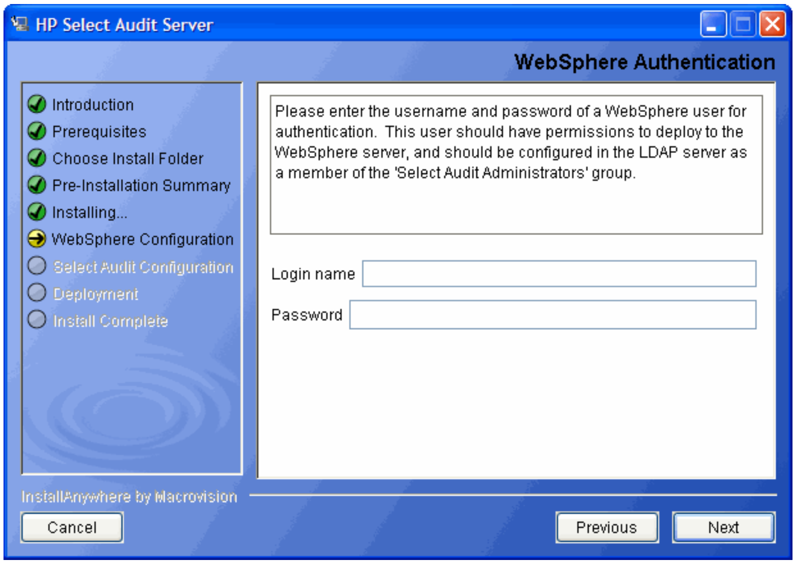
c Type the cn name of the LDAP server in the **LDAP Principal** field.

d Type the password for the LDAP server in the **LDAP Password** field.

e Type the base DN for the server, broad enough to cover both groups and users, in the **LDAP Search Base** field.

f Type the attribute that uniquely identifies a user in the **LDAP User Search Attribute** field.

19 Click **Next**. The **WebSphere Authentication** screen opens.



Please enter the username and password of a WebSphere user for authentication. This user should have permissions to deploy to the WebSphere server, and should be configured in the LDAP server as a member of the 'Select Audit Administrators' group.

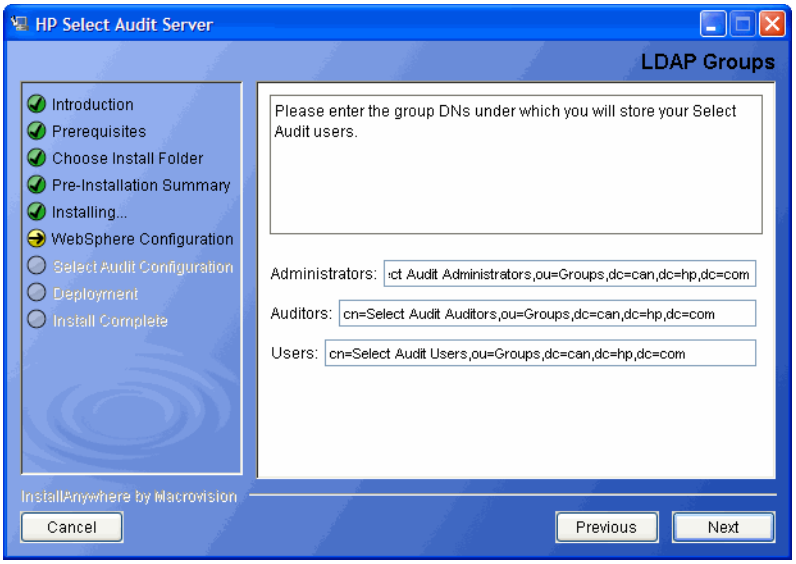
Login name

Password

20 Type the user name and password of a user with permission to deploy and create services on the domain.

This user should be a member of the Select Audit Administrators group.

21 Click **Next**. The **LDAP Groups** screen opens.



Please enter the group DNs under which you will store your Select Audit users.

Administrators: :ct Audit Administrators,ou=Groups,dc=can,dc=hp,dc=com

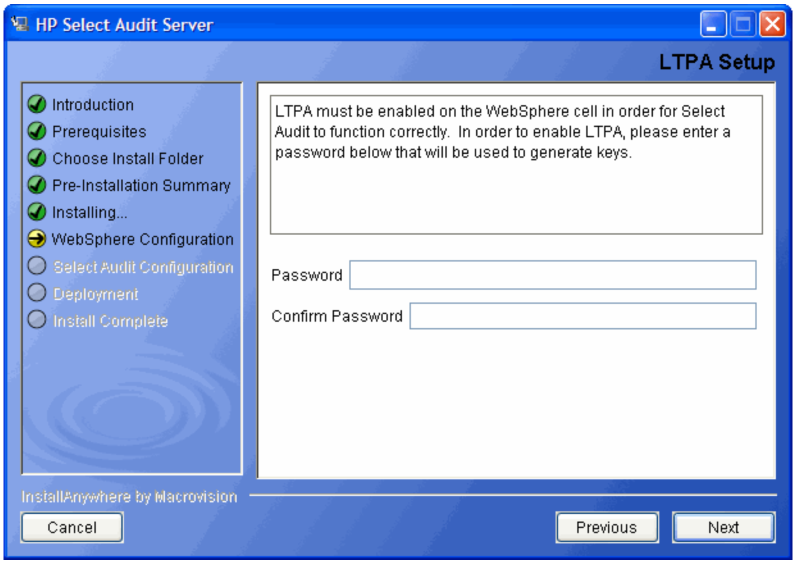
Auditors: cn=Select Audit Auditors,ou=Groups,dc=can,dc=hp,dc=com

Users: cn=Select Audit Users,ou=Groups,dc=can,dc=hp,dc=com

22 Type the group DNs for Select Audit Administrators, Auditors and Users in the appropriate fields.

➤ The group DNs specified should be under the base DN specified in step 21.

23 Click **Next**. If LTPA is already enabled on the domain, go to step 25, otherwise, the **LTPA Setup** screen opens.



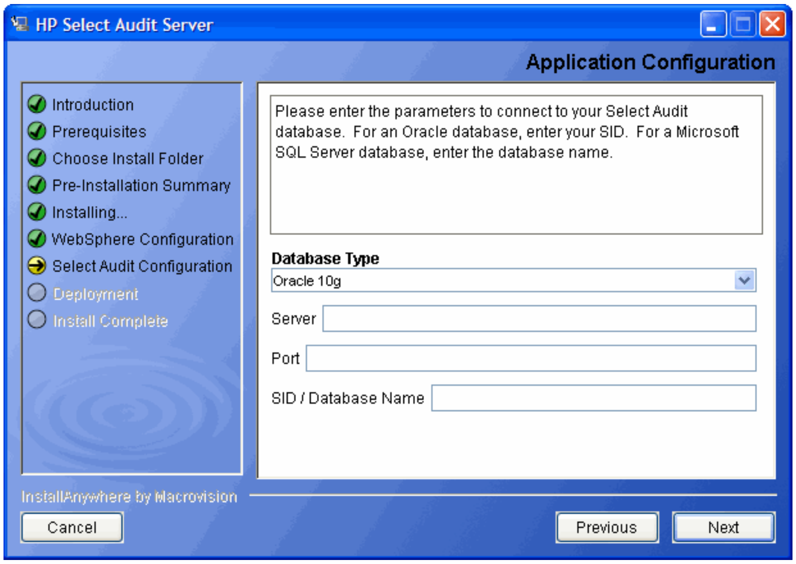
LTPA must be enabled on the WebSphere cell in order for Select Audit to function correctly. In order to enable LTPA, please enter a password below that will be used to generate keys.

Password

Confirm Password

24 Type the LTPA password in the **Password** field and retype it in the **Confirm Password** field.

25 Click **Next**. The installer verifies the settings and configures WebSphere. Once it is finished, the **Application Configuration** screen opens.



Please enter the parameters to connect to your Select Audit database. For an Oracle database, enter your SID. For a Microsoft SQL Server database, enter the database name.

**Database Type**
Oracle 10g

Server

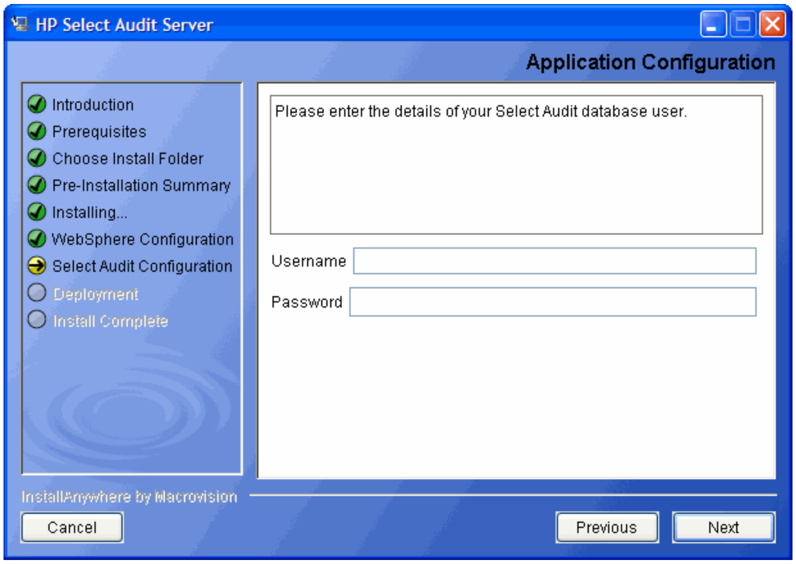
Port

SID / Database Name

26 Enter the database connection parameters as follows:

- Select your database type from the **Database Type** drop-down list.
- Type the database server address in the **Server** field.
- Type the database listener port number in the **Port** field.
- If you are using an Oracle database, type the SID in the **SID/Database Name** field.
- If you are using an MSSQL database, type the database name in the **SID/Database Name** field.

27 Click **Next**. The **Application Configuration** log-on information screen opens.



Please enter the details of your Select Audit database user.

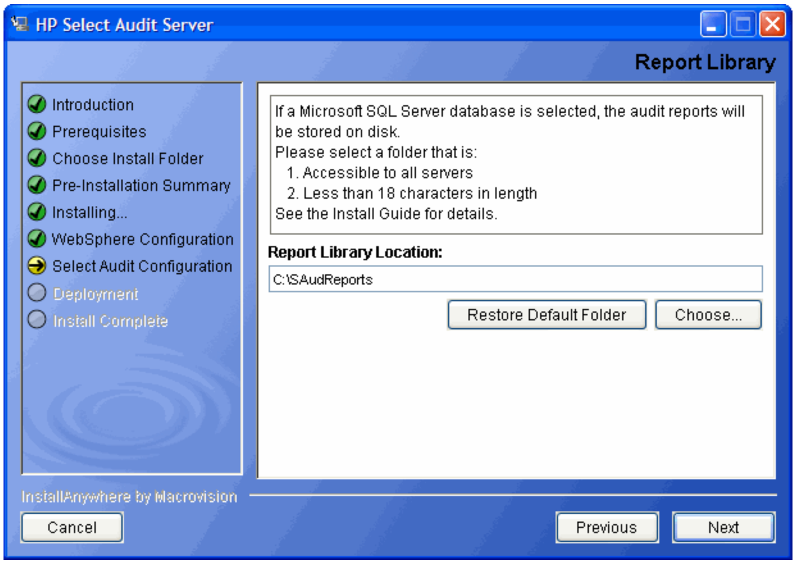
Username

Password

28 Type your database user name in the **Username** field and your database password in the **Password** field.

29 Click **Next**. The installer tests the database connection.

- If you are using Oracle, go to step 31.
- If you are using MSSQL, the **Report Library** screen opens.

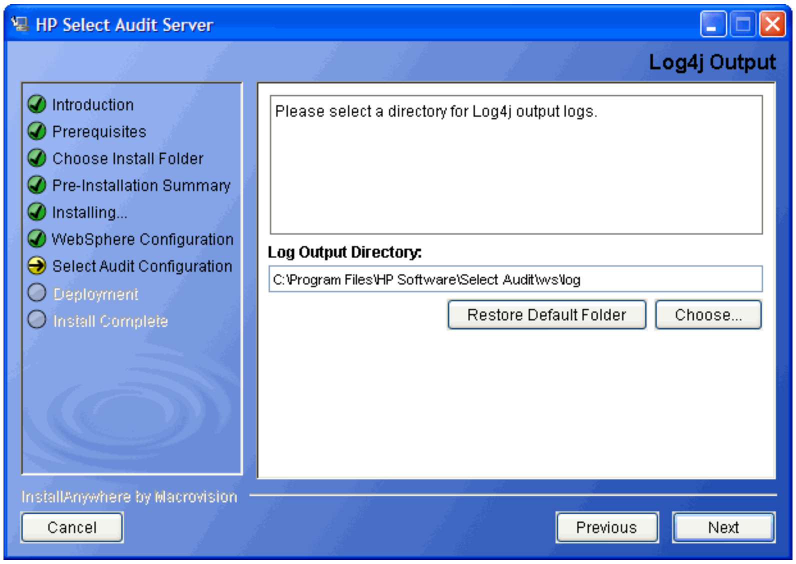


If a Microsoft SQL Server database is selected, the audit reports will be stored on disk.
Please select a folder that is:
1. Accessible to all servers
2. Less than 18 characters in length
See the Install Guide for details.

**Report Library Location:**

C:\SAudReports

30 Select a location for the audit reports and click **Next**. The **Log4J Output** screen opens.



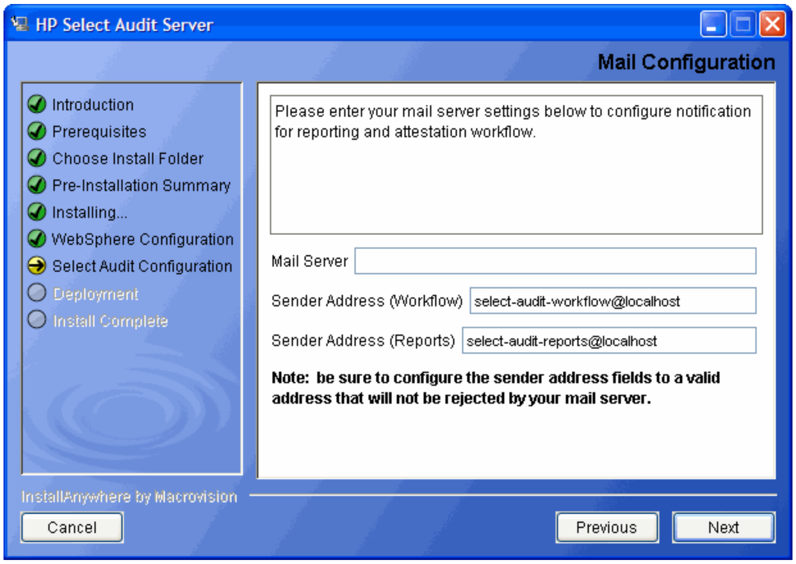
Please select a directory for Log4j output logs.

**Log Output Directory:** C:\Program Files\HP Software\Select Audit\ws\log

31 Click **Choose** or type the directory location where you would like Select Audit log output stored in the **Log Output Directory** field.

> Click **Restore Default** to restore the Select Audit defaults.

32 Click **Next**. The **Mail Configuration** screen opens.



Please enter your mail server settings below to configure notification for reporting and attestation workflow.

Mail Server

Sender Address (Workflow) select-audit-workflow@localhost

Sender Address (Reports) select-audit-reports@localhost

**Note: be sure to configure the sender address fields to a valid address that will not be rejected by your mail server.**

33 Complete the screen as follows:

- Type your mail server name in the **Mail Server** field.
- Type a valid email address for where workflows are sent from in the **Sender Address (Workflow)** field.

- Type a valid email address for where report notifications are sent from in the **Sender Address (Reports)** field.

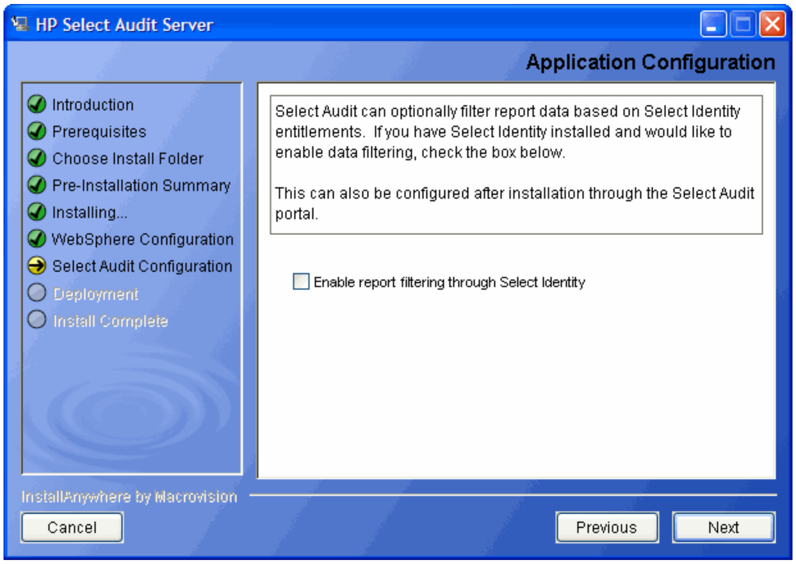
**Mail Server** and **Sender Address (Workflow)** entries are stored in a `workflow.properties` file as:

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

`workflow.properties` is located in `<install_dir>/dist/config/properties`.

An invalid **Sender** address may be rejected by your SMTP server which will lead to a workflow email notification failure. To change the SMTP server and/or the **Sender** address, update these entries manually and restart the application server.

34 Click **Next**. The **Application Configuration** Select Identity filtering screen opens.



Select Audit can optionally filter report data based on Select Identity entitlements. If you have Select Identity installed and would like to enable data filtering, check the box below.

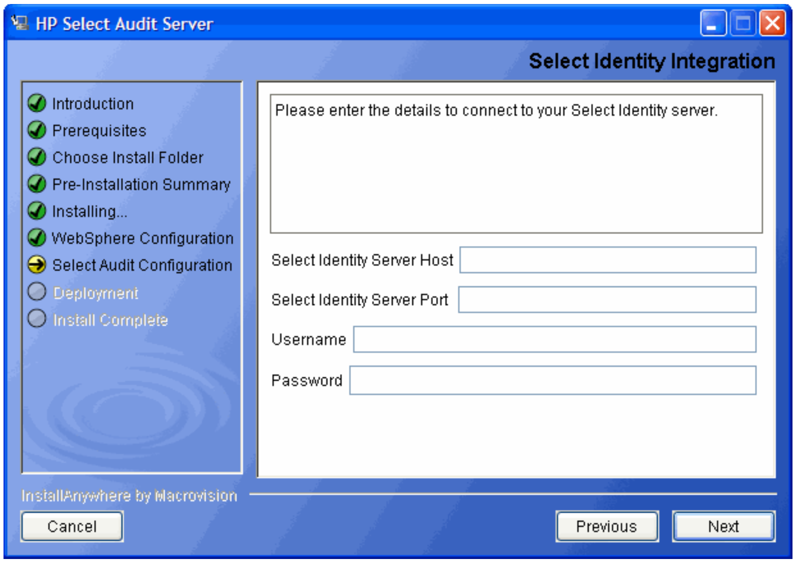
This can also be configured after installation through the Select Audit portal.

□ Enable report filtering through Select Identity

35 Select the **Enable report filtering through Select Identity** check box to filter report data based on Select Identity entitlements. Refer to the *HP Select Audit 1.02 Administration Guide* for more information about integrating Select Audit with Select Identity.

36 Do one of the following:

- Click **Next** if you chose to integrate with Select Identity. The **Select Identity Integration** screen opens.
- If you chose not to integrate with Select Identity, go to step 40.



Please enter the details to connect to your Select Identity server.

Select Identity Server Host

Select Identity Server Port

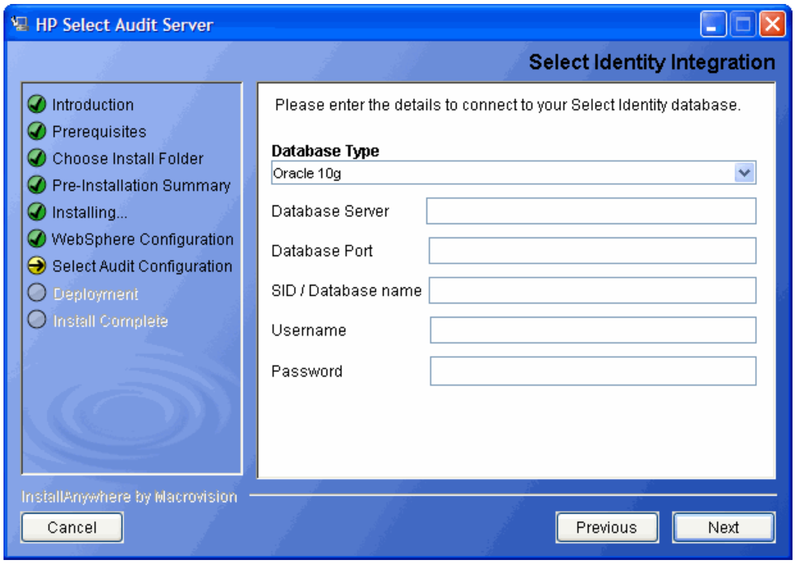
Username

Password

37 Complete the screen as follows:

- Type the Select Identity server host name in the **Select Identity Server Host** field.
- Type the Select Identity port number in the **Select Identity Server Port** field.
- Type the Select Identity server user name in the **Username** field.
- Type the Select Identity server password in the **Password** field.

38 Click **Next**. The **Select Identity Integration** database configuration screen opens.



Please enter the details to connect to your Select Identity database.

Database Type: Oracle 10g

Database Server

Database Port

SID / Database name

Username

Password

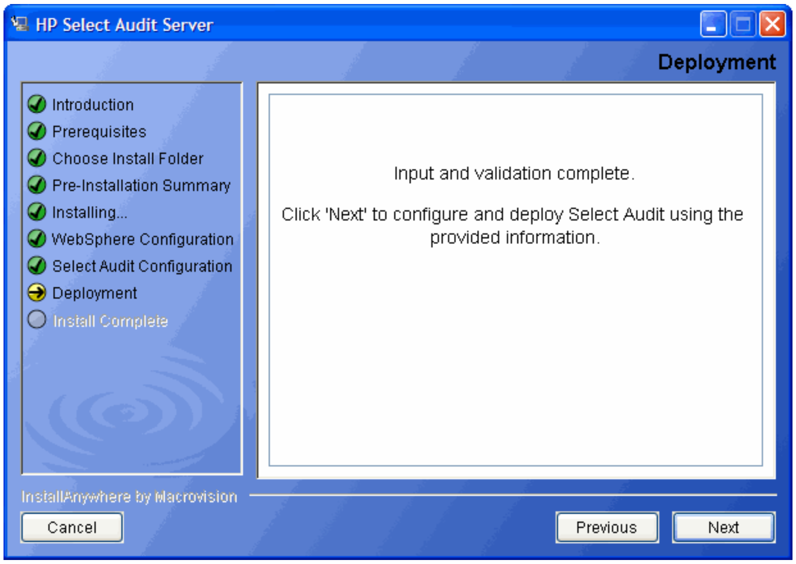
39 Complete the screen as follows:

- Select a database type from the **Database Type** drop-down list.
- Type the Select Identity database address in the **Database Server** field.
- Type the Select Identity port number in the **Database Port** field.
- If you are using an Oracle database, type the Select Identity SID in the **SID/Database Name** field.

- If you are using an MSSQL database, type the Select Identity database name in the **SID/Database Name** field.
- Type the Select Identity database user name in the **Username** field.
- Type the Select Identity database password in the **Password** field.

40 Click **Next**. The installer validates your settings.

If the validation is not successful, click **Previous** and correct your settings. If the validation is successful, the validation is complete the **Deployment** screen opens.

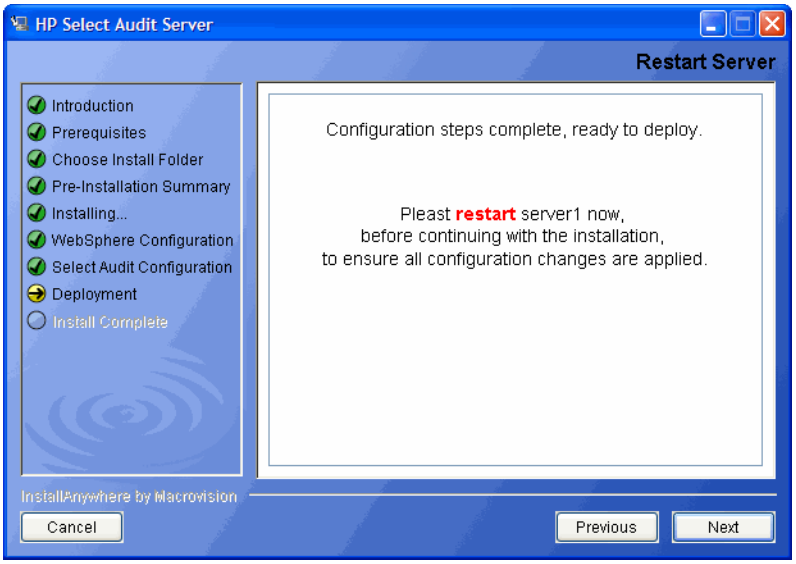


Input and validation complete.

Click 'Next' to configure and deploy Select Audit using the provided information.

41 Click **Next**. The installer configures the Audit Server.

42 When the configuration is complete, the **Restart Server** screen opens.



Configuration steps complete, ready to deploy.

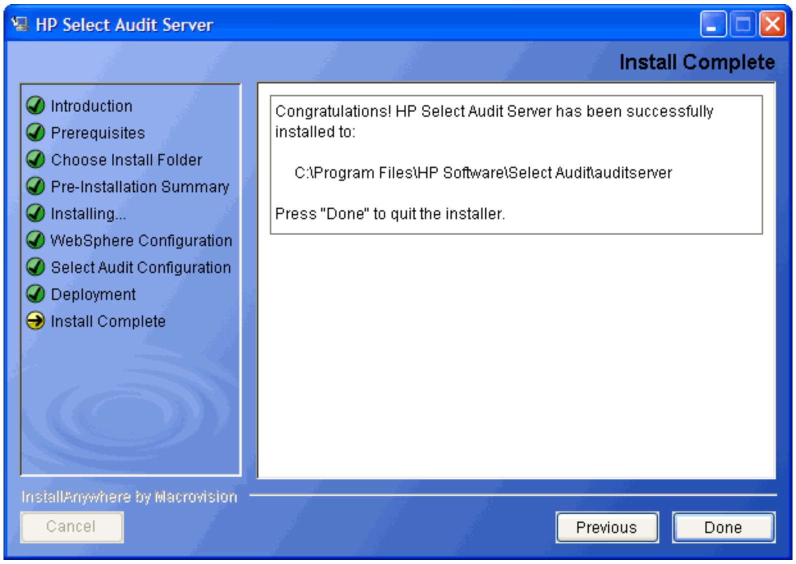
Pleast **restart** server1 now,
before continuing with the installation,
to ensure all configuration changes are applied.

43 Stop and restart the WebSphere server/cluster.

44 Click **Next**.

A prompt opens reminding you to restart the WebSphere server.

45 Click **Yes**. The installer performs the final Audit Server configuration. When the installer has configured the Audit Server, the **Install Complete** screen opens.



Congratulations! HP Select Audit Server has been successfully installed to:

C:\Program Files\HP Software\Select Audit\auditserver

Press "Done" to quit the installer.

46 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 WebSphere (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.

## Enabling Load Balancing for Clusters

If you are installing on a cluster, the load balancer may be configured pre-installation or post-installation, depending on the type of load balancer you are using. If the load balancer is already configured at install time, follow the instructions in the installer to enter the load balancer URL when prompted. No further steps are required.

If the load balancer must be configured post-deployment, enter the URL to connect directly to one of the managed servers, instead of the final load balancer URL on the WebSphere Connection Info screen. See step 12 on page 51 for more information.

After the installation is complete, the load balancer can be enabled by editing the following files:

- In <install_dir>/dist/config/audit_config.xml, the field \AuditConfigServer\LocalServer\Server\ServerHost should contain the base URL of the load balancer, for example:

  ```
  http://audit.myserver.com:80
  ```

- In the file <install_dir>/dist/reporting/ReportServer/SelectAuditReportServer.ear/ReportServer.war/WEB-INF/conf/scopeserver.xml, update the properties "protocol", "host" and "port" to match the load balancer URL, for example:

  ```
  <Property name="protocol">http</Property>
  <Property name="host">audit.myserver.com</Property>
  <Property name="port">80</Property>.
  ```

Restart all servers after making the changes.

## Configuring Log4j

When the Select Audit Server is installed, log4j.properties and commons-logging.properties are installed on the <install_dir>/dist/config/properties/ directory. It is essential that the log4j.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. You may specify only one log4j configuration file per JVM.

### Enabling Logging

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

- DEBUG
- INFO
- WARN
- FATAL

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

### Setting Appenders

Log4j.rootCategory defines the default log behavior for any loggers that are not explicitly defined otherwise. It is set to use both the MAIN file appender, which writes to sa.log, and the CONSOLE appender, which writes out to the Console. All other loggers are descendents of this logger and can be configured to give output from specific modules of the application.

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

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

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

## 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, for example, `C:\WINDOWS\Fonts\ArialUni.ttf`.

b Create a new folder, for example, `c:\fop` and change directories to 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 code to the file:

```
<!-- <!DOCTYPE configuration SYSTEM "config.dtd"> -->
<configuration>
  <entry>
  <key>fontBaseDir</key>
  <value>C:\fop</value>
  </entry>
  <fonts>
    <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>
  </fonts>
</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, type the location of your config file created in Register Fonts with FOP, for example:

```
<Property name="fopConfigFile">C:\\fop\\userconfig.xml</Property>
```

b For fopFont, type the name of the font you specified in that config file, for example:

➤ 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.

## Uninstalling the Audit Server

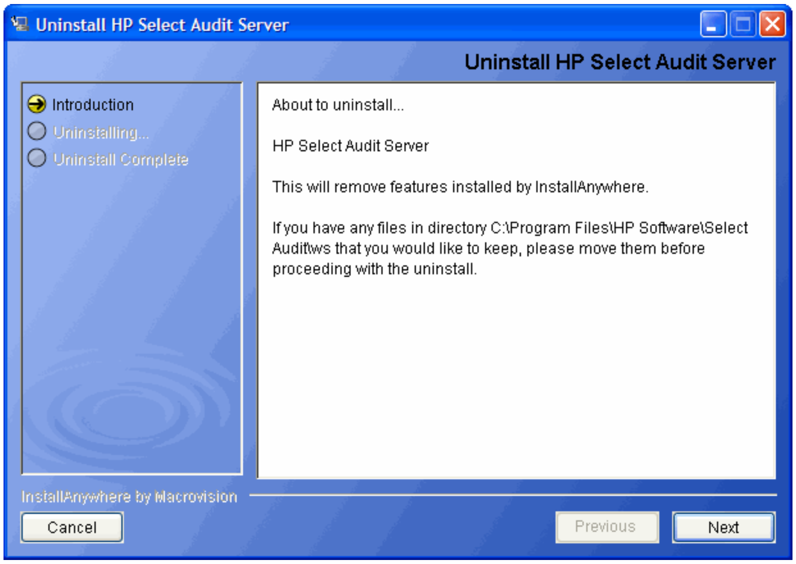
Audit Server uninstaller executables are created on the machine where the Audit Server is installed during the Server installation. After installing the Audit Server on Windows, there is an Uninstall_Select_Audit folder under the C:\Program Files\HP Software\Select Audit directory. This folder contains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

⚠ If you are installing, uninstalling 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 /HP Software/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 Software\Select Audit\auditserver\Uninstall_Select_Audit` directory. The **Select Audit Uninstall Introduction** screen opens.


Uninstall HP Select Audit Server
Uninstall HP Select Audit Server
Introduction
Uninstalling...
Uninstall Complete
InstallAnywhere by Macrovision
Cancel
Previous
Next

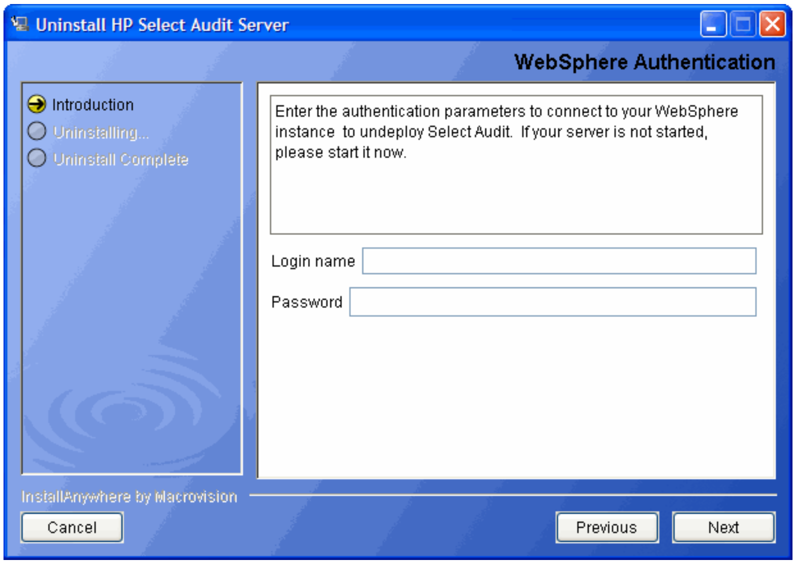
About to uninstall...

HP Select Audit Server

This will remove features installed by InstallAnywhere.

If you have any files in directory C:\Program Files\HP Software\Select Audit\ws that you would like to keep, please move them before proceeding with the uninstall.

2 Click **Next**. The **WebSphere Authentication** screen opens.



Enter the authentication parameters to connect to your WebSphere instance to undeploy Select Audit. If your server is not started, please start it now.

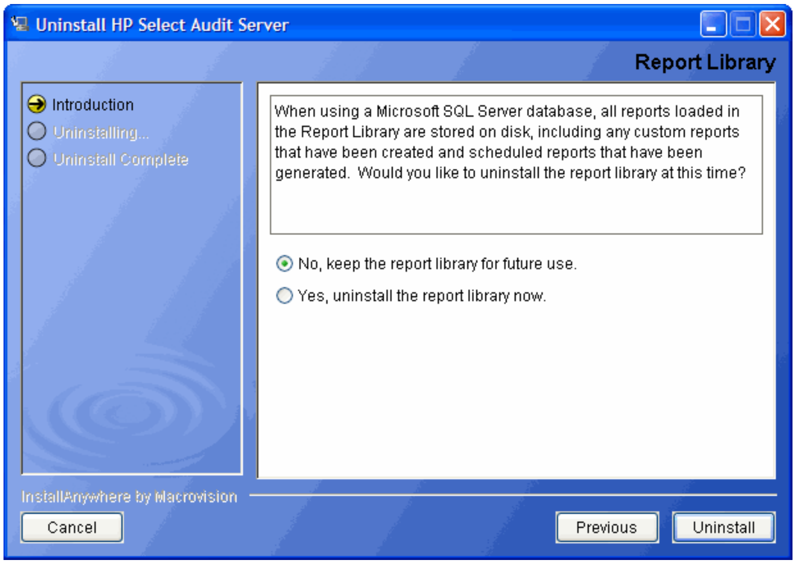
Login name

Password

3 Type the Server administrator name in the **Login name** field and Server administrator password in the **Password** field in the corresponding fields. This user must have privileges to undeploy and remove services on the domain.

> The WebSphere server must be running to properly uninstall Select Audit.

4 Click **Next**. If you are using MSSQL, the **Report Library** screen opens, otherwise, go to step 6.



When using a Microsoft SQL Server database, all reports loaded in the Report Library are stored on disk, including any custom reports that have been created and scheduled reports that have been generated. Would you like to uninstall the report library at this time?

● No, keep the report library for future use.

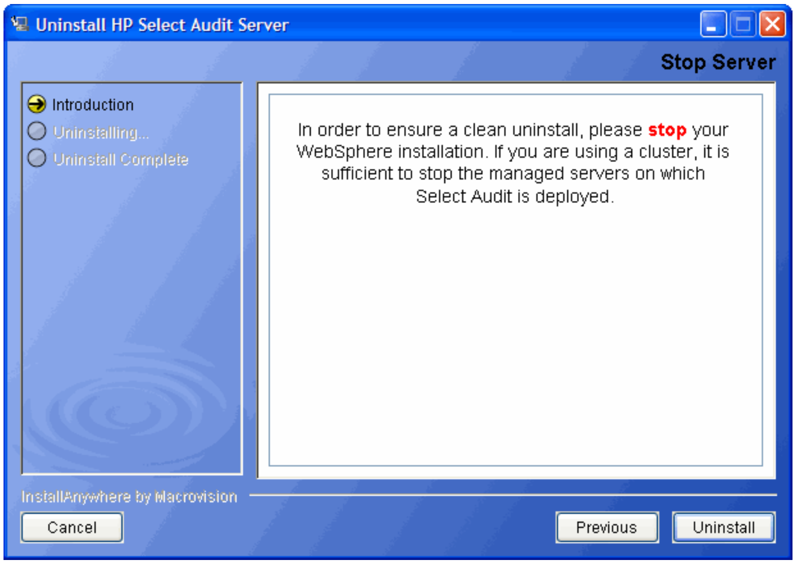
○ Yes, uninstall the report library now.

When using a Microsoft SQL Server database, all reports loaded in the Report Library are stored on disk, including any custom reports that have been created and scheduled reports that have been generated.

5 Do one of the following:

- Click **Yes** to uninstall the Report Library, including all custom reports and schedules permanently.
- Click **No** to leave any custom reports on disk to be restored later.

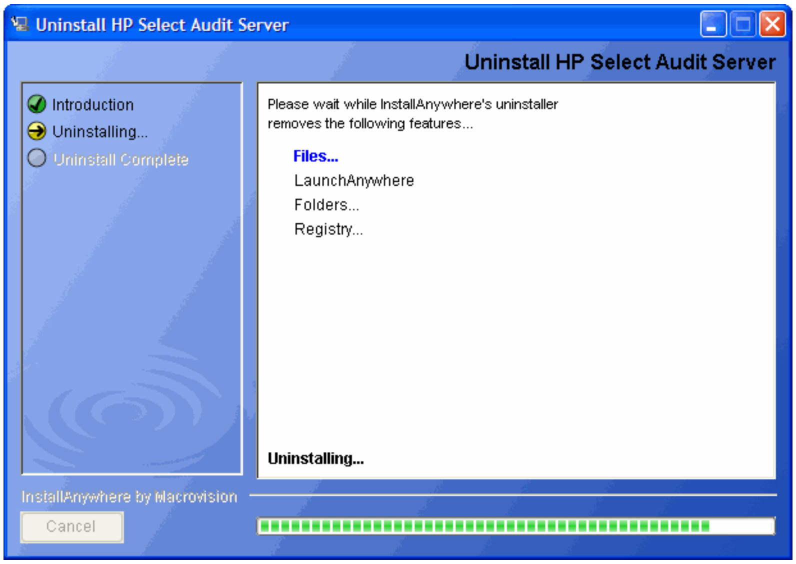
6 Click **Next**. The **Stop Server** screen opens.



In order to ensure a clean uninstall, please **stop** your WebSphere installation. If you are using a cluster, it is sufficient to stop the managed servers on which Select Audit is deployed.

7 Stop WebSphere and click **Uninstall**. The **Uninstall HP Select Audit Server** screen opens.

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

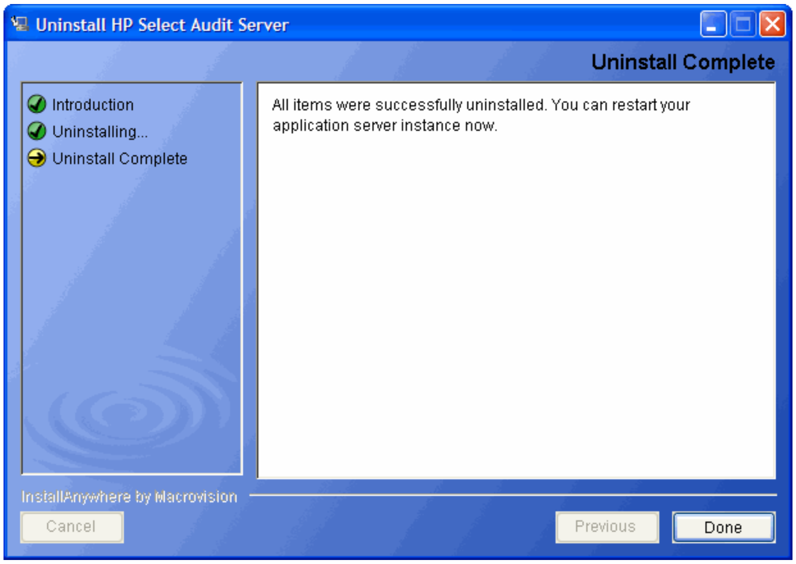

Uninstall HP Select Audit Server
Uninstall HP Select Audit Server
Introduction
Uninstalling...
Uninstall Complete
InstallAnywhere by Macrovision
Cancel

Please wait while InstallAnywhere's uninstaller removes the following features...

Files...
LaunchAnywhere
Folders...
Registry...

Uninstalling...

The uninstaller removes the Select Audit features. When the Audit Server is uninstalled, the **Uninstall Complete** screen opens.



All items were successfully uninstalled. You can restart your application server instance now.

8 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.

9 Restart the application server so that the changes take effect.

# 5 Installing the Select Audit Connector

This chapter provides an overview of how to install and uninstall the Select Audit Connector on your network.

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 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.

# Installing the Connector 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 installing, uninstalling 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

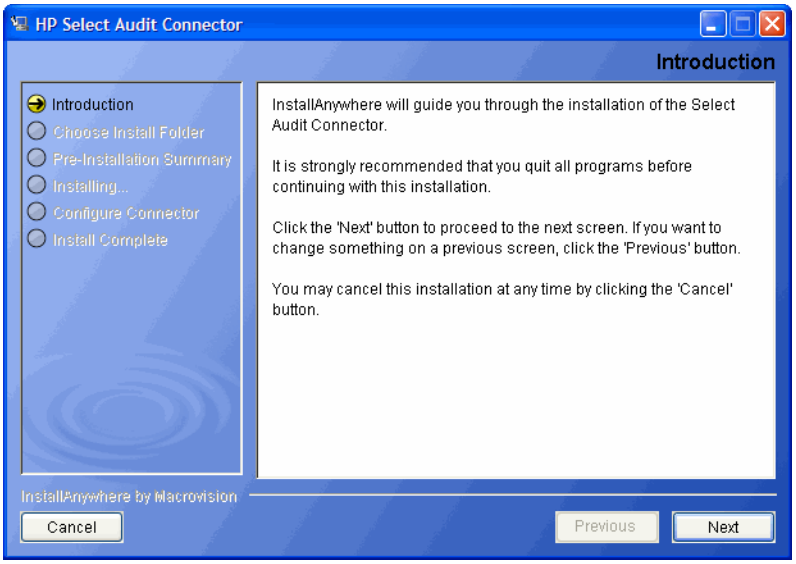
- **On HP-UX, Linux or Solaris:**

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

➤ You should be logged in using the root user to install the Audit Connector to ensure the service can be properly registered to run at startup.

⚠ A memory fault may occur when starting the Connector on HP-UX IA64 11.31 if the Connector user's login shell is `/usr/local/bin/bash`. This may be caused by the login shell of the user launching the Connector using the `su` command in the `SAudConn` startup script. If a memory fault occurs when the Connector user's login shell is `/usr/local/bin/bash`, change the user's login shell to `/bin/sh` and start the Connector again.

The installer extracts the installation files and then prepares the Select Audit Connector Install wizard. When it has finished loading, the **Introduction** screen opens.



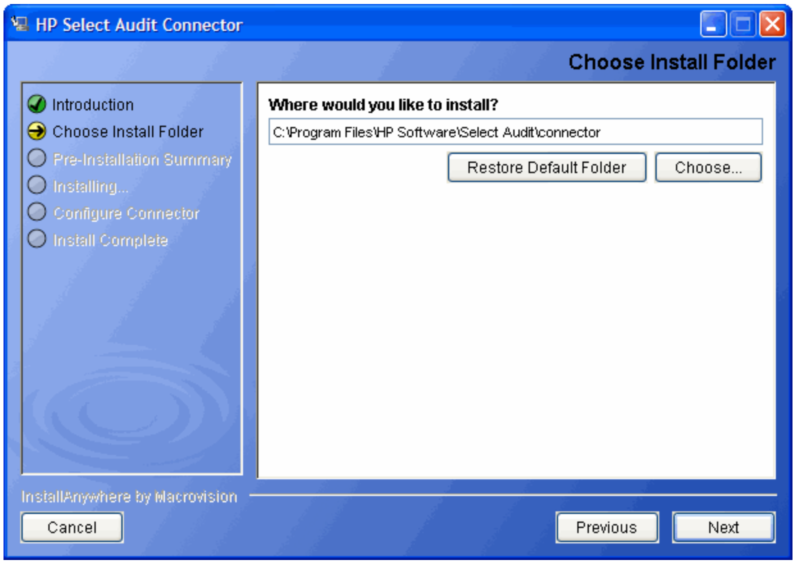
InstallAnywhere will guide you through the installation of the Select Audit Connector.

It is strongly recommended that you quit all programs before continuing with this installation.

Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

2 Click **Next**. The **Choose Install Folder** screen opens.



Where would you like to install?

C:\Program Files\HP Software\Select Audit\connector

3 Do one of the following:

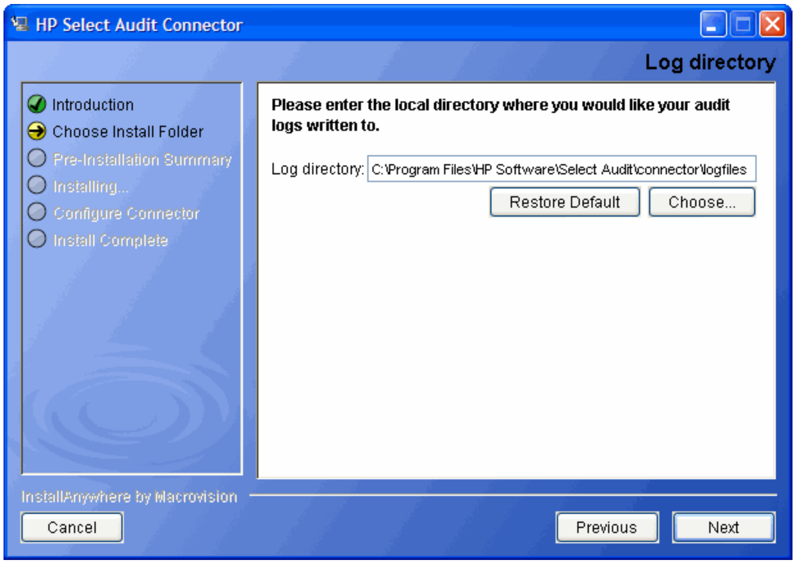
- If the default location is acceptable, proceed to step 4.
- If you want to select a different installation folder, click **Choose**, select a folder and then click **OK**. The new folder is shown in the **Where would you like to install Select Audit?** field.

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:

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

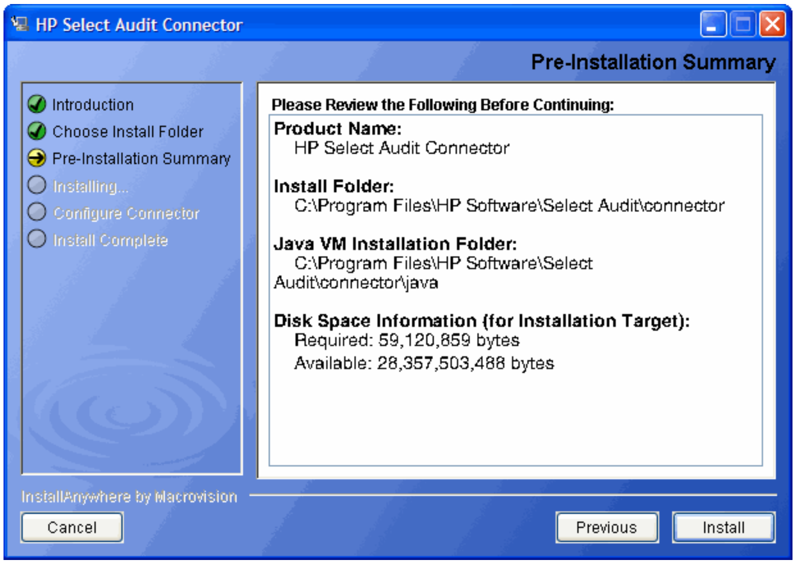
4 Click **Next**. The **Log Directory** screen opens. The Log directory is where audit event logs are temporarily stored before being sent to the server.



Please enter the local directory where you would like your audit logs written to.

Log directory: C:\Program Files\HP Software\Select Audit\connector\logfiles

5 Select the local directory that you want to write audit logs to and click **Next**. The **Pre-Installation Summary** screen opens.



Pre-Installation Summary

Please Review the Following Before Continuing:

**Product Name:**
HP Select Audit Connector

**Install Folder:**
C:\Program Files\HP Software\Select Audit\connector

**Java VM Installation Folder:**
C:\Program Files\HP Software\Select Audit\connector\java

**Disk Space Information (for Installation Target):**
Required: 59,120,859 bytes
Available: 28,357,503,488 bytes

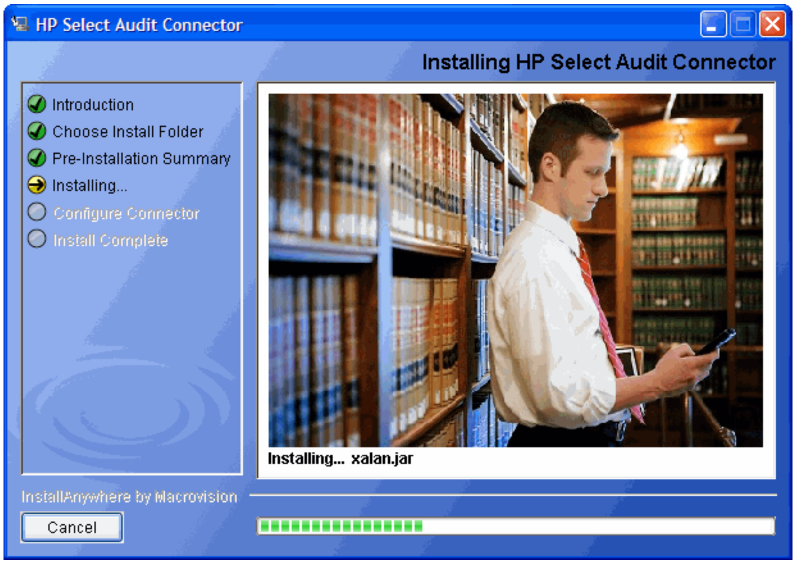
The **Pre-Installation Summary** screen creates a digest of the following installation information you provided to this point:

- 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**.

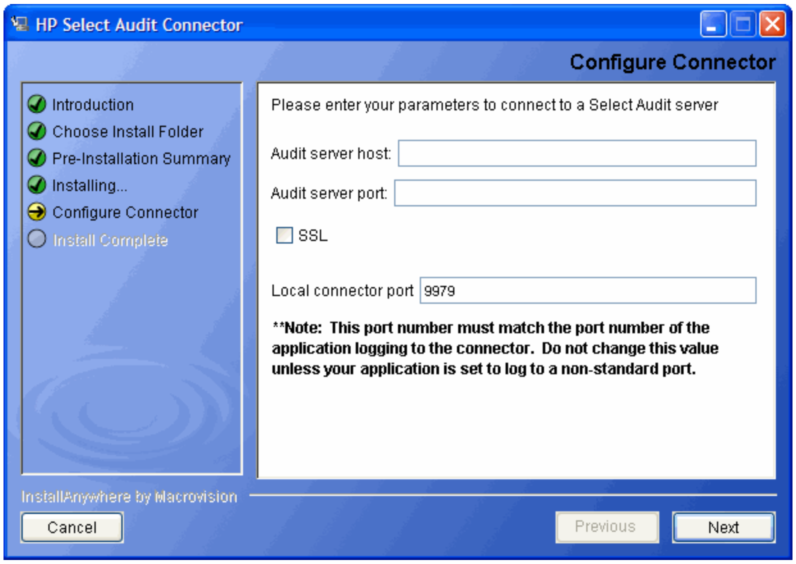
> To change any of the installation settings, click **Previous** to return to the screen containing the settings you want to change.

The Audit Connector begins to install and the **Connector Installation** screen opens.



Installing... xalan.jar

When the Connector installer is finished, the **Configure Connector** screen opens.



Please enter your parameters to connect to a Select Audit server

Audit server host:

Audit server port:

☐ SSL

Local connector port 9979

****Note: This port number must match the port number of the application logging to the connector. Do not change this value unless your application is set to log to a non-standard port.**

7 Customize your configuration on the **Configure Connector** screen:

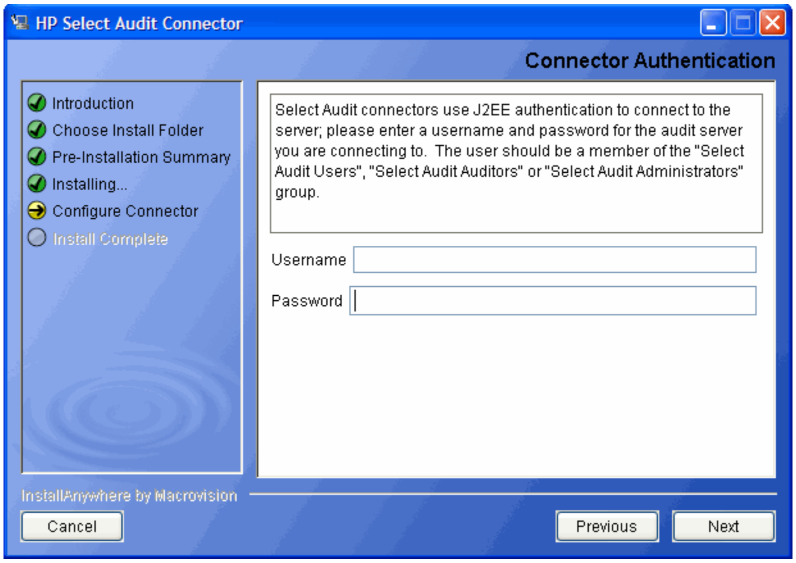
- Type the server host name in the **Audit server host** field.
- Type the server port number in the **Audit server port** field.
- Type the port number of the application logging to the Audit Connector in the **Local connector port** field.

> 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 opens.

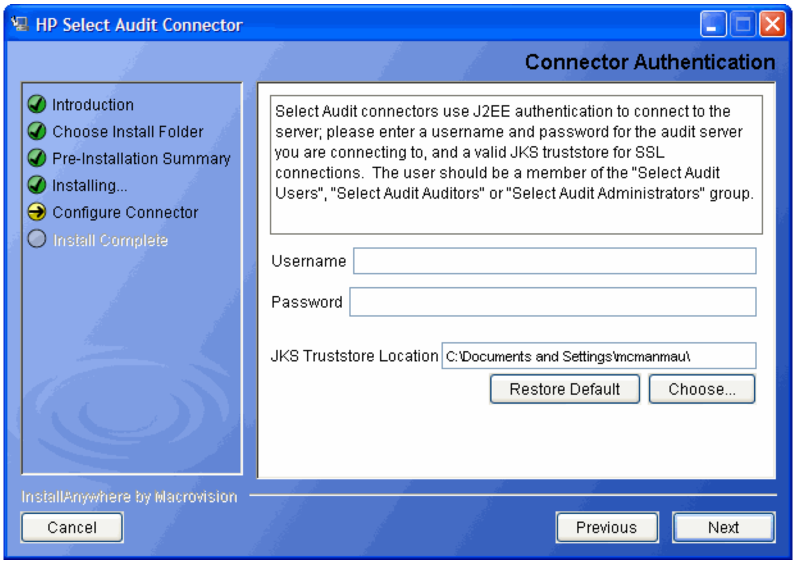


Select Audit connectors use J2EE authentication to connect to the server; please enter a username and password for the audit server you are connecting to. The user should be a member of the "Select Audit Users", "Select Audit Auditors" or "Select Audit Administrators" group.

Username

Password

If you are using SSL the **SLL Connector Authentication** screen opens.



HP Select Audit Connector

Connector Authentication

Select Audit connectors use J2EE authentication to connect to the server; please enter a username and password for the audit server you are connecting to, and a valid JKS truststore for SSL connections. The user should be a member of the "Select Audit Users", "Select Audit Auditors" or "Select Audit Administrators" group.

Username

Password

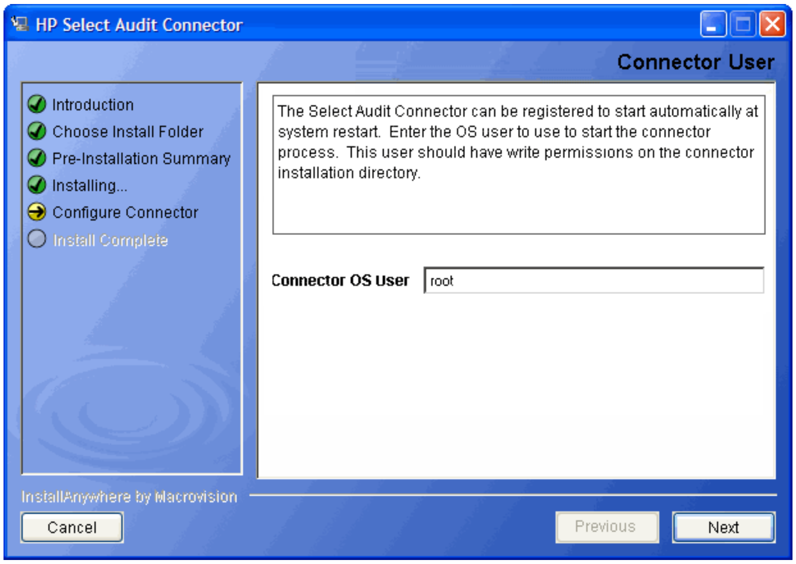
JKS Truststore Location C:\Documents and Settings\mcmanmau\

10 Type the **Username** and **Password** required to authenticate to the Audit Server.

The user name and password are the credentials of an application server user in the **Select Audit Users** group. These credentials must be predefined on the application 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**. If you are installing on UNIX, the **Connector User** screen opens.



HP Select Audit Connector

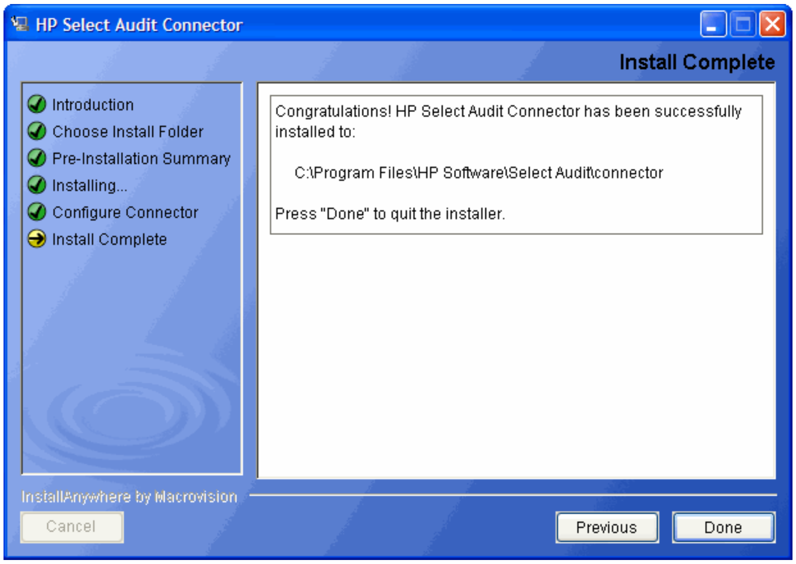
Connector User

The Select Audit Connector can be registered to start automatically at system restart. Enter the OS user to use to start the connector process. This user should have write permissions on the connector installation directory.

Connector OS User root

12 If you are a UNIX user, type the OS user you want to use to start the Connector in the **Connector OS User** field.

13 Click **Next**. The **Please Wait** screen opens. When the Audit Connector has been configured, the **Install Complete** screen opens.



Congratulations! HP Select Audit Connector has been successfully installed to:

C:\Program Files\HP Software\Select Audit\connector

Press "Done" to quit the installer.

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

For Windows installations, the installer does the following:

- It creates the Audit Connector's local configuration file `connector.props` in your installation directory root. (See Chapter 3, Configuring Select Audit in the *HP Select Audit 1.02 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.

- It 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 `HP Software/SelectAudit/connector` directory. It can be run with the options `start`, `stop` and `restart`.

## Installing the Connector 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 root user. 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:

  `/HP Software/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, user name and password.

7 When the installer is finished, an `Installation Complete` message is shown. Press **Enter** to exit the installer.

## Installing the Connector 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 Connector

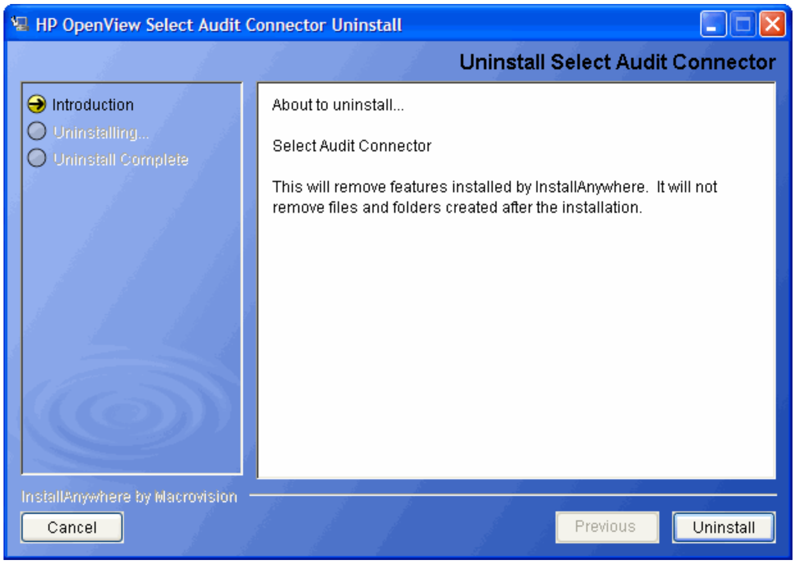
Audit Connector uninstaller executables are created on the machine where the Audit Connector is installed during the Connector installation. After installing the Audit Connector on Windows, there is an `Uninstall_Connector` folder under `C:\Program Files\HP OpenView\Select Audit` directory. This folder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

⚠ If you are installing, uninstalling 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 `/HP Software/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 opens.

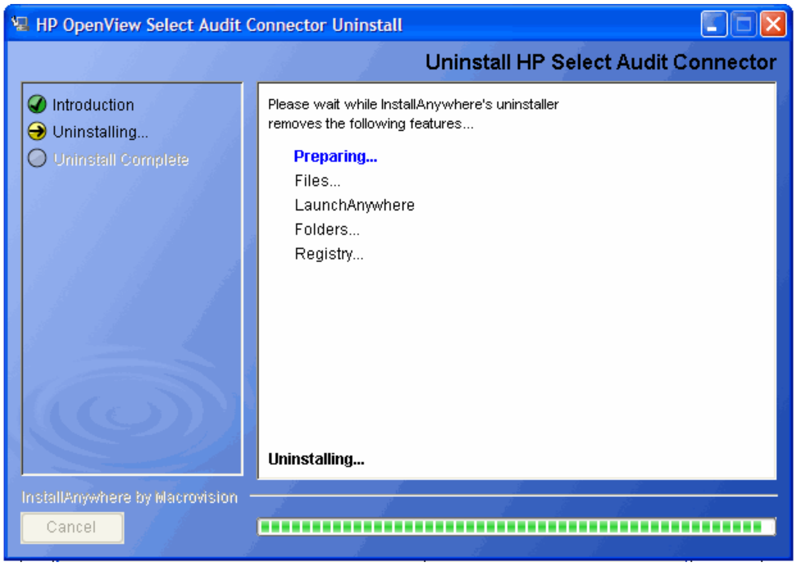

HP OpenView Select Audit Connector Uninstall
Uninstall Select Audit Connector
Introduction
Uninstalling...
Uninstall Complete
InstallAnywhere by Macrovision
Cancel
Previous
Uninstall

About to uninstall...

Select Audit Connector

This will remove features installed by InstallAnywhere. It will not remove files and folders created after the installation.

2 Click **Uninstall**. The **Uninstall Select Audit Connector** screen opens listing the features being uninstalled.


HP OpenView Select Audit Connector Uninstall
Introduction
Uninstalling...
Uninstall Complete
InstallAnywhere by Macrovision
Cancel

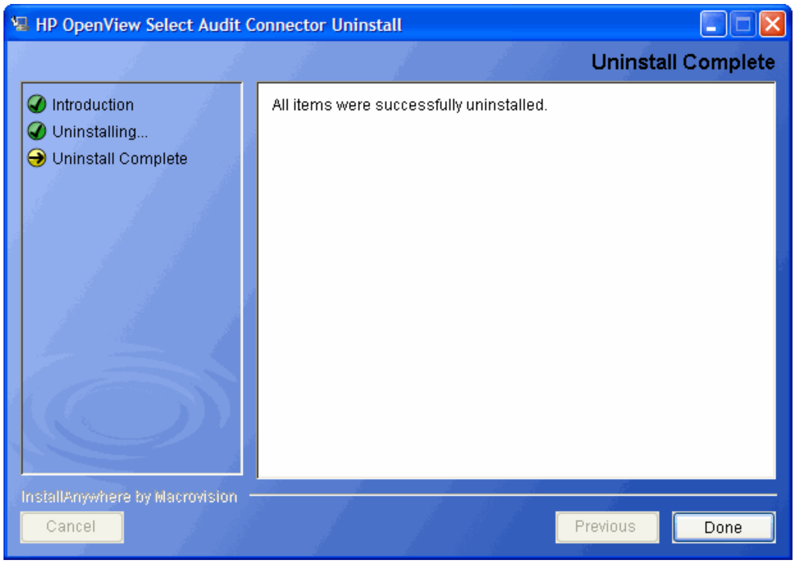
Uninstall HP Select Audit Connector

Please wait while InstallAnywhere's uninstaller removes the following features...

Preparing...
Files...
LaunchAnywhere
Folders...
Registry...

Uninstalling...

When Select Audit is uninstalled, the **Uninstall Complete** screen opens.


HP OpenView Select Audit Connector Uninstall
Introduction
Uninstalling...
Uninstall Complete
InstallAnywhere by Macrovision
Cancel
Previous
Done

Uninstall Complete

All items were successfully uninstalled.

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.

# 6 Using Self-Healing Services

HP Self-Healing Services (SHS) are part of HP's built-in support. SHS integrates with HP Select 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 79
- Data Collector on page 79
- Using SHS on page 81

## 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 Self-Healing Services enable HP software to automatically detect problems and take steps to remedy them.

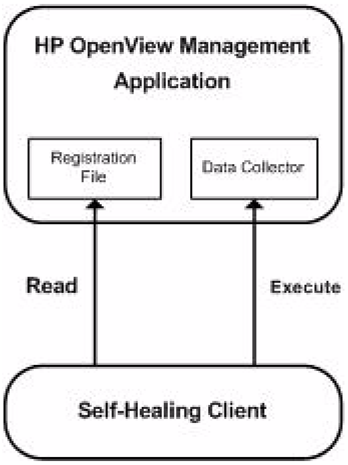
When HP software detects it has suffered a problem, information surrounding the problem is gathered. The gathered information consists of artifacts such as application configuration files, log files and system environmental settings. This information is sent securely to HP. When received, the information 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 1.

**Figure 1    Self-Healing Services**

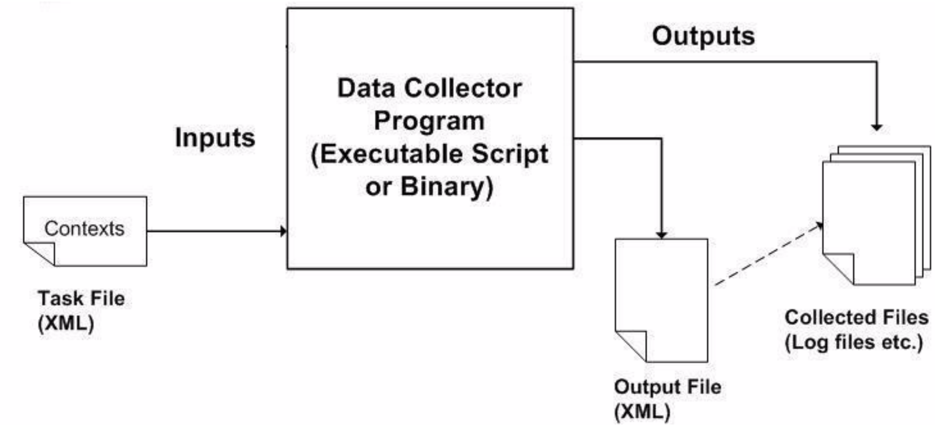


The Data Collector must be registered with the OS through a signed registration file. You must create the registry key entry for SHS to register with the Self-Healing Client.

## 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 81 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 2.

**Figure 2    Data Collection Process**


Inputs
Outputs
Data Collector Program (Executable Script or Binary)
Contexts
Task File (XML)
Output File (XML)
Collected Files (Log files etc.)

## Data Collected

SHS can be used to collect Select Audit configuration details, as well as log files, environment data, database configuration details, application server configuration files, the startup script, and so on. For a full list of the files collected, see `<install_dir>/shs/saud-collector-config.xml`.

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).

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

**On UNIX:**

The file `slctaud.xml` must be copied from `<install_dir>/shs/reg to /var/opt/hpsupport/reg/dc` to register with the Self-Healing Client.

**On Windows:**

The file is copied automatically in the Windows registry at install time.

## Using the Data Collector in a Clustered Environment

Each managed server that is part of the cluster requires access to some files on disk, for example, `audit_config.xml` and `scopeserver.xml`. When installing on the cluster, the installer is only run once on the machine running the main server.

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

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 1.02 installer at the following location:

```
\HP Software\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. Start the data collector using one of the following methods:
   - Double-click `run-data-collector.bat` in the `SHS` folder.
   - Type the following command from the command line.

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

   The arguments used in the command are described in Table 5.

   **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 Software\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.

# A Installer Configurations

This appendix contains descriptions of the actions the WebLogic and WebSphere installers perform when installing Select Audit. It contains the following sections:

- WebLogic Installation Steps on page 83
- WebSphere Installation Steps on page 88

## WebLogic Installation Steps

The WebLogic installer makes changes to the existing WebLogic server at different stages of the wizard so that Select Audit will operate correctly. These changes are described according to the different wizard stages.

### Installation Stage

The installation wizard does the following during the installation stage.

- It installs the Select Audit application files.
- It installs the JDK 1.4.2 in the `<install_dir>/java` directory. This is used only by the installer and uninstaller.
- It creates `<install_dir>/SelectAudit_install_debug.txt` to log installer output and error messages.
- On UNIX systems, the installer attempts to register the Self-Healing Service by copying `shs/reg/slctaud.xml` to the `/var/opt/hpsupport/reg/dc` directory. If the installer user does not have write access to this directory, they will be shown an error message. This registration can be done manually post-installation if desired.

### Input and Validation Stage

During the Input and Validation stage, the installer performs the following steps:

- It makes a basic connection to the load balancer and Administration server URL to ensure that the connection string is valid.
- It stores the user configuration and keyfile. In order to avoid passing the WebLogic user name and password to the WebLogic APIs that are called to set up the domain environment, the installer creates a user configuration file that stores an encrypted password, and a keyfile that is used to encrypt and decrypt the password. The files are deleted at the end of the installation.

  ➤ If the installation is cancelled prior to its completion, the files should be deleted from `<install_dir>/setup` to ensure the integrity of the system.

- It checks the servers are running using the WebLogic APIs to ensure that the given server or cluster is running, as well as the Administration server.
- It validates the domain using the WebLogic APIs to validate that the domain name and security provider name match the parameters supplied.
- It tests the database connection by creating a simple JDBC connection to the supplied Oracle or Microsoft SQL Server database. It verifies that the Select Audit schema is in place by performing a simple Select statement on what should be an empty table (AUDITEVENT).
- For Microsoft SQL server, it creates the supplied library store directory, if it does not already exist.

  ➤ For a cluster deployment, this folder should be created in advance as a shared drive to which all servers have access. The path must be fewer than 18 characters in length.

- It tests the mail server. A basic connection is made to port 25 on the mail server. If there is a failure, the user will have the option of ignoring the warning and continuing.
- It validates Select Identity information by making a connection to the given server at `/lmz/webservice/`, logging in with the given credentials and requesting the current set of permissions for that user. It then validates the connection to the Select Identity database as above.

## Application Configuration Step

The steps the WebLogic installer performs during the Application Configuration stage are described below:

- It configures the Report server XML files. The Select Audit Report server stores its configuration in XML files that contain database connection details, LDAP authentication parameters, mail server settings, and so on. (Refer to `directory.xml`, `library.xml` and `scopeserver.xml`.) All passwords are encrypted before being stored.
- It creates the log4j output directory and configures the `log4j.properties` file. The installed `log4j.properties` file will be used by WebLogic for all applications that use log4j.

  ➤ If you have other applications installed that use a `log4j.properties` file, the two properties files should be merged.

- It writes the mail server host name and return address to the `workflow.properties` file in order to send email notifications from the Attestation Workflow feature.
- It configures `audit_config.xml` by storing information to the bootstrap the stored MBeans for Select Audit Configuration. This includes the JNDI name of the Select Audit data source, the server connection settings and the encrypted WebLogic credentials.
- It configures SHS scripts by configuring which files are collected for Self-Healing Services.
- It sets up Select Identity Filtering. The Select Identity settings are written to the database in the SACFGATTRIBUTE table and any existing filtering settings are removed. (There should be none at this point).

  It updates the Report server XML files to use the proxy data source to filter report data based on permissions and to use a custom directory provider instead of the default WebLogic embedded LDAP provider.

- It loads the workflow templates. The installer writes the two default Attestation Workflow templates to the WFTEMPLATE and WFAPPDEFINEDATA tables in the Select Audit schema. Previously-loaded templates will be removed. (There should be none at this point).
- It configures the Operations Model by copying the configuration files for the Oracle or MSSQL database as needed for the Operations Model.

## WebLogic Domain Configuration Step

The installer configures the WebLogic domain in the following ways:

- It makes a copy of `startWebLogic.cmd/sh` called `startWLSelectAudit.cmd/sh` to be configured with the Select Audit classpath and JVM arguments. The original startup script remains unchanged but the new modified script must be used to start the server before deployment.
- It sets the Remote Start settings for managed servers. If you are installing on a cluster, the installers will add the Select Audit `JAR` files and the JVM settings will be added to the Remote Start settings for each managed server in the cluster, as well as setting the supplied BEA Java Home and BEA Home. This ensures that when starting a server from node manager, the classpath settings will be available to all servers. Existing classpath settings will be included at the end of the Select Audit classpath.
- It modifies `vde.prop`. In order for the Report server login module to function correctly, the property `vde.aclcheck` must be set to `0` (default `1`) in `<server_home>/ldap/conf/vde.prop` for each server. For managed servers, this must be done manually.
- It creates the Select Audit connection pool using the WebLogic APIs. The installer creates a JDBC connection pool named SelectAuditConnectionPool, with the given Oracle or Microsoft SQL Server database settings, targeted to the Administration server and the target server or cluster. If there is a naming conflict on the connection pool, the installer will prompt you to recreate the object.
- It create three JDBC data sources:

| Name | JNDI Name | Purpose |
|---|---|---|
| SelectAuditDataSource | jdbc.SelectAudit | Main data source for Select Audit application processing (configuration, data input, and so on). |
| SAudDataSource | jdbc/SAudDataSource | Report server data source used for storing and executing reports based on Audit data. |
| SelectAuditWorkflowDataSource | jdbc.TruAccess | Attestation Workflow data source, for scheduling and executing attestation workflow events. |

If there is a naming conflict on any of the data sources, the installer will you prompt to recreate the objects.

- It creates JMS Queues. These JMS Queues are referenced by the Attestation Workflow engine. They are not used by Select Audit but must be created for the proper functioning of the Workflow Engine.

| Name | Type |
|---|---|
| jms.OVSIQCF | JMSConnectionFactory |
| jms.OVSITCF | JMSConnectionFactory |
| OVSIFileStore | JMSFileStore |
| OVSIPagingStore | JMSFileStore |
| OVSIServer | JMSServer |
| jms.OVSIWfRequestExpireQueue | JMSQueue |
| jms.OVSIWorkflowQueue | JMSQueue |

If there is a naming conflict, the installer will prompt you to recreate the JMS objects.

- It stops the managed servers. If you are running a cluster, the installer will prompt you to shut down all managed servers before creating the startup class, to avoid configuration conflicts.
- It creates the startup class. Select Audit requires a WebLogic startup class to initialize its configuration module. This is accomplished by editing `config.xml` while the servers are stopped.
- It restarts WebLogic. You are prompted to restart all WebLogic servers using the new startup script to start the Administration server.
- It checks that the servers are running using the WebLogic APIs to verify that the servers are up and running.
- It creates WebLogic groups and roles. For authentication, Select Audit relies on four predefined groups and three predefined roles:

| Group | Role | Users |
|---|---|---|
| Select Audit Administrators | Select Audit Administrator | Supplied WebLogic user is added to this group. |
| Select Audit Auditors | Select Audit Auditor | |
| Select Audit Users | Select Audit User | |
| Select Audit Report Developers | None | |

➤ Members of the Select Audit Developers group must also belong to another of the three groups in order to have login access.

➤ For external LDAP, only roles are created, the groups and associations must be created manually.

- It creates the proxy connection pool and data source using the WebLogic APIs to create a second JDBC connection pool and a fourth JDBC data source. This data source is used when report filtering is enabled to filter results to allow only the information that the current user has been granted access to. The connection pool uses a custom JDBC driver, but connects to the same database as the first connection pool. This is only used when Select Identity filtering is enabled.

| Name | JNDI Name |
|---|---|
| SelectAuditProxyConnectionPool | |
| SelectAuditProxyDataSource | jdbcproxy/SAudDataSource |

If there is a naming conflict, the installer will prompt you to recreate the object.

- It creates the Select Identity connection pool and data source. This connection pool and data source are used to connect to the Select Identity database which can be Oracle or Microsoft SQL Server.

| Name | JNDI Name |
|---|---|
| SelectIdentityIntegrationPool | |
| SelectIdentityIntegrationDataSource | jdbc.IdentityIntegration |

If there is a naming conflict, the installer will prompt you to recreate the objects.

- It deploys the applications. Using WebLogic APIs, the installer deploys the Select Audit Server, Select Audit Report server, and Select Audit Workflow Engine applications to the given server or cluster. Any existing applications with the same name will be undeployed.

| Name | Type |
|---|---|
| SelectAuditServer | Application |
| SelectAuditWorkflow | Application |
| SelectAuditReporting | Web Application Module |

## Post-Deployment Configuration Step

Once the installer has configured Select Audit, it does the following:

- It loads the default reports. Select Audit comes with a set of predefined reports that are based on Select * application data. The Report server has a SOAP report loader that is used to upload and publish these reports. For Oracle, the reports are stored in the database, for Microsoft SQL Server installations, the reports are stored on the file system.
- It loads the ACLs and sets the default permissions on the loaded reports.

## Installation Cleanup Step

When the installation is complete, the installer deletes the user configuration and key files, all passwords stored in installer variables are nulled and the InstallAnywhere install log is created with a success/failure message for each step.

If installation is cancelled early, the entire install directory should be deleted to prevent plain text passwords from being stored in a properties file.

# WebSphere Installation Steps

The WebSphere installer makes changes to the existing WebSphere server at different stages of the wizard so that Select Audit will operate correctly. These changes are described according to the different wizard stages.

## Installation Stage

The installation wizard does the following during the installation stage.

- It installs the Select Audit application files.
- It installs the JDK 1.4.2 in the `<install_dir>/java` directory. This is used only by the installer and uninstaller.
- It creates `<install_dir>/SelectAudit_install_debug.txt` and log installer output and error messages.
- On UNIX systems, the installer attempts to register the Self-Healing Service by copying `shs/reg/slctaud.xml` to the `/var/opt/hpsupport/reg/dc` directory. If the installer user does not have write access to this directory, they will be shown an error message. This registration can be done manually post-installation if desired.

## Input and Validation Stage

During the Input and Validation stage, the installer performs the following steps:

- It makes a basic connection to the load balancer and Administration server URL to ensure that the connection string is valid.
- It validates the LDAP by searching for the given WebSphere user in the supplied LDAP server.
- It checks the servers are running using the WebSphere administration APIs to ensure that the given server or cluster is running.
- It tests the database connection by creating a simple JDBC connection to the supplied Oracle or Microsoft SQL Server database. It verifies that the Select Audit schema is in place by performing a simple Select statement on what should be an empty table (AUDITEVENT).
- For Microsoft SQL server, it creates the supplied library store directory, if it does not already exist.

  ➤ For a cluster deployment, this folder should be created in advance as a shared drive to which all servers have access. The path must be fewer than 18 characters in length.

- It tests the mail server. A basic connection is made to port 25 on the mail server. If there is a failure, the user will have the option of ignoring the warning and continuing. See the Configuring a Mail Session in WebSphere on page 34 for details on configuring mail services after installation.
- It validates Select Identity information by making a connection to the given server at `/lmz/webservice/`, logging in with the given credentials and requesting the current set of permissions for that user. It then validates the connection to the Select Identity database as above.

## Application Configuration Step

The steps the WebSphere installer performs during the Application Configuration stage are described below:

- It configures the Report server XML files. The Select Audit Report server stores its configuration in XML files that contain database connection details, LDAP authentication parameters, mail server settings, and so on. (Refer to `directory.xml`, `library.xml` and `scopeserver.xml`.) All passwords are encrypted before being stored. These XML files are configured and then the `.war` file is updated with the new configuration. An `.ear` file is built containing the configured `.war` file for deployment.
- It sets up Select Identity Filtering. The Select Identity settings are written to the database in the SACFGATTRIBUTE table and any existing filtering settings are removed. (There should be none at this point).

  It updates the Report server XML files to use the proxy data source to filter report data based on permissions and to use a custom directory provider instead of the default WebSphere embedded LDAP provider.
- It creates the log4j output directory and configures the `log4j.properties` file. The installed `log4j.properties` file will be placed on the WebSphere classpath for target servers.
- It configures the Operations Model by copying the configuration files for the Oracle or MSSQL database as needed for the Operations Model.
- It writes the mail server host name and return address to the `workflow.properties` file in order to send email notifications from the Attestation Workflow feature.
- It loads the workflow templates. The installer writes the two default Attestation Workflow templates to the WFTEMPLATE and WFAPPDEFINEDATA tables in the Select Audit schema. Previously-loaded templates will be removed. (There should be none at this point).
- It configures `audit_config.xml` by storing information to the bootstrap the stored MBeans for Select Audit Configuration. This includes the JNDI name of the Select Audit data source, the server connection settings and the encrypted WebSphere credentials.
- It configures SHS scripts by configuring which files are collected for Self-Healing Services.

## WebSphere Server Configuration Step

The installer configures the WebSphere server in the following ways:

- It sets the classpath and shared libraries. For each target server, the `<install_dir>/dist/config/properties` folder is added to the JVM level classpath so that the applications' properties files are accessible. A shared library object is created containing the common `JAR` files shared between applications.
- It creates a custom service and login module using the WebSphere administration APIs. A custom service is created to bootstrap the application's configuration MBean service. A JAAS login module is also configured to enable login to the Report server application.

  On UNIX systems, a generic JVM argument is added to each server to set the option `headless=true`, to allow the models to display correctly without an xserver environment.

For all operating systems, the installer also sets “`-Xms256M -Xmx1024M -Dclient.encoding.override=UTF-8`” to ensure that enough memory is available for each server and to have reports with non-ASCII characters display correctly.

- It creates J2C Auth aliases. In order to authenticate with the database, each of the JDBC data sources requires a J2C authentication data entry. The installer creates one for the Select Audit database user and a second for the Select Identity database user, if Select Identity filtering is selected. If there is a naming conflict on SelectAuditDBAlias or SelectIdentityIntegrationDBAlias, the installer will prompt you to recreate the objects.
- It creates JDBC Services using the WebSphere administration APIs to create three JDBC providers, as follows:

| Name | Description | Data Sources | Application |
|---|---|---|---|
| SelectAuditJDBC Provider | Simple Oracle or MSSQL JDBC Provider | jdbc.SelectAudit | SelectAuditServer |
| | | jdbc/SAudDataSource | SelectAuditReportServer |
| | | jdbc/TruAccess | SelectAuditWorkflow |
| SelectAuditProxy Provider | Custom JDBC Provider for report filtering | jdbcproxy/ SAudDataSource | SelectAuditReportServer |
| SelectAuditIdentity JDBCProvider | Regular JDBC Provider, for connecting to Select Identity database | jdbc.IdentityIntegration | SelectAuditServer |

If there is a naming conflict, the installer will prompt to recreate all objects.

- It creates JMS Queues: These JMS Queues are referenced by the Attestation Workflow engine. They are not used by Select Audit but must be created for successful deployment and proper functioning of the Workflow Engine.

| Name | Type | JNDI Name |
|---|---|---|
| jms.OVSIQCF | JMSConnectionFactory | jms/OVSIQCF |
| jms.OVSIWfRequestExpire Queue | JMSQueue | jms/ OVSIWfRequestExpireQueue |
| jms.OVSIWorkflowQueue | JMSQueue | jms/OVSIWorkflowQueue |
| eis.OVSIWfRequestExpire Queue | JMSActivationSpecification | eis/ OVSIWfRequestExpireQueue |
| eis.OVSIWorkflowQueue | JMSActivationSpecification | eis/OVSIWorkflowQueue |

If there is a naming conflict, the existing objects will be used as no specific configuration is required.

- It enables SSO on the WebSphere domain, and LTPA if it is not already enabled. Several Select Audit `JAR` files are copied to the WebSphere `lib/ext` folder to ensure that deployment is sucessful. URL rewriting is enabled on the web container of each target server.
- It restarts the server. At this point, the servers must be restarted for all configuration changes to take effect.
- It checks that the servers are running using the WebSphere APIs to verify that the servers are up and running.
- It deploys the applications. Using WebSphere APIs, the installer deploys the SelectAuditServer, SelectAuditReportServer and SelectAuditWorkflow applications to the given server or cluster. Any existing application of the same name will be undeployed. After deploying, the URL rewriting option is enabled on the deployed report server application.
- It starts the three deployed applications using the WebSphere APIs.

## Post-Deployment Configuration Step

Once the installer has configured Select Audit, it does the following:

- It loads the default reports. Select Audit comes with a set of predefined reports that are based on Select * application data. The Report server has a SOAP report loader that is used to upload and publish these reports. For Oracle, the reports are stored in the database, for Microsoft SQL Server installations, the reports are stored on the file system.
- It loads the ACLs and sets the default permissions on the loaded reports.

## Installation Cleanup Step

When the installation is complete, the installer deletes the user configuration and key files, all passwords stored in installer variables are nulled and the InstallAnywhere install log is created with a success/failure message for each step.

# Index