HP Select Audit Software

for the Windows® and HP-UX® operating systems

Software Version: 1.1

Installation Guide

Document Release Date: January 2008
Software Release Date: January 2008

Legal Notices

Warranty

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

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

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

Trademark Notices

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

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

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

Documentation Updates

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

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

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

http://h20230.www2.hp.com/selfsolve/manuals

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

Support

You can visit the HP software support web site at:

www.hp.com/go/hpsoftwaresupport

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 9
Audience 9
The Select Audit Documentation Set 9
Installation Environment 10
Supported Platforms 10
Minimum System Requirements 11
Platform Availability 11
Chapter Summary 12

2 Pre-Installation Information 13
Select Audit Installers 13
Audit Server 13
Audit Connector 13
The Impact of Running Control Panel Applications 14
The Importance of the Correct Administration Entitlements 14
Before Installing Select Audit 14
Creating a New Database Instance 14
Oracle 14
MSSQL 15
Setting Up The Database Schemas 16
To configure the Oracle database server 16
To configure the Microsoft SQL Server 2000 database server 16
To configure the Microsoft SQL Server 2005 database server 19
Adding Users to Roles 26
Integrating with Select Identity 26
Auditing Select Identity Data with Select Audit 26
Filtering Select Audit Reports using Select Identity Entitlements 27
Requirements and Recommendations 27
Select Audit Authentication Options 28
About CRL Validation 29
Installing Select Audit and Select Identity on the Same Domain 29
Select Identity Server Configuration 29
Creating a Key Store and Trust Store for the Select Identity Server 29
Configuring WebLogic to Enable SSL 30
Configuring Select Identity Security 37
Creating a Select Identity Administrator and Certificate Configuration 37
Select Audit Configuration 37
Select Audit Configuration Options 38
Installing on HP-UX 38

Installing in a Clustered Environment . . . 39
Installing in a Clustered Environment on WebLogic . . . 39
Installation Order . . . 39
3 Installing Select Audit on WebLogic . . . 41
Installing the Audit Server . . . 41
Post-Installation Steps . . . 59
Enabling Load Balancing for Clusters . . . 60
Configuring Log4j . . . 60
Enabling Logging . . . 60
Setting Appenders . . . 61
Configuring UTF-8 Fonts in PDF Channel Reports . . . 61
Uninstalling the Audit Server . . . 62
To uninstall the Audit Server . . . 63
4 Installing the Select Audit Connector . . . 67
Select Application Configuration Requirements . . . 67
Select Audit Connector Installer Mode Overview . . . 67
Installing the Connector in Default Mode . . . 68
Installing the Connector in Console Mode . . . 74
Installing the Connector in Silent Mode . . . 75
Post-Installation Steps . . . 75
Registering the Connector to Run at Startup (Unix) . . . 75
Uninstalling the Audit Connector . . . 76
To uninstall the Audit Connector . . . 76
5 Using Self-Healing Services . . . 79
Self-Healing Services . . . 79
Data Collector . . . 79
Data Collection Process . . . 79
Data Collected . . . 80
Using the Data Collector in a Clustered Environment . . . 80
Using SHS . . . 81
To start collecting data . . . 81
A Installer Configurations . . . 83
WebLogic Installation Steps . . . 83
Installation Stage . . . 83
Input and Validation Stage . . . 83
Application Configuration Step . . . 84
WebLogic Domain Configuration Step . . . 85
Post-Deployment Configuration Step . . . 87
Installation Cleanup Step . . . 88
Index . . . 89

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 1.1 to suit their business and industry environment. This guide assumes a working knowledge of the following:

- WebLogic 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 1.1 Administration Guide*, © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. (`administration_guide.pdf`).
- *HP Select Audit 1.1 Installation Guide*, © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. (`installation_guide.pdf`).
- *HP Select Audit 1.1 User's Guide*, © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. (`user_guide.pdf`).
- *HP Select Audit 1.1 Sarbanes-Oxley Model Guide*, © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. (`sb_model_guide.pdf`)
- *HP Select Audit 1.1 Concepts Guide*, © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. (`concepts_guide.pdf`)
- *HP Select Audit 1.1 Report Center User's Guide*, © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. (`rpt_center_guide.pdf`)
- *HP Select Audit 1.1 Report Designer's Guide*, © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. (`rpt_design_guide.pdf`)

- *HP Select Audit 1.1 Report Developer's Guide*, © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. (`rpt_devel_guide.pdf`)
- *HP Select Audit 1.1 LDAP Configuration Guide,* © Copyright 2006 - 2008 Hewlett-Packard Development Company, L.P. (`ldap_provisioning.pdf`)

Online help is available with the Audit Portal.

Installation Environment

Select Audit has two installers: a Connector installer and a Server installer for WebLogic. 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 platforms, servers and applications supported by Select Audit are listed in Table 1.

Table 1 Supported Platforms, Servers and Applications

Select Audit Server Operating system support	• Microsoft Windows 2003 (32 bit) • HP-UX 11.23, 11.31 Itanium
Select Audit Connector Operating system support	• Microsoft Windows 2003 IA32/EM64T/AMD64 • Red Hat Linux AS3, AS4 IA32/EM64T/AMD64 • HP-UX 11.23 PA-RISC, 11.23 Itanium, 11.31 Itanium • Solaris 9, 10 SPARC
Application and portal servers	• BEA WebLogic Application Server 9.2 MP1
Audit connectors	• HP Select Identity 4.1x, 4.20 and 4.21 • HP Select Access 6.2 SP2 • HP Select Federation 6.5, 6.6, and 7.0
Audit storage and databases	• Oracle 9i, 10g • Microsoft SQL Server 2000 and 2005
Compliance report packs	• Sarbanes-Oxley (Optional)
Directory server	• SunOne version 5.2

Minimum System Requirements

To install the Select Audit server, 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 HP-UX
Processor	Pentium 4	Pentium 4
Memory	2 GB RAM	2 GB RAM
Disk space (combination of temporary space and real space required for a full install)	250 MB	For HP-UX: 220 MB
Video card	256 colors	256 colors
Operating systems	Windows 2003 Server Service Pack 2	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 2 GB of memory for each managed server.

Platform Availability

The Select Audit Server is available for the Windows 2003 and HP-UX platforms. The Select Audit connector is available for Windows 2003, 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 1.1 Release Notes* (`SAudit_release_notes_1.1.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 the Select Audit Connector	This chapter describes how to install the Select Audit Connector.
Chapter 5, 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 installer performs 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 and related components on a WebLogic server. The installer copies the necessary files to your system and then configures the application server and the Select Audit application to create a fully deployed system.

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.

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 the Java application and the JRE required to run it. The connector is installed as a service on Windows, and can optionally be registered for automatic restart.

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 HP-UX, only run installers using the same user that is used to run the application server. Ensure that `printenv` is in your path.

- On HP-UX , it is usually located in `usr/bin`.

Before Installing Select Audit

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

1. Install WebLogic 9.2 MP 1.
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.

If Select Audit has been previously installed on a machine, the uninstaller should be executed before attempting to install again to ensure a clean installation. For details on using the uninstaller, see To uninstall the Audit Server on page 63.

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. In the next step, a script is provided to create a new database user for use by the application. You must log onto the database server as a DBA user to run this script.

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.

`http://e-docs.bea.com/wls/docs92/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\weblogic92`.

   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.

XA Configuration Details

To properly coordinate distributed transaction processing between WebLogic and SQL Server 2005, XA Transaction processing is required.

To use XA data sources together with Microsoft Distributed Transaction Coordinator (MS DTC) for handling distributed transactions, you must configure the MS DTC service in SQL Server 2005. The MS DTC service should be marked **Automatic** in Service Manager to make sure that it is running when the SQL Server service is started. To enable MS DTC for XA transactions, follow these steps on your SQL 2005 server:

1. From **Control Panel**, open **Administrative Tools**, and then open **Component Services**.
2. Expand **Component Services**, right-click **My Computer**, and then select **Properties**.

3 Click the **MSDTC** tab, and then click **Security Configuration**.

4 Select the **Enable XA Transactions** check box, and then click **OK**. This will cause a MS DTC service restart.

5 Click **OK** again to close the **Properties** dialog box, and then close **Component Services**.

6 Stop and then restart SQL Server to ensure that it syncs up with the MS DTC changes.

You can configure the JDBC driver distributed transaction components by following these steps:

1 Copy the sqljdbc.dll and instjdbc.sql files from the WL_HOME\server\lib directory (of a WebLogic 9.2 installation) to the SQL_Server_Root/Binn directory of the MS SQL Server database server, where WL_HOME is the directory in which WebLogic server is installed, typically C:\bea\weblogic92.

2 Using Microsoft SQL Server Management Studio, click **New Query** and run the instjdbc.sql file as user "sa".

Setting Up The Database Schemas

Select Audit supports the following databases:

- Oracle 9i and 10g
- Microsoft SQL Server 2005

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 must 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 Microsoft SQL Server 2000 database server

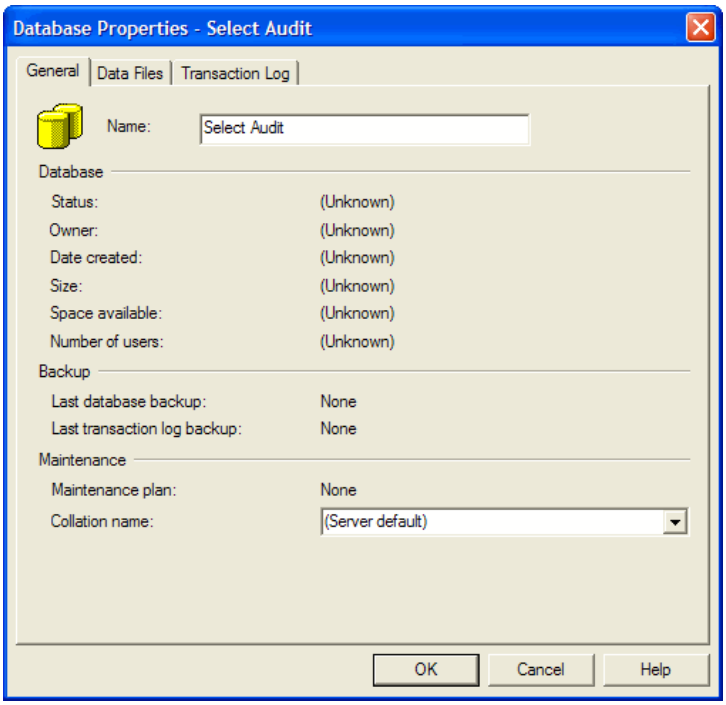
Before you install Select Audit, configure the MSSQL database using the Microsoft SQL Server Enterprise Manager interface.

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.



4 Type a name for the database, such as Select_Audit.

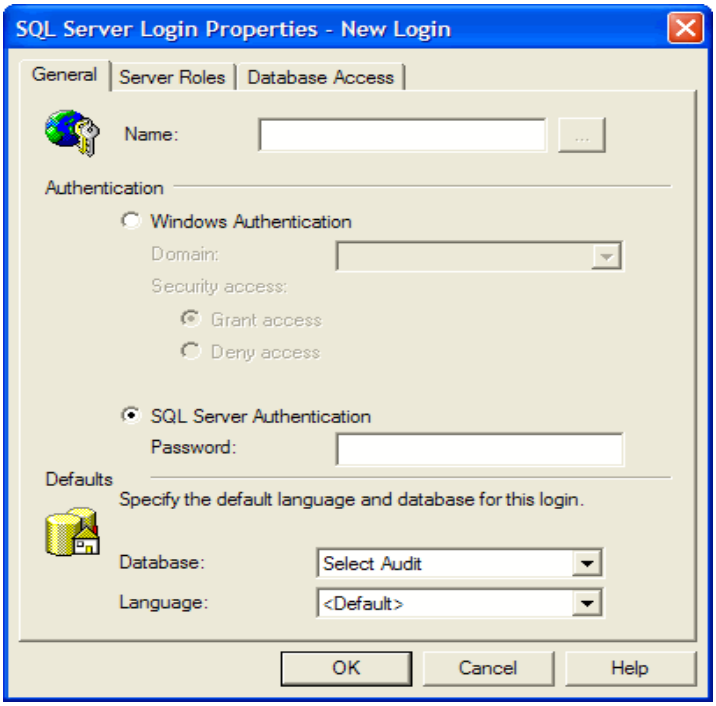
5 Click **OK** to finish creating the database.

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.



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 schema name.

— Replace `$DB_NAME$` with the name of the database you created in step 2.

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**.

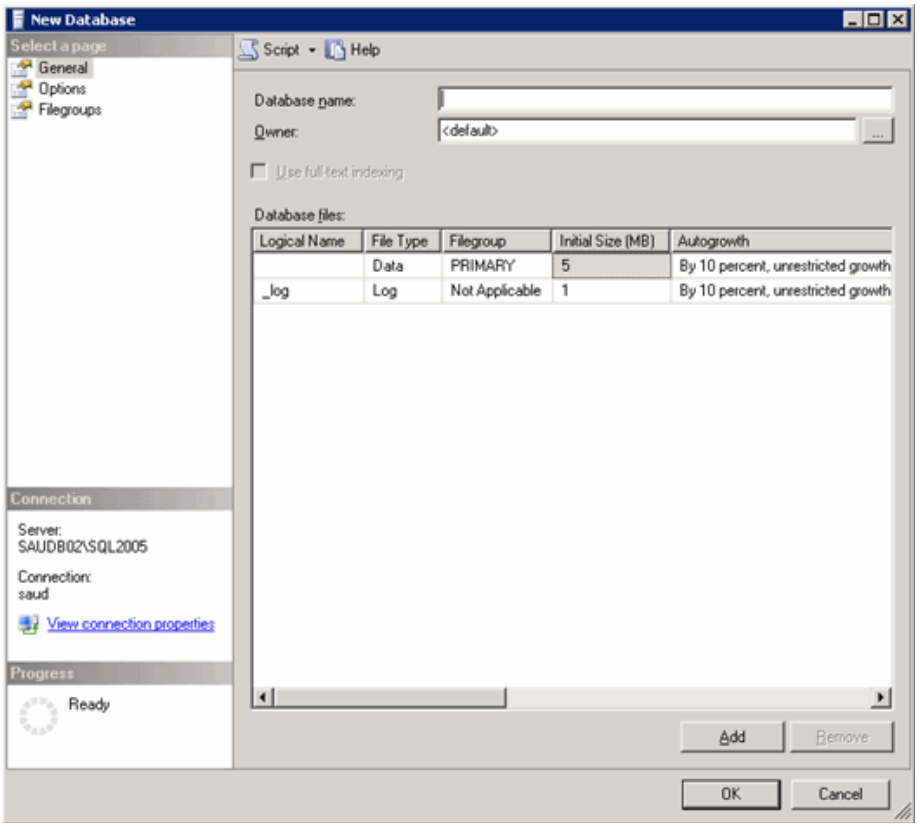
To configure the Microsoft SQL Server 2005 database server

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

1 Log in to the Microsoft SQL Server Management Studio.

2 On the left side of the Microsoft SQL Server Management Studio screen right-click the **Databases** folder and select **New Database**.

The **New Database** dialog opens.



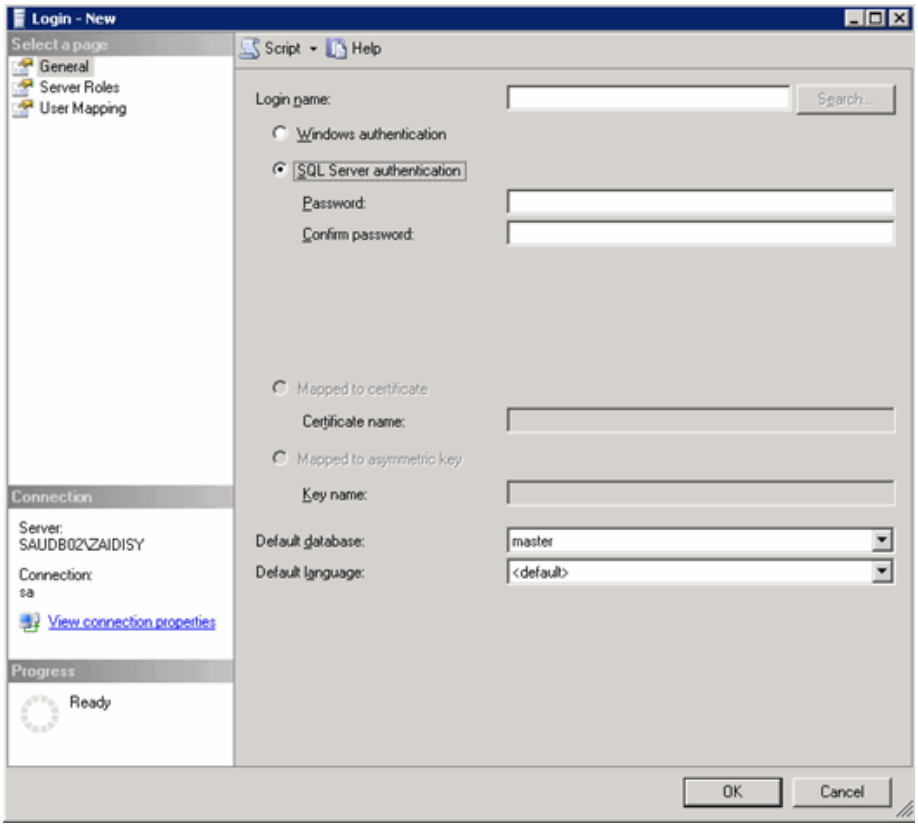
Type a name for the database, such as Select_Audit, and click **OK** to create the database.

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

a Expand the **Security** folder in the SQL Server Management Studio interface.

b Right click the **Logins** folder and select **New Login**.

The **Login - New** dialog opens.



c Type a user name such as SAud and select the **SQL Server Authentication** radio button as the authentication type. Enter and confirm a password for this account.

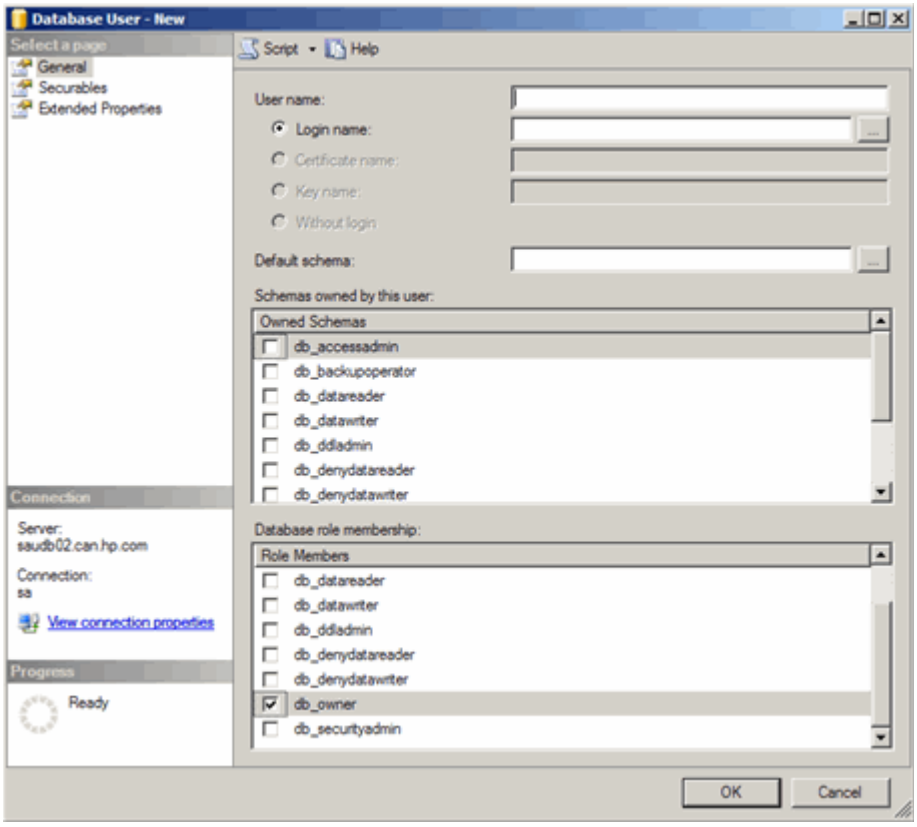
d Keep the remaining default settings and click **OK** to finish.

4 Configure the security settings for the new user account by completing the following steps:

a Expand the **Databases** folder in the SQL Server Management Studio interface and double-click on your new database.

b Double-click the **Security** folder and expand the **Users** folder.

c Right-click the **Users** folder and select **New User**. The **Database User - New** dialog opens.



Enter a **User name** and **Login name** values.

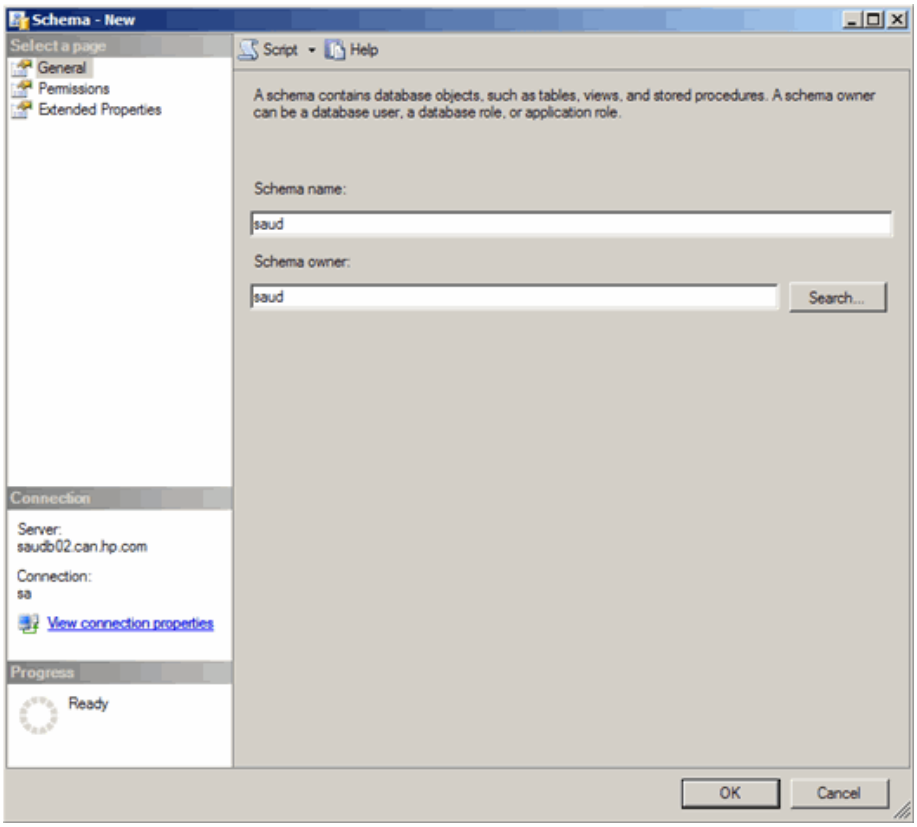
d Click the **db_owner** checkbox in the **Database role membership** section as pictured above.

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

5 Configure the database schema by performing the following steps:

a Expand your new database in the Microsoft SQL Server Management Studio interface and right-click the **Security** folder.

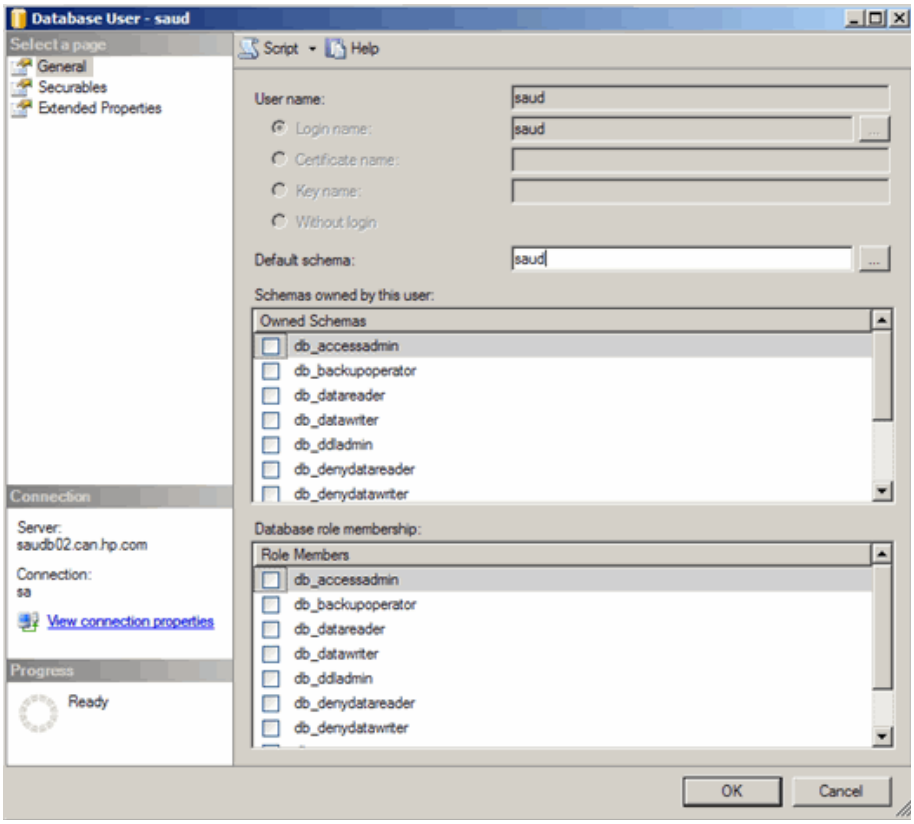
b Select **New** → **Schema** from the menu. The **Schema - New** panel displays.



Enter the **Schema name** and **Schema owner** values, and click **OK**.

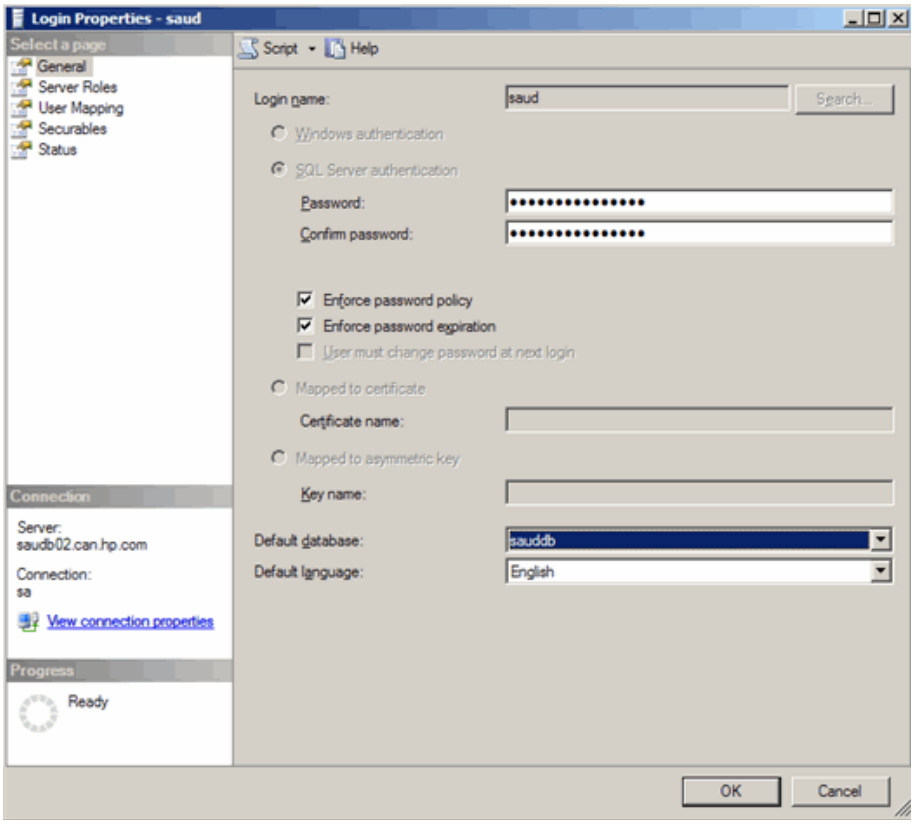
The **Schema name** you define **must** be the same as the database user name created in step 4 on page 21.

c Returning to the **Security** folder in step a above in the Microsoft SQL Server Management Studio interface, select **Security** → **Users** from the menu, and double-click the user you created in step 3 above. The **Database User** properties panel displays.



Enter the appropriate **Default schema** and click **OK**.

d Returning to the Microsoft SQL Server Management Studio interface, select **Security** → **Logins** and double-click the user you created in step 3 above and modify the **Default database** information.



Click **OK** to complete the login user account configuration.

6 Connect using SQL Server Authentication and the new login user ID and password you created earlier in this section. This should automatically select the new database created for Select Audit.

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

a Using the Microsoft SQL Server Management Studio interface, select **File** → **Open** → **File**. Select the `create_all.sql` script from the Select Audit database home directory. The script displays in the right-hand side of the screen.

b Edit the `create_all.sql` script by doing the following:

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

— Replace `$DB_NAME$` with the name of the database you created in step 2.

c Run the script by clicking **Execute** in the task bar.

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.

d Verify that no error message is shown.

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

a Using the Microsoft SQL Server Management Studio interface, select **File** → **Open** → **File**. Select the `init_all.sql` script from the Select Audit database home directory. The script displays in the right-hand side of the screen.

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

c Run the script by clicking **Execute** in the task bar. Messages in the console indicate that rows are being created.

d Verify that no error message is shown.

e Close the Microsoft SQL Server Management Studio interface.

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) if you are using an external LDAP server. If you are using WebLogic embedded LDAP, the groups will be created by the installer. The installer maps the roles to these 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. As above, this group should be created in your LDAP if you are using an external LDAP server. If you are using WebLogic embedded LDAP, the group will be created by the installer. Users in the Report Developers group must also belong to one of the three standard groups to be granted login access. They have access to the Developer Center and to error output from reports.

Integrating with Select Identity

Select Identity (SI) can be configured with Select Audit such that Select Audit can report and model Select Identity audit data, and Select Identity permissions can be applied to Select Audit users to control the flow of information.

Auditing Select Identity Data with Select Audit

Select Identity is configured to send audit event data to a Select Audit connector. This enables users to:

- Pass Select Identity request, transaction, configuration, and maintenance data into Select Audit for complance auditing in Sarbanes-Oxley and other regulatory settings (HIPAA does not apply here).
- Incorporate data from the Select Identity XML audit data stream into a wide range of reports.

Filtering Select Audit Reports using Select Identity Entitlements

Select Audit is configured to filter results based on a user's entitlements in Select Identity, and allows Select Identity administrators to view configuration reports in Select Audit, depending on the access rights they have for Select Identity configuration reports. The Select Audit reports filter by the managed service and the context of the Select Identity administrator; you can only see reports for users and services you manage.

Requirements and Recommendations

The following guidelines apply to integrated Select Identity-Select Audit systems:

- Select Identity and Select Audit should be installed in separate Web Application Server domains.
- Select Audit must be able to connect to the Select Identity database.
- For auditing, Select Identity must be able to send data to Select Audit via the port on which the Select Audit agent listens.

The Select Identity Installation Guide contains a section that specifically covers Select Audit integration. Technicians working on each side should be familiar with the other's documentation in addition to their own.

Filtering can be set up in the following scenarios:

- During Select Audit installation, using the Select Identity configuration options that are built into the Select Audit installer.
- On an established system. In this case, Select Identity integration configuration resides in the Select Audit user interface.

  ➤ Ensure that there are pre-existing Select Identity user accounts corresponding to those with access from Select Audit; you must create these on the Web application Server.

If you are integrating with Select Identity, 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 1.1 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

Select Audit Authentication Options

User Name and Password with non-SSL

The user name and password are sent in plain text.

- Select Identity: no specific configuration is needed.
- Select Audit:
  - Key store and trust store are not required.
  - Select Identity filtering is required. When configuring, SSL should be disabled, and user name and password should be entered.

User Name and Password with SSL enabled

Select Identity still authenticates Select Audit using a password. Select Audit sends the user name and password to Select Identity using SSL.

- Select Identity:
  - Requires key store and trust store for the Select Identity server.
  - WebLogic must be configured to enable SSL.
  - Security Setup is required on the Select Identity server, but with the Security Level set to **None**.

  For details, see Select Identity Server Configuration on page 29.
- Select Audit:
  - Requires a trust store for the Select Identity server. Either the Select Identity server certificate or the certificate's signer certificate must be in the trust store.
  - Filtering must be enabled in Select Identity. To do this, SSL must be enabled, trust store information is required, and user name/password authentication is required. If CRL verification is enabled, the Select Identity server certificate must *not* be revoked and must contain a CRL url.

  For details, see Select Audit Configuration on page 37.

Using Certificates (with SSL enabled)

Select Audit will send a certificate to identify itself, and Select Identity will compare and verify the certificate with the certificate associated with the user record. This process requires SSL be enabled.

- Select Identity:
  - Requires both a key store and trust store for the Select Identity server. The client certificate sent by Select Audit must be in the trust store.
  - WebLogic must be configured to enable SSL. The "Client Certificate Required" must be selected as the Security Level. If Certificate Usage Validation is enabled, ensure the client certificate has TSL Web Client Authentication usage. If CRL checking is enabled, ensure the client certificate has a HTTP-based CRL url and that the certificate is not revoked.

— When configuring security in Select Identity, ensure the certificate associated with the administrator is the same as the one sent by Select Audit.

For details, see Select Identity Server Configuration on page 29

- Select Audit:
  - — Requires trust store configuration. Either the Select Identity server certificate itself or the certificate's signer certificate must be in the trust store.
  - — Requires key store configuration. The key store should contain the certificate sent by Select Audit.
  - — Enable Select Identity filtering. SSL must be enabled, and valid key and trust store information must be entered. Certificate Authentication must be chosen with valid configuration information entered. If CRL Verification is enabled, ensure the Select Identity server certificate is not revoked and contains a CRL url.

  For details, see Select Audit Configuration on page 37.

About CRL Validation

Loading CRL may be quite time consuming in an enterprise environment. Both Select Identity and Select Audit can cache the CRL list and allow customers to specify the reload interval. If the interval is set to zero, the CRL list will not be cached and will be loaded every time CRL verification is needed.

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.

To integrate both the Select Identity and Select Audit configuration changes to the WebLogic startup script, edit the Select Identity script

`<si_install_dir>/WebLogic/scripts/weblogic/myStartWL`

to call the Select Audit script,

`<domain_dir>/startWLSelectAudit`

in place of the default `<domain_dir>/startWebLogic` script.

Select Identity Server Configuration

Depending on the authentication option chosen between Select Audit and Select Identity (listed in Select Audit Authentication Options on page 28) you may not need to complete all these steps.

Creating a Key Store and Trust Store for the Select Identity Server

This keystore is used to store the mutual authentication key pair, and is configured as follows:

1. Run the keytool utility to create a keystore and a key pair. When you create a key pair, a keystore is automatically created during this process.

2 Generate a certificate request file, as shown in this command line example which creates an X.509 certificate request file at `./req/myReq.csr` for a certificate at `myKeyAlias` in the keystore:

```
keytool -certreq -keyalg RSA -alias myKeyAlias -file ./req/myReq.csr
-keystore ./ks/myKeystore -storetype JKS
```

3 Send the new request file to your certificate authority for digital signing.

4 Import the signed certificate back to the keystore from which you generated the certificate request. The following command line example imports the signed certificate file `./signed/signedCert.pem` to `ks/myKeystore` at the key alias named `myKeyAlias`:

```
keytool -import -trustcacerts -alias myKeyAlias -file ./signed/
signedCert.pem -keystore ./ks/myKeystore -storetype JKS
```

5 Import the signed certificate to the appropriate truststore. The following command line example imports the signed certificate file `./signed/signedCert.pem` to `ks/mytruststore` at the key alias named `myKeyAlias`:

```
keytool -import -trustcacerts -alias myKeyAlias -file ./signed/
signedCert.pem -keystore ./ks/mytruststore -storetype JKS
```

6 Select Identity uses java property files to identify keystores. Generate the property files for the keystore and/or truststore by executing either genprop.sh (HP-UX) or genprop.bat (Windows).

When prompted to specify the file type to generate, select the appropriate option:

— For keystores, select option **2: OVSI secure object migration keystore**

— For truststores, select option **3: OVSI truststore**

7 Register the keystore and/or truststore on the application server.

8 Register the keystore and/or truststore property files in Select Identity. For more information refer to the *HP Select Identity Administration Online Help*.

9 The Select Audit server's certificate must be registered in the Select Identity trust store.

Configuring WebLogic to Enable SSL

Perform this procedure to configure WebLogic system security parameters and enable mutual authentication functionality.

A best practice recommendation is to use a new keystore to avoid having to change an existing keystore for other applications that may be implemented already.

Prerequisites

The following conditions must be met before you can perform this procedure:

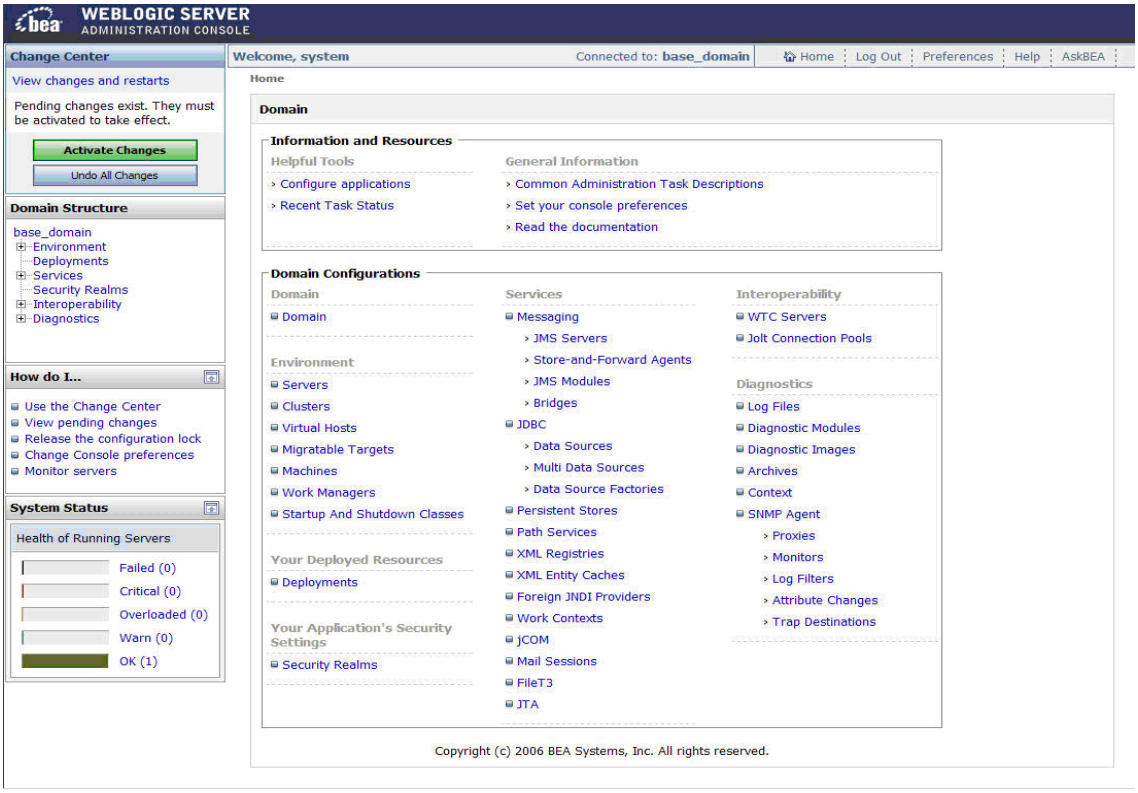
- You have administrative privileges to the WebLogic server.
- You know the keystore and truststore file locations.
- You know how your business uses SSL and Select Identity.
- You have identified whether you will be using Select Identity in secure or regular HTTP mode.
- You have determined if Select Identity is running in secure mode only.

Procedure – Single Server

To configure a single WebLogic server to enable mutual authentication, perform the following steps:

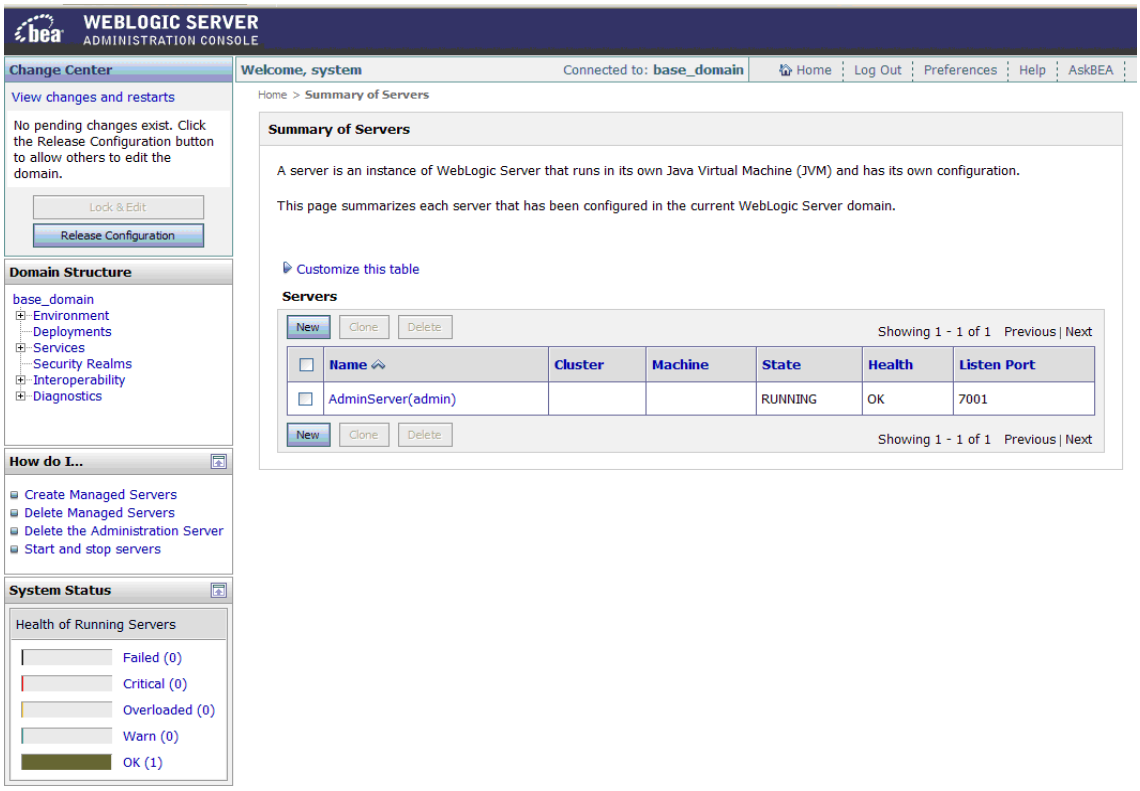
1 Log in to the **WebLogic Server Console**.

Figure 1 WebLogic Server Console



2 From the **Domain Structure** panel, navigate to **<My Domain>** → **Environment** → **Servers.** The **Summary of Servers** page displays, containing a list of all servers that are available.

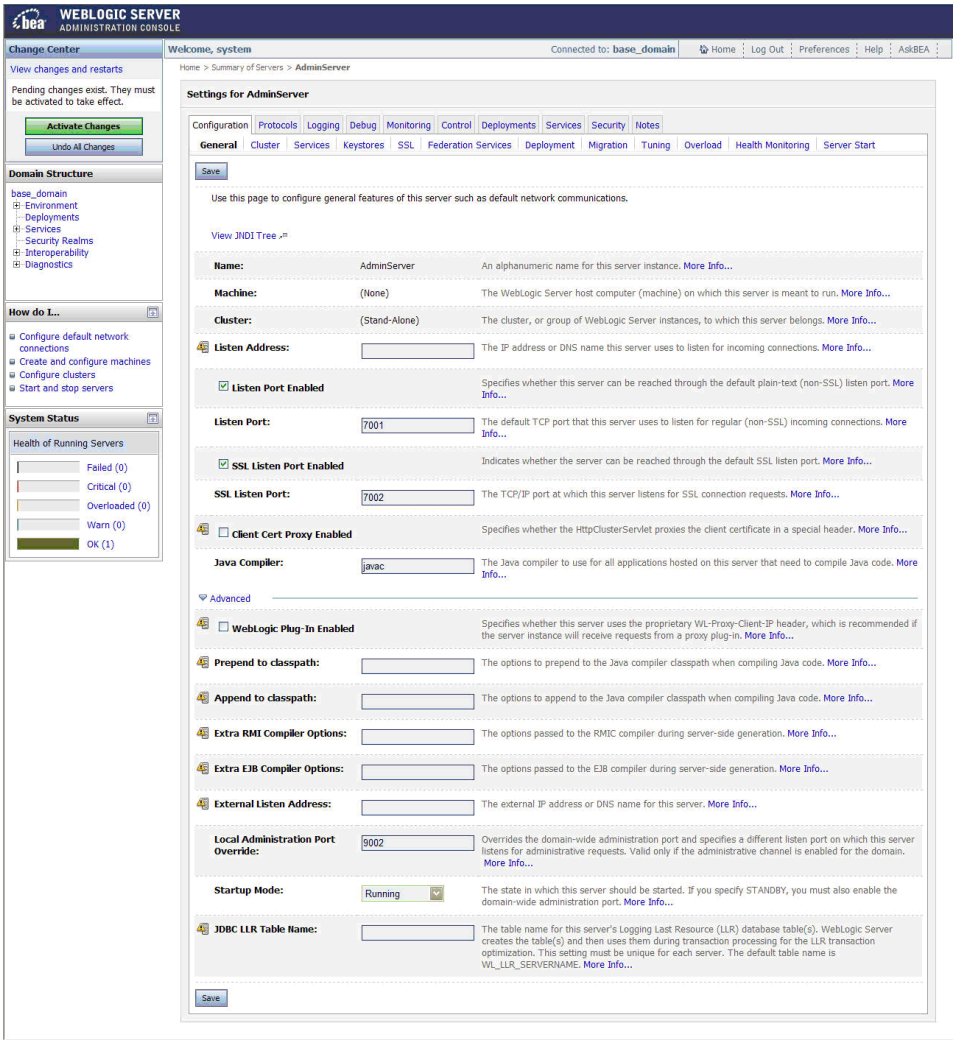
Figure 2 Summary of Servers



3 Select the server you want to configure. In this example, select **AdminServer(admin)**.

The **Settings for <Your Admin Server>** page opens. Click **Lock & Edit** to enable data entry on this screen. You will use this page to configure general features of this server such as the default network communications.

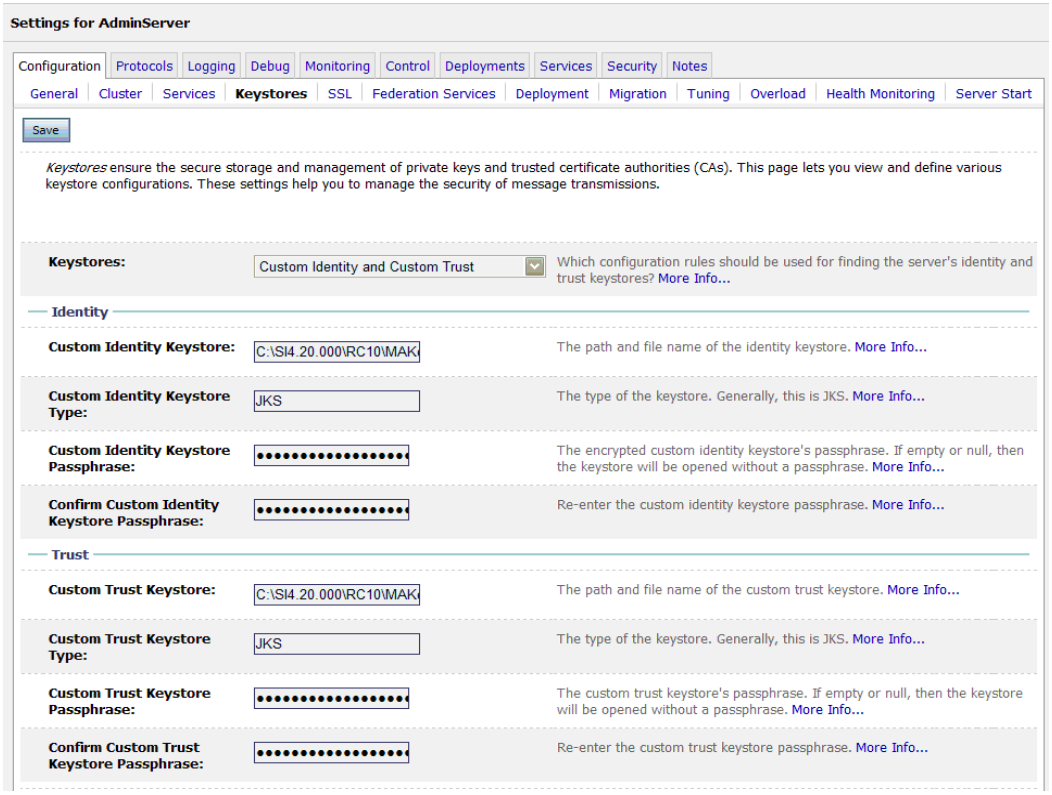
Figure 3 Settings for <Your Admin Server>



4 Click the **Configuration** → **KeyStores** tab.

The **Keystores** page opens.

Figure 4 Keystores Tab



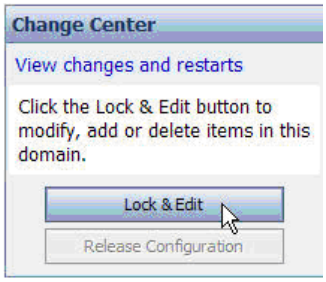
Keystores ensure the secure storage and management of private keys and trusted certificate authorities (CAs). The **Keystores** page allows you to view and define keystore configurations. These settings help you manage the security of message transmissions.

After you configure identity and trust keystores for a WebLogic server instance, you can configure its SSL attributes. These attributes include information about the identity and trust location for particular server instances. You will use the **Configuration: SSL** page (discussed later in this section) to identify this information.

5 On the **Change Center** panel, click **Lock & Edit**.

This allows you to make changes to the page. After you make changes, the option name temporarily changes to **Activate Changes**.

Figure 5 Lock & Edit Button



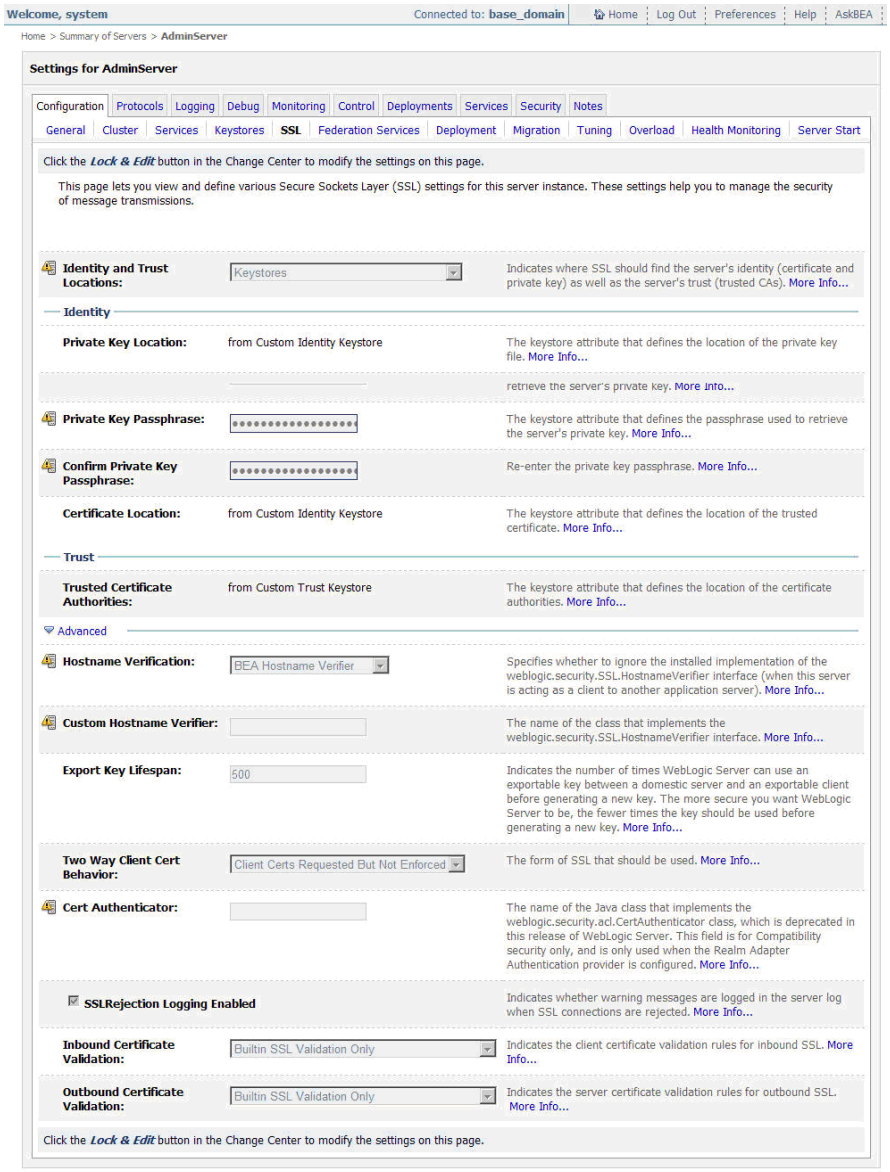
6 In the **Identity** and **Trust** sections, enter the appropriate values.

7 Click **Save**, and then click **Activate Changes**.

8 Click the **SSL** tab.

The **SSL Configuration** page opens. This page enables you to view and define SSL settings for this server instance.

Figure 6 SSL Configuration



9 Be sure the **Two Way Client Cert Behavior** field is set to **Client Certs Required But Not Enforced**.

10 On the **Change Center** panel, click **Lock & Edit**.

11 Enter the appropriate values for the **SSL Configuration** page.

12 Click **Save**, then click **Activate Changes**.

A success message displays under the tabs.

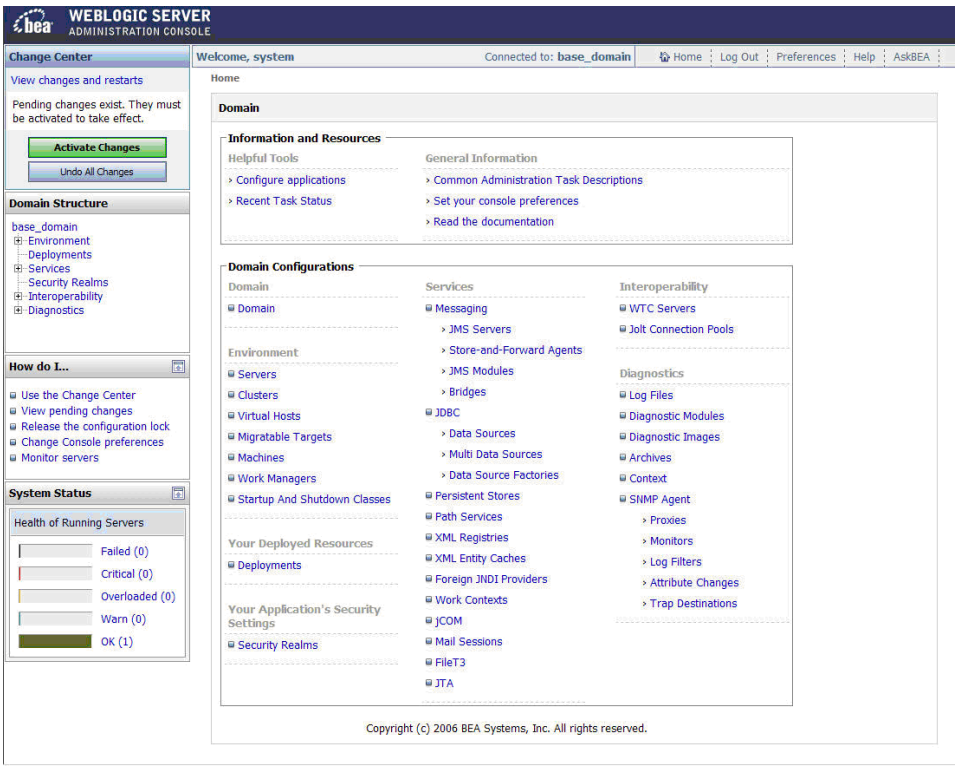
13 To configure the Select Identity security setup to use the keystore and truststore, use the Select Identity user interface. For more information, refer to the *HP Select Identity Administration Online Help*.

Procedure – Clustered Servers

To configure a cluster of WebLogic servers to enable mutual authentication, secure object migration, and key rotation functionality, perform the following steps:

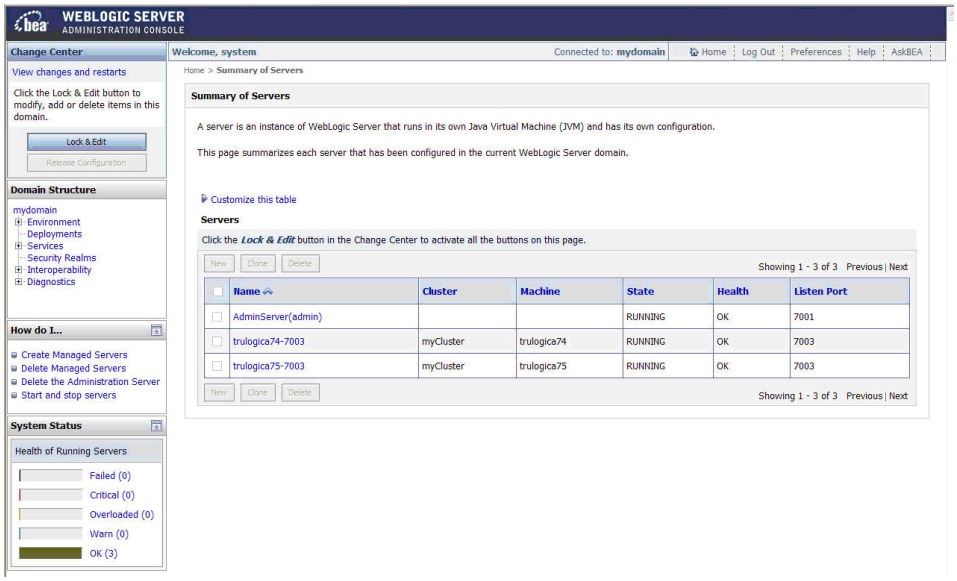
1 Log in to the **WebLogic Server Console**.

Figure 7 WebLogic Server Console



2 From the **Domain Structure** panel, navigate to **<My Domain>** → **Environment** → **Servers.** The **Summary of Servers** page displays, containing a list of all servers that are available.

Figure 8 Summary of Servers



You can now see the server and the cluster group, which in the above example, displays two servers that are part of the cluster.

3 Click the admin server and configure the keystore and truststore information by following the procedure that you used to configure a single server. (See steps 5-12 for configuring a WebLogic single server.)

4 Configure the keystore and truststore information for each server in the cluster by following the procedure that you used to configure a single server.

5 To configure the Select Identity security setup to use the keystore and truststore, use the Select Identity user interface. For more information, refer to the *HP Select Identity Administration Online Help*.

When installing keystores, you can verify your installation by turning on the WebLogic auto debugging property. For more information about how to do this, refer to your WebLogic reference materials.

Configuring Select Identity Security

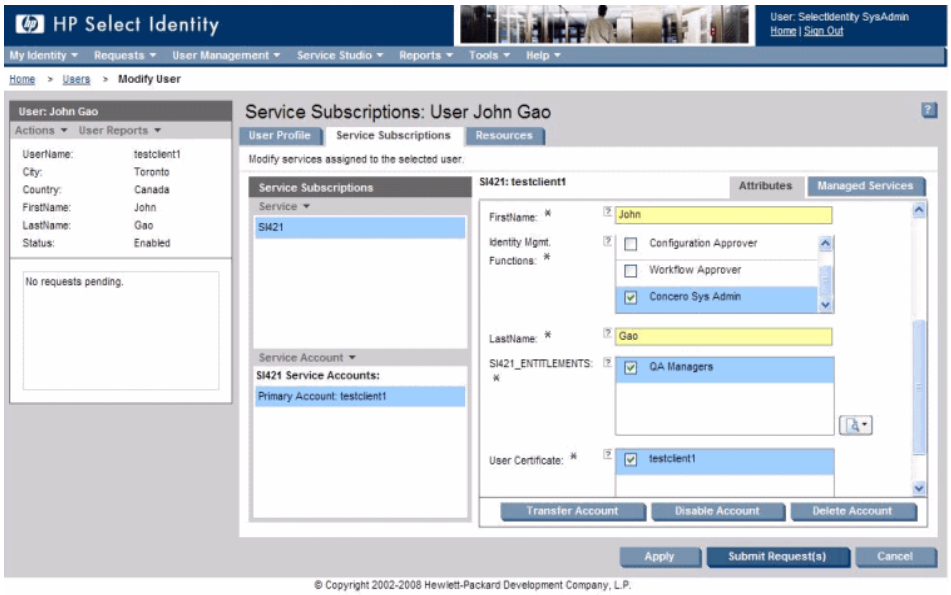
Perform the following tasks while logged on as **sisa** on the Select Identity server:

1 Go to **Tools** → **System Security** → **Security Setup** and import the key store and trust store by providing the property files.

2 Go to **Certificate Policy** and choose the appropriate Security Level and other options as appropriate for the chosen authentication options.

Creating a Select Identity Administrator and Certificate Configuration

1 In Select Identity, create a Select Identity user as a member of the Administration service. Make sure this user has the Identity Management function Concero Sys Admin. Assign this user a user certificate to be used by the Select Audit server for authentication using mutual authentication (using a User Certificate), as shown in the following screen:

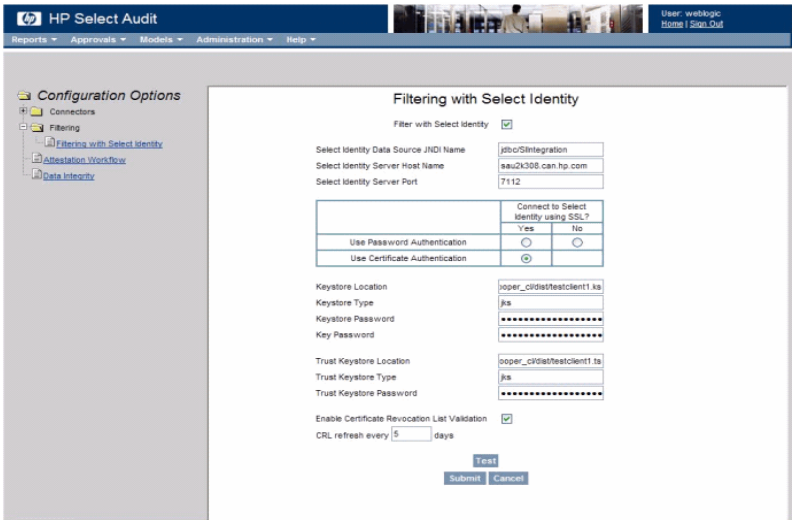


Select Audit Configuration

Depending on the authentication option chosen between Select Audit and Select Identity (listed in Select Audit Authentication Options below) you may not need to complete all these steps.

Select Audit Configuration Options

1. Set up a trust store. The trust store is used to verify the Select Identity server's certificate. It is needed when SSL is enabled between Select Audit and Select Identity. Either the Select Identity server certificate itself or the certificate's signer certificate must be in the trust store.
2. Set up a key store. The key and certificate used by Select Audit must be in the key store.
3. Enable Select Identity filtering through the Select Audit configuration page in the audit portal, as shown in the following screenshot:



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.

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.

To run Select Audit in a clustered environment, note the following:

IMPORTANT: In order to run Select Audit in a clustered environment, load balancing *must* be enabled. For details, see Enabling Load Balancing for Clusters on page 60.

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.

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 Select Audit 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.

  If the installer is cancelled for any reason, run the uninstall utility immediately (see To uninstall the Audit Server on page 63) or manually delete the entire installation directory. If this cannot be done, delete the WebLogic config and keyfile from `<install_dir>/setup` and remove any passwords from `<install_dir>/uninstall_Select_Audit/installvariables.properties`.

OR

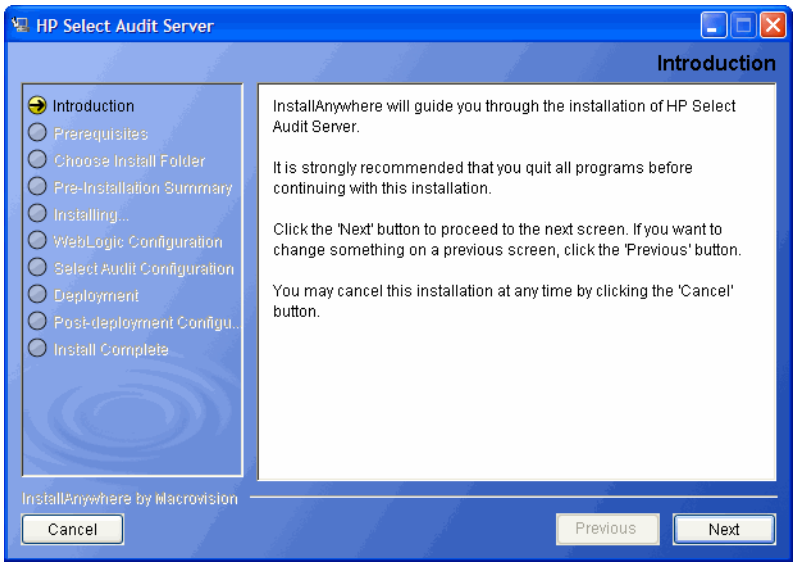
- **On HP-UX:**

  Type the following command:

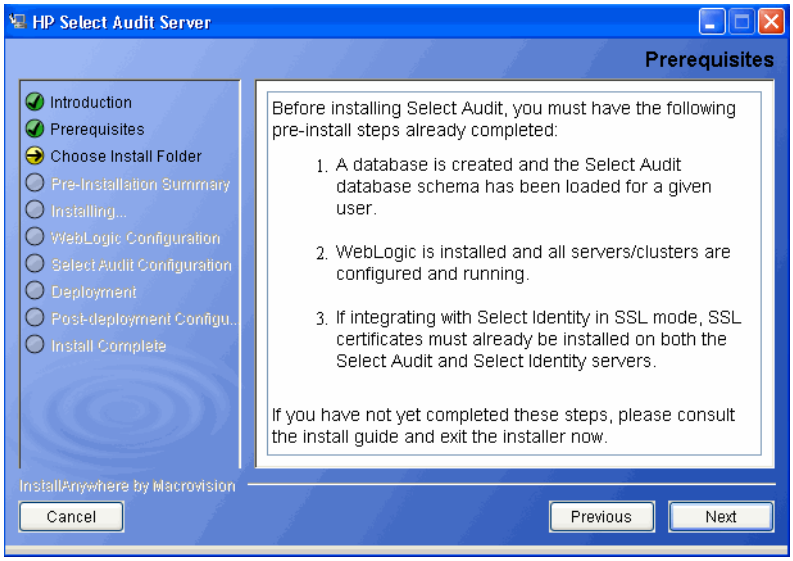
  `./SelectAuditServerWLInstall.bin`.

  You should be logged in as the same user that the WebLogic Server is running under.

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.

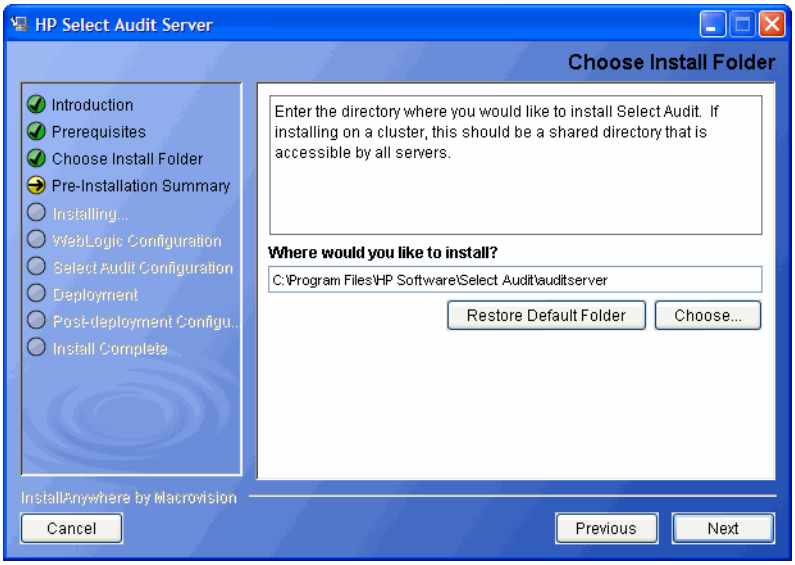


2 Click **Next**. The **Prerequisites** screen opens.



3 Review the listed prerequisites and confirm they have been met before proceeding. To review the pre-installation steps, see Chapter 2, Pre-Installation Information.

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



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

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

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

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.

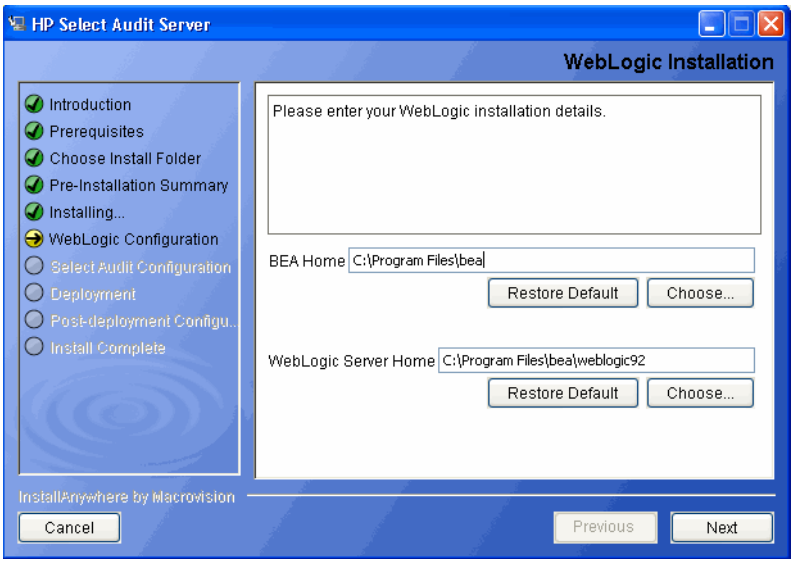
- The installation location of the Java Virtual Machine that the Select Audit Install wizard has automatically installed. The Java Virtual Machine is required to run the installer and the uninstaller only; it is not required for other Select Audit components.
- The amount of disk space required for the 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.

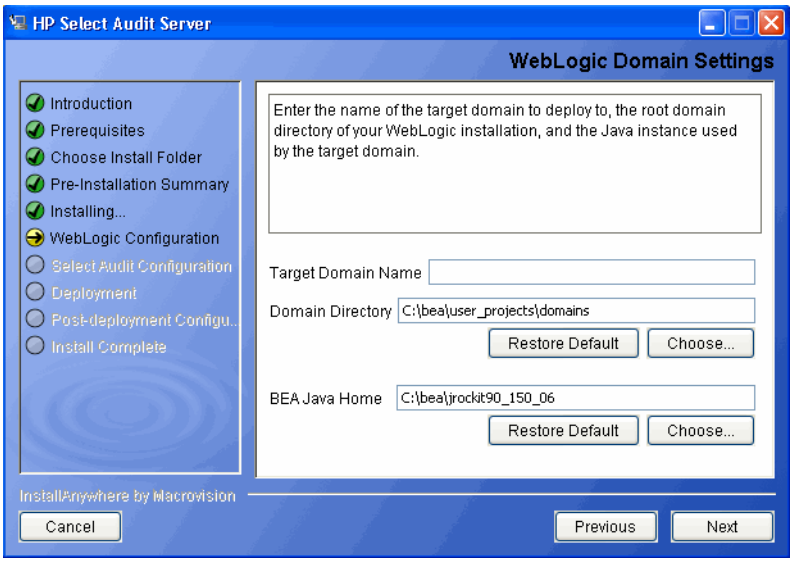
The Audit Server begins to install and the **Server Installation Progress** screen opens.

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



8 Select your WebLogic home directory and WebLogic Server directory by clicking **Choose** beside each field.

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



Note: Before restarting the servers in Task 36 on page 55:

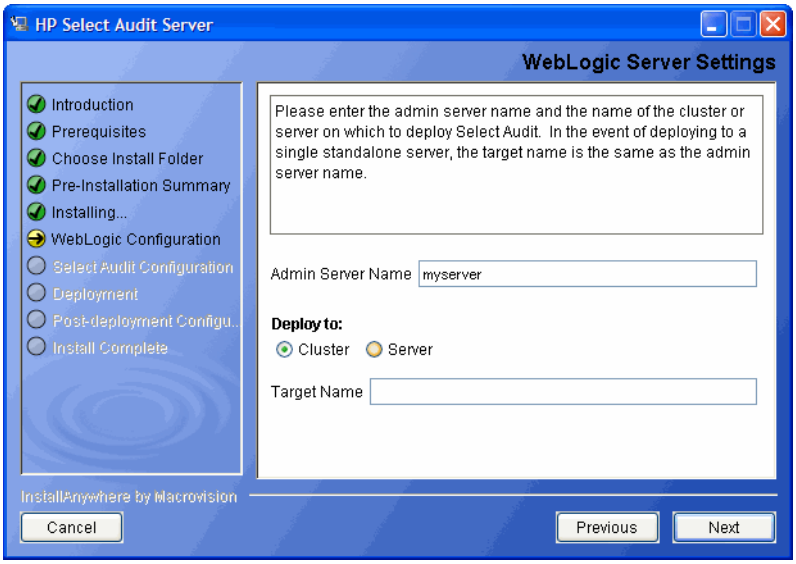
If there are remote servers installed on a different path than the **BEA Java Home** directory, open the WebLogic console and edit the Server Start settings for each remote server to ensure that **BEA Home**, **Java Home**, **weblogic.jar** and **tools.jar** are pointing to the correct path.

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.



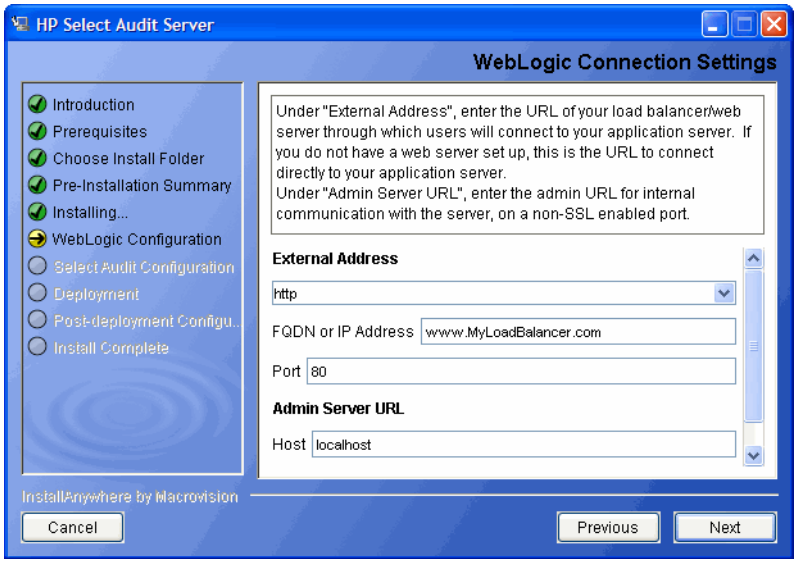
12 Do the following:

- 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.



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 Administration server port number of the in the **Port** field.
- Type the administration URL that will be used for internal communication to the administration server from the managed servers and the installer in the **Host** field.

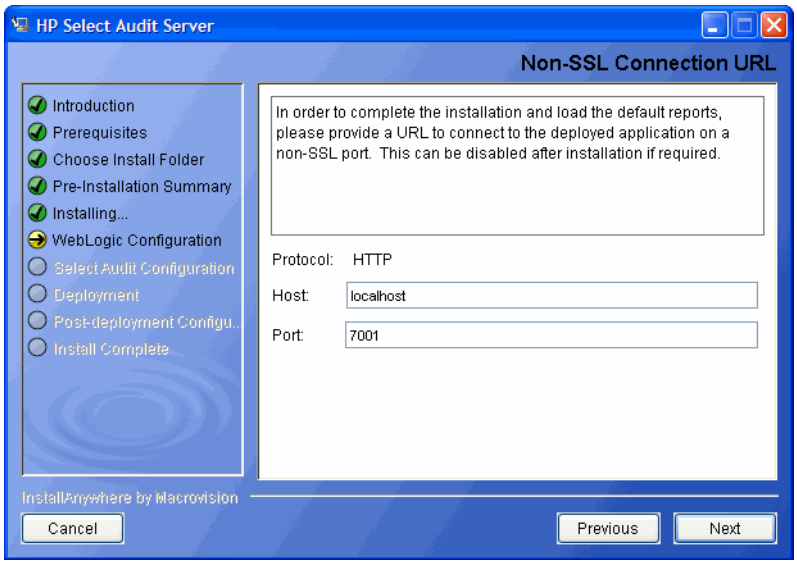
> If a web server has not been set up, enter the URL of one of the managed servers where the application will be deployed, and configure the load balancer after installation is complete. For details, see Post-Installation Steps on page 59.

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.

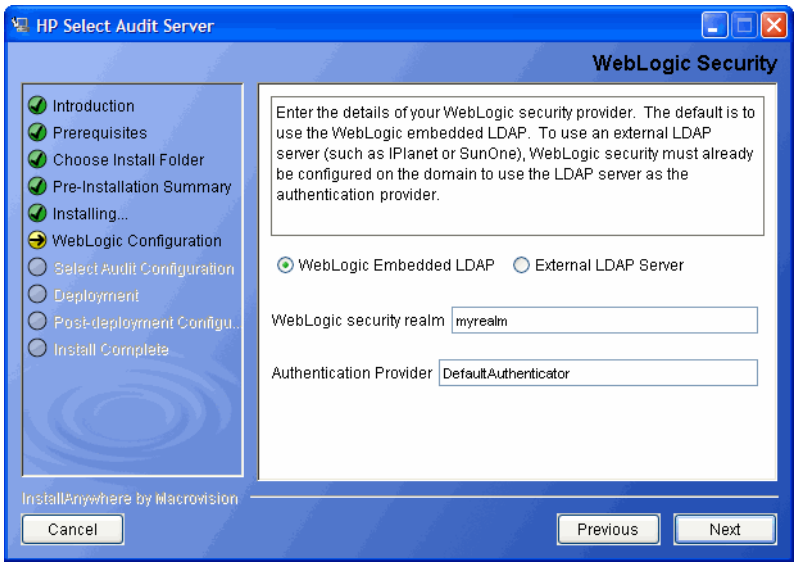
> Import the CA certificate to the `cacerts` file used as the trust store for your Java Virtual machine. You can often use the keytool utility to do this:

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



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

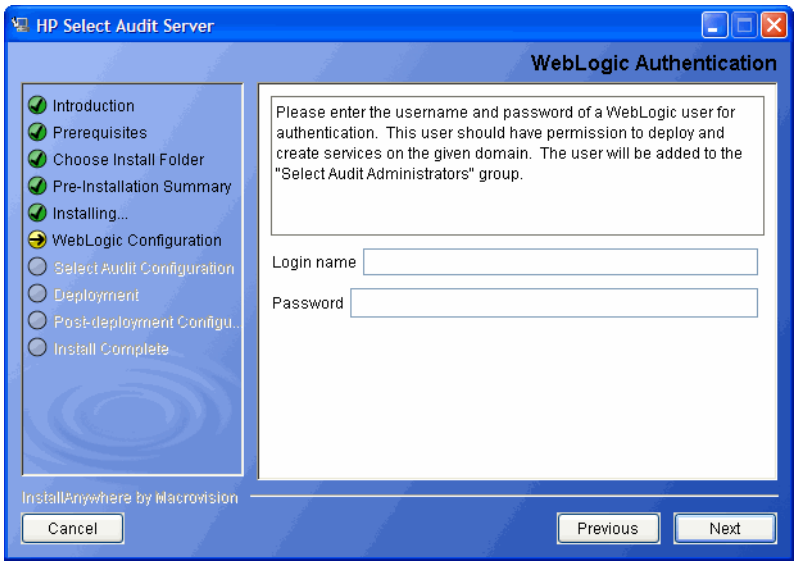
17 Click **Next**. The **WebLogic Security** screen opens.



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.

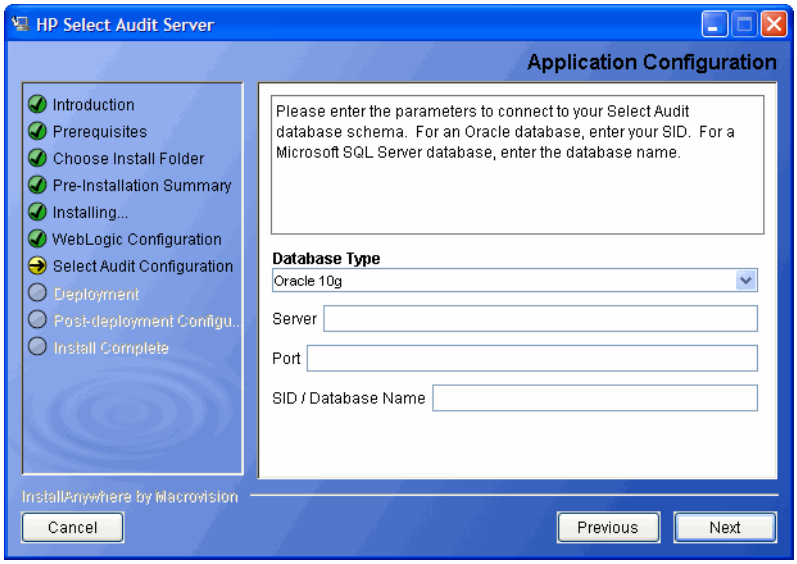
19 Click **Next**. The **WebLogic Authentication** screen opens.



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.

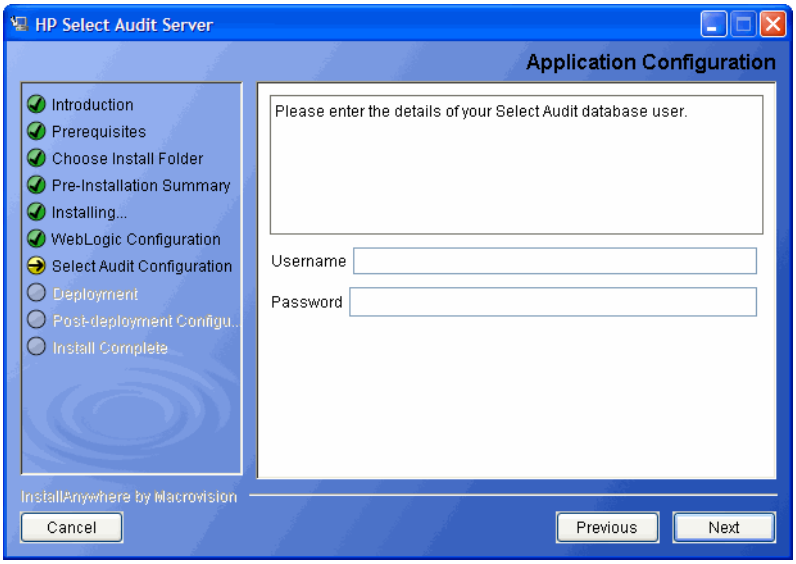
21 Click **Next**. The **Application Configuration** screen opens.



22 Enter the database connection parameters as follows:

- Select your database type (Oracle 10g/9i or Microsoft SQL Server 2005/2000) 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.

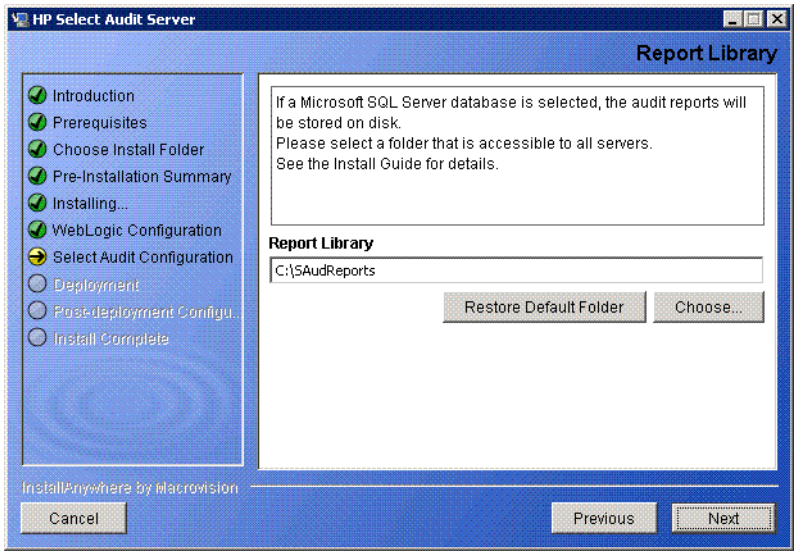
23 Click **Next**. The **Application Configuration** log-on information screen opens.



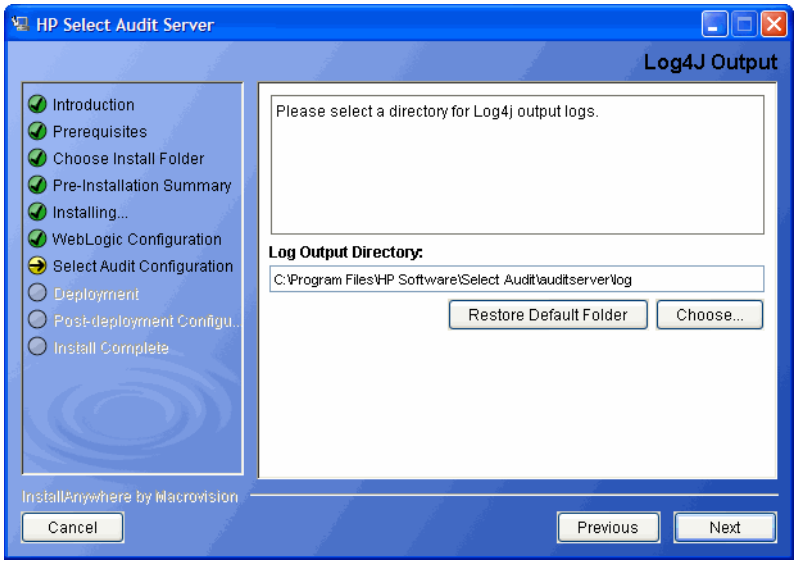
24 Type your database user name in the **Username** field and your database password in the **Password** field.

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.



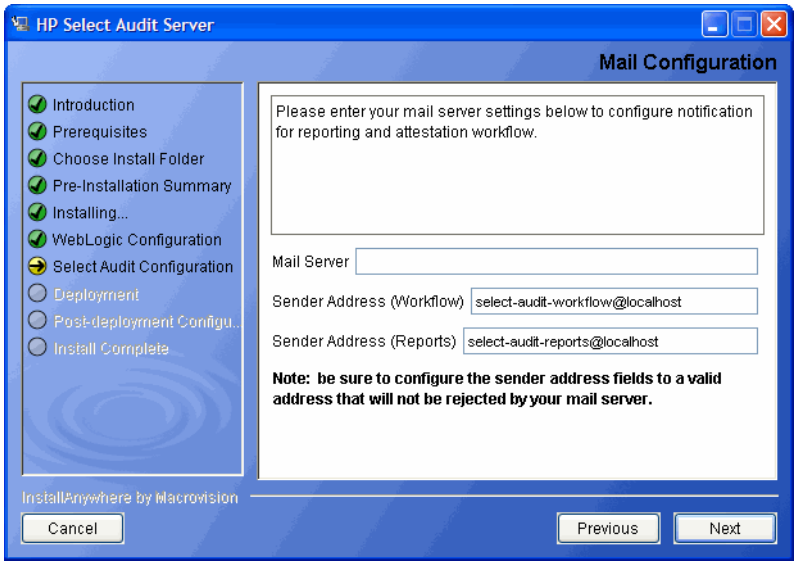
26 Select a location for the audit reports and click **Next**. The **Log4J Output** screen opens.



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.



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. During installation, **Mail Server** and **Sender Address (Workflow)** entries are stored in

  `<install_dir>/dist/config/properties/workflow.properties`

These parameters are stored as:

```
mail.smtp.host=[host-name]

mail.from=[sender-address]
```

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

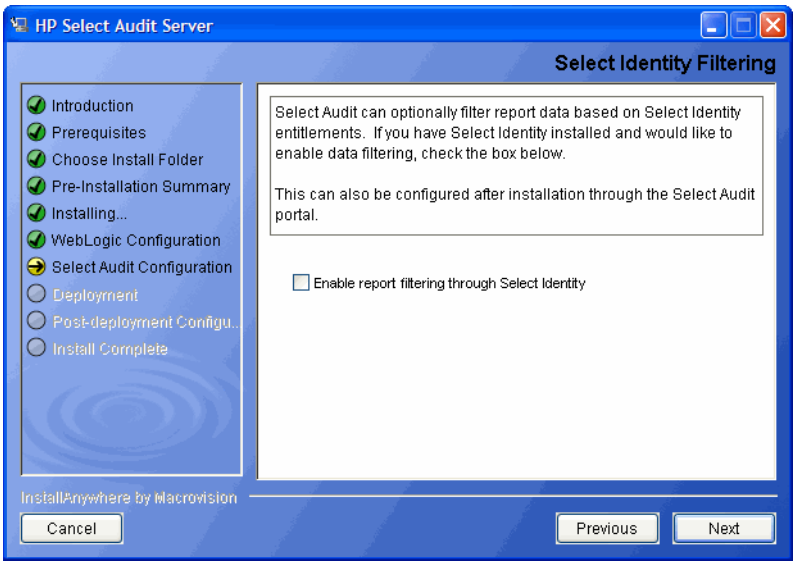
Also, open

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

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

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

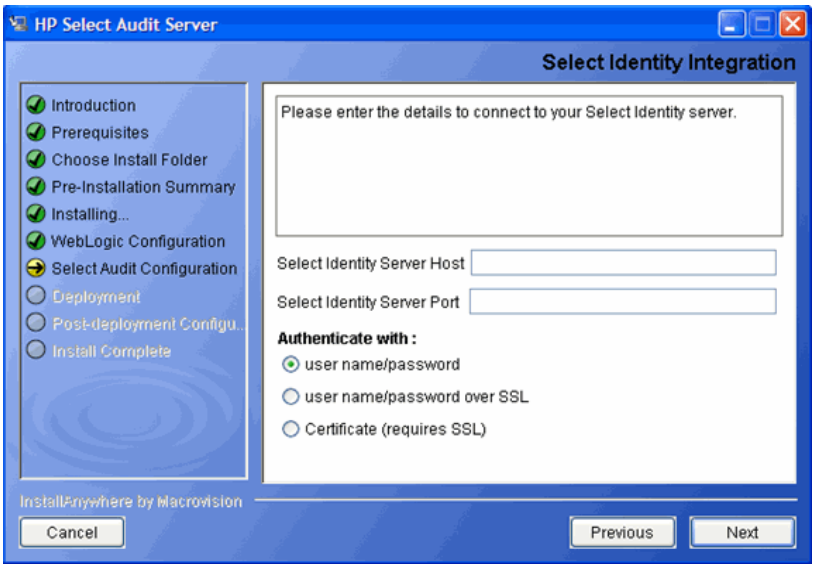
30 Click **Next**. The **Application Configuration** Select Identity filtering screen opens.



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 1.1 Administration Guide* for more information about integrating Select Audit with Select Identity.

32 Do one of the following:

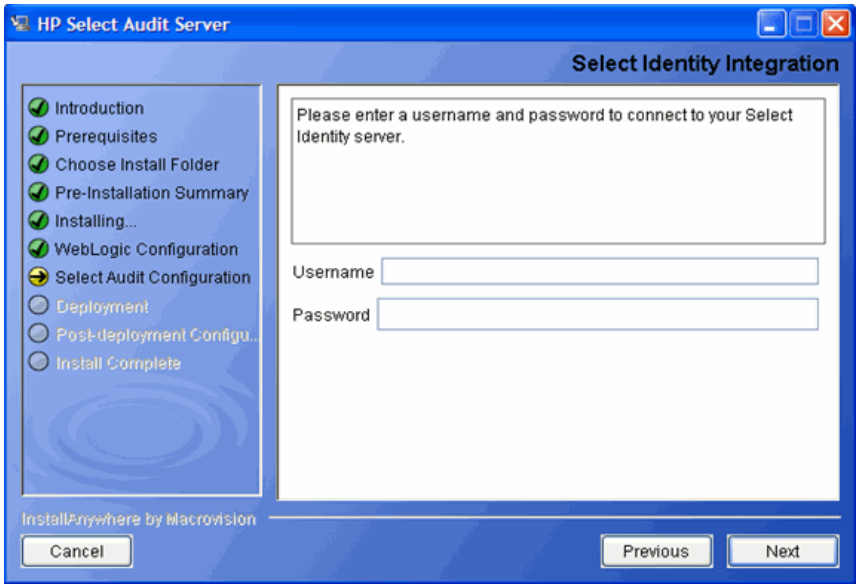
- To integrate with Select Identity, select the **Enable report filtering through Select Identity** checkbox and click **Next**. The **Select Identity Integration** screen opens.
- If you decide not to integrate with Select Identity, click **Next** and go to step 36.



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.
- Select a radio button to configure authentication using **username/password**, **username/password over SSL**, or **certificate (requires SSL)**. Based on your choice, the following screens open when you click **Next**:

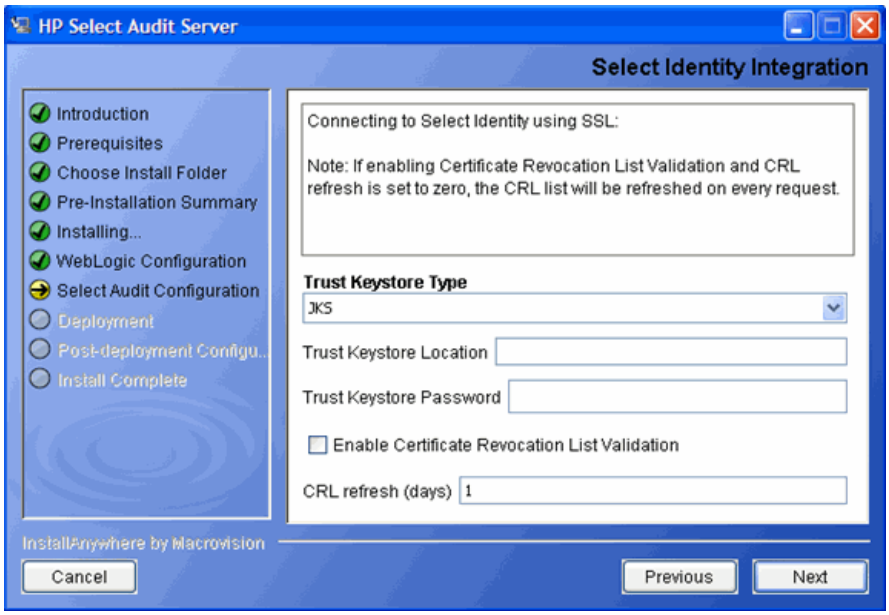
Username/Password



Enter the Select Identity server **Username** and **Password** and press **Next**. Proceed to step 34.

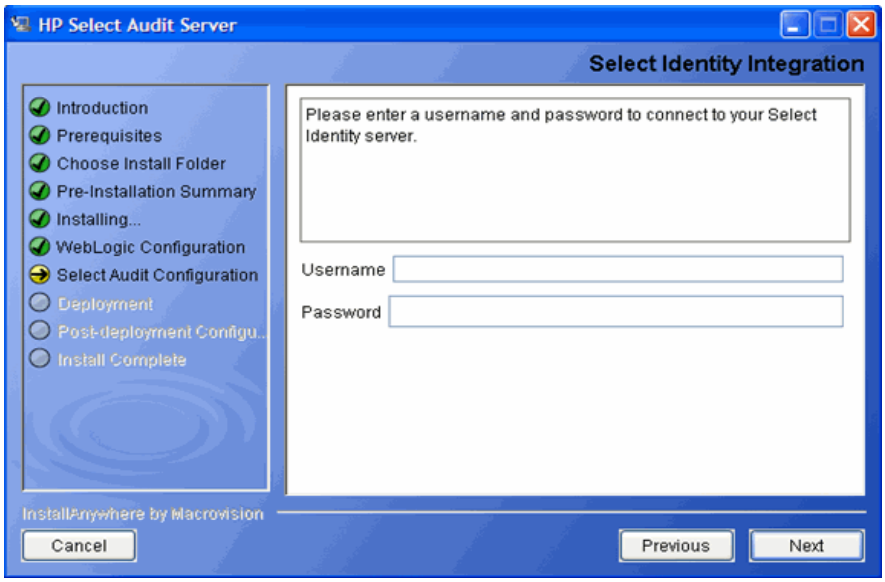
Username/password over SSL

First you are advised that you must obtain the SSL port number from your SI server. Then, the following screen displays:



Select a **Trust Keystore Type** from the dropdown list. Then, specify the **Trust Keystore Location** and **Trust Keystore Password**. Finally, select the **Enable Certificate Revocation List Validation** checkbox if desired, and specify the **CRL refresh** rate.

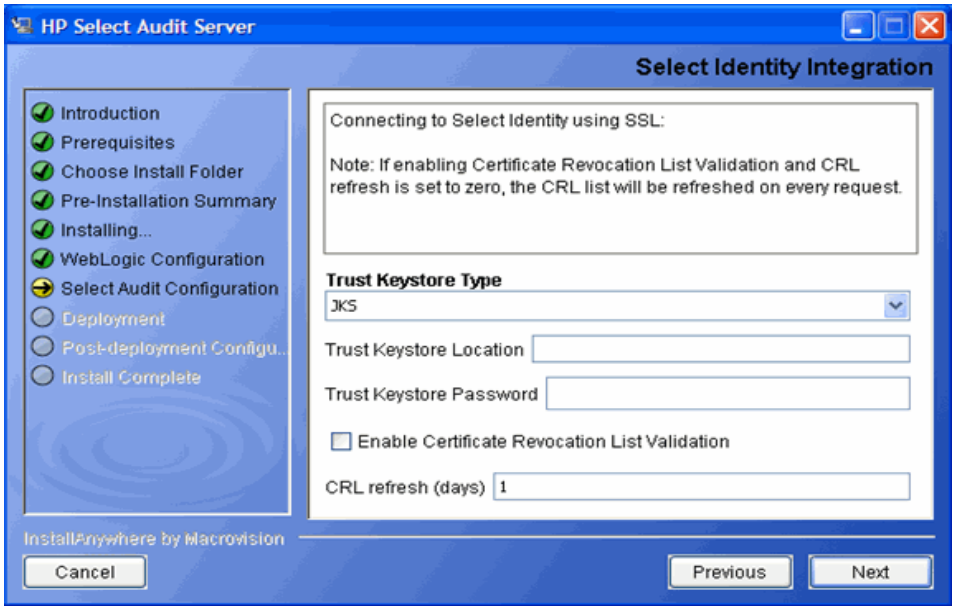
Click **Next** to proceed to the Select Identity server connection screen.



Enter the Select Identity server **Username** and **Password** and press **Next**. Proceed to step 34.

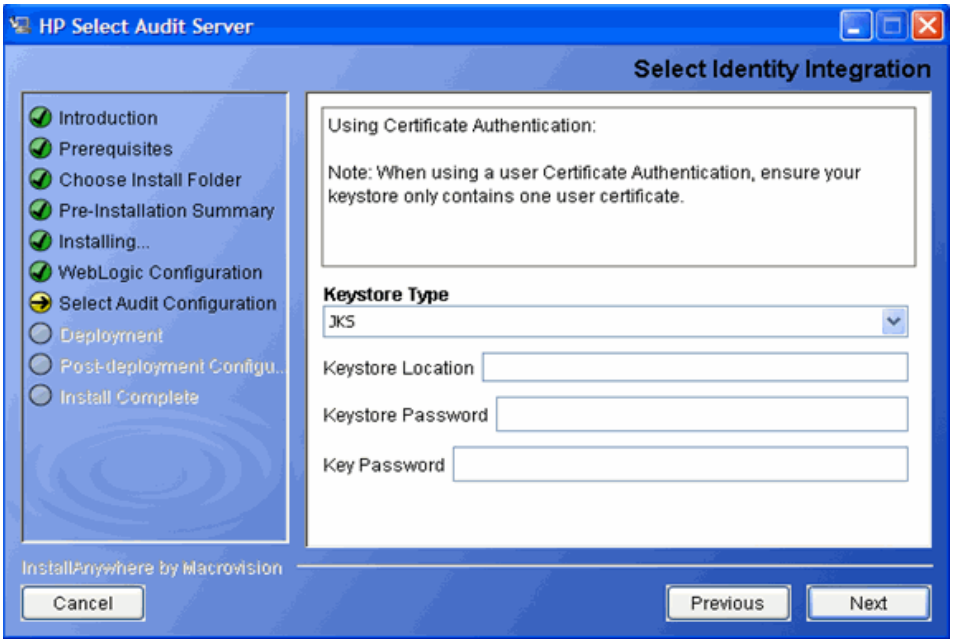
Certificate (requires SSL)

First you are advised that you must obtain the SSL port number from your SI server. Then, the following screen displays:



Select a **Trust Keystore Type** from the dropdown list. Then, specify the **Trust Keystore Location** and **Trust Keystore Password**. Finally, select the **Enable Certificate Revocation List Validation** checkbox if desired, and specify the **CRL refresh** rate.

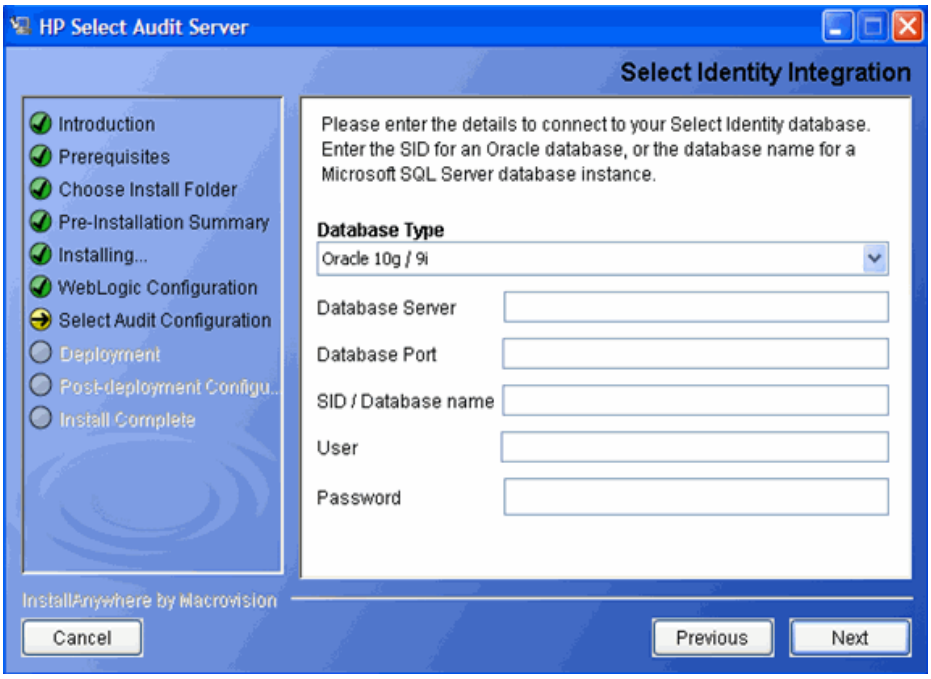
Click **Next** to proceed to the Select Identity keystore screen.



Select a **Keystore Type** from the dropdown list. Then, specify the **Keystore Location** and **Keystore Password**. Finally, enter the **Key Password**

Click **Next** to proceed to the Select Identity database configuration screen.

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



35 Complete the screen as follows:

- Select a database type (Oracle 10g/9i or Microsoft SQL Server 2005/2000) 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.

Check the remote start settings if deploying to remote machines with different WebLogic installation paths, as discussed in Task 9 on page 44.

Click **Next** to continue. When the installer has configured the Audit Server, the **Stop Servers** screen opens.

Clustered Environments

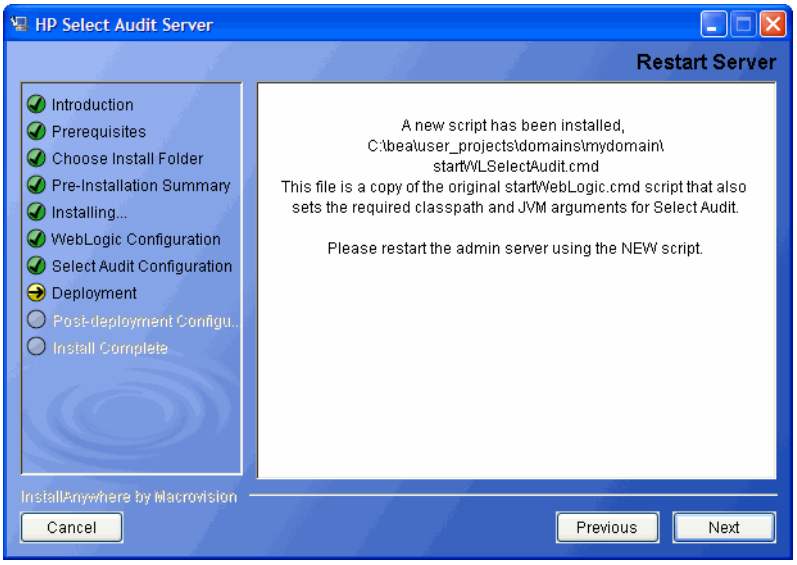
For proper functioning in clustered environments, LDAP configuration attributes need to be set for each managed server.

Change the `vde.aclcheck` parameter to `0` (the default is `1`) in the `<wl_domain>/servers/<server_name>/data/ldap/conf/vde.prop` file on each of the managed server machines.

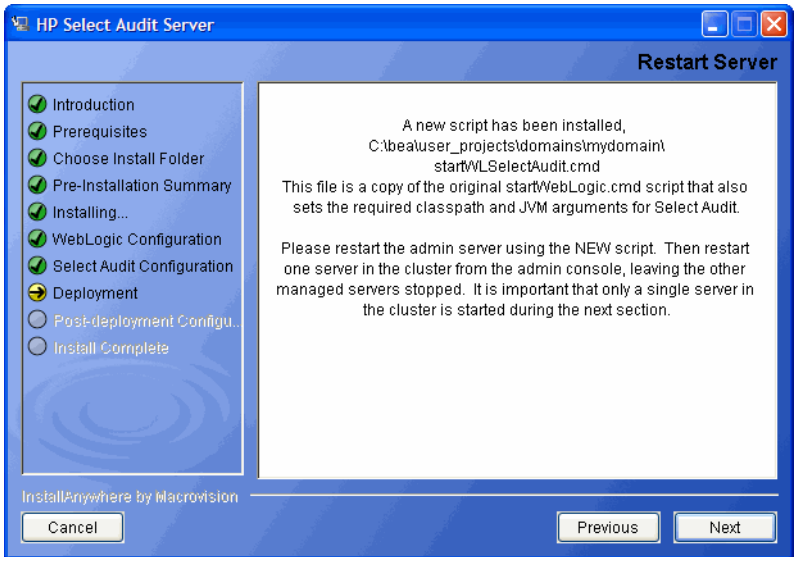
37 Stop the WebLogic server.

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.



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



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

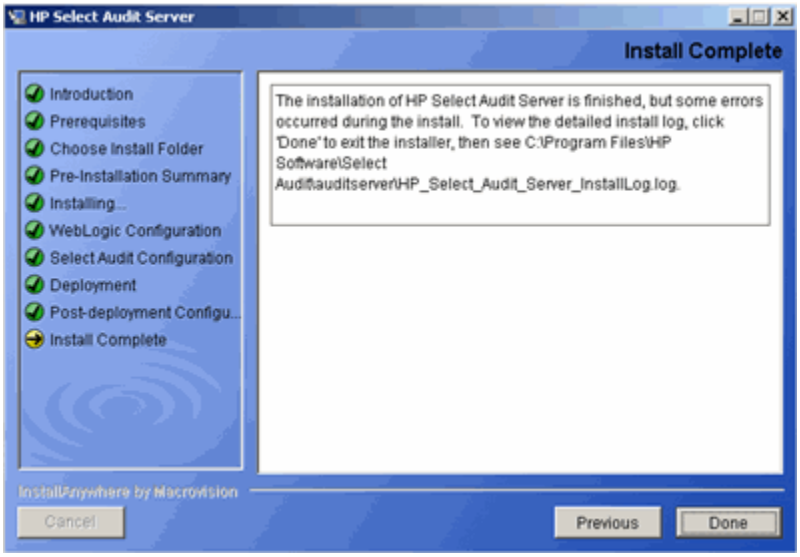
If you are running a cluster, start the Administration server first and then a single managed server in the cluster, leaving the rest of the cluster members stopped. After deployment, the **Deployment Complete** screens opens.

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.

If the installation completes successfully but with errors, the following screen opens giving the location of an error log file with error details.



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`.

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 WebLogic Connection Info screen. See Step 13 on page 46 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/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, `<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

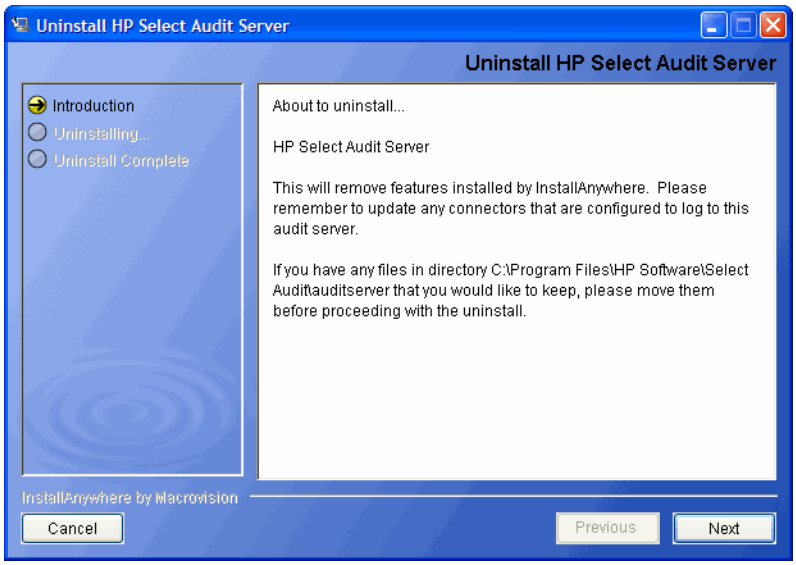
Audit Server uninstaller executables are created on the machine where the Audit Server is installed during the Server installation. After installing the Audit Server on Windows, there is an `Uninstall_Select_Audit` folder under the `C:\Program Files\HP Software\Select Audit` directory. This folder contains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

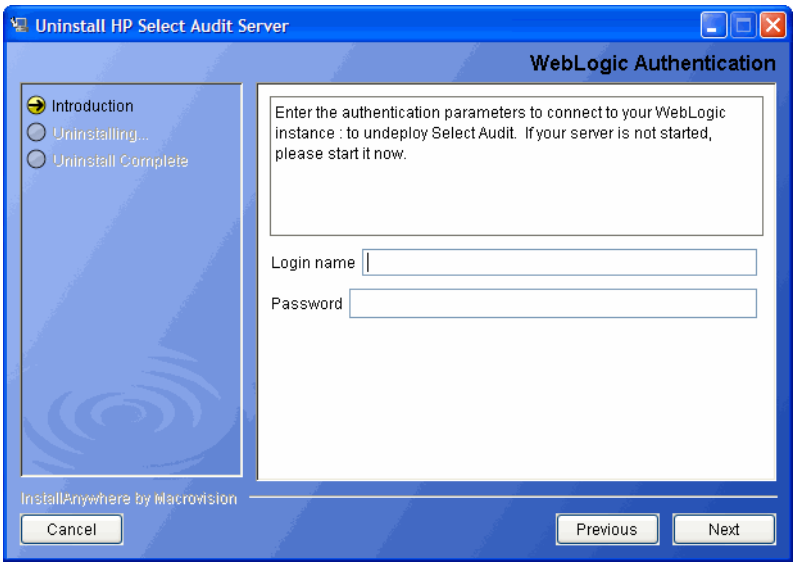
On HP-UX under the server installation directory `/opt/HP/SelectAudit/auditserver`, there is a `Uninstall_Server` directory that contains the `Uninstall_Select_Audit` binary.

To uninstall the Audit Server

1 Run `Uninstall_Select_Audit.exe` under the `HP Software\Select Audit\auditserver\Uninstall_Select_Audit` directory. The **Select Audit Uninstall Introduction** screen opens.



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



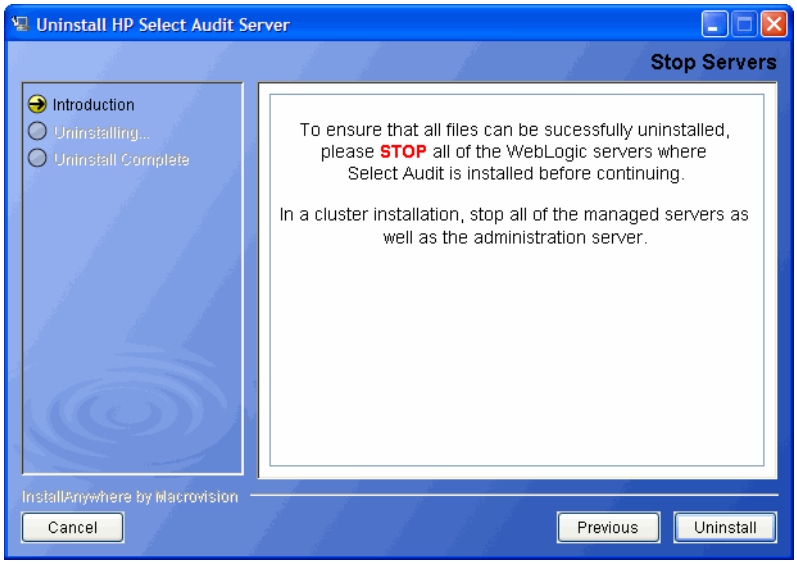
3 Type the Server administrator name in the **Login name** field and Server administrator password in the **Password** field in the corresponding fields. This user must have privileges to undeploy and remove services on the domain.

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

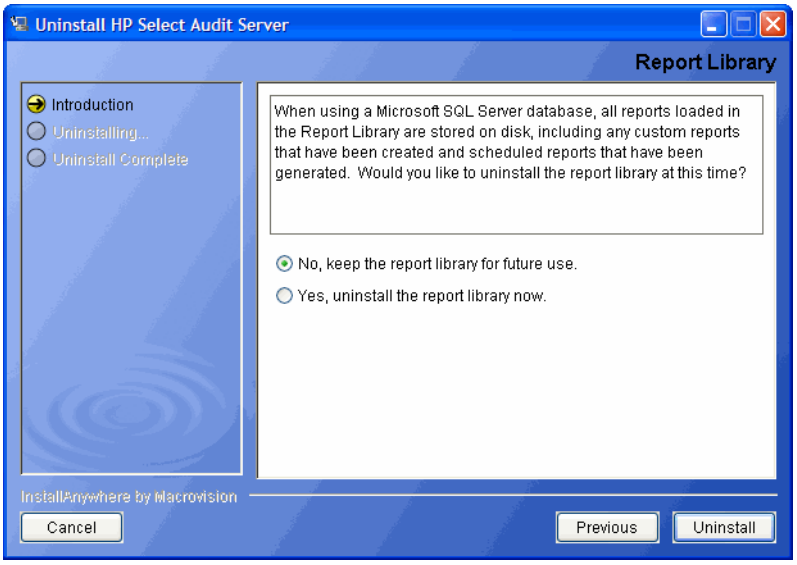
4 Click **Next**. The **Security Roles** screen opens.

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

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



7 Stop the servers and click **Uninstall**. If you are using MSSQL, the **Report Library** screen opens, otherwise, go to step 9.



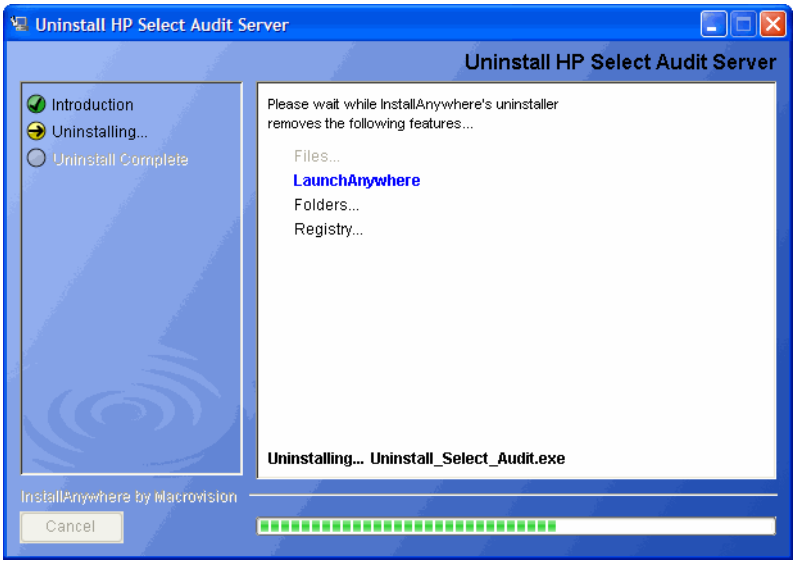
When using a Microsoft SQL Server database, all reports loaded in the Report Library are stored on disk, including any custom reports that have been created and scheduled reports that have been generated.

8 Do one of the following:

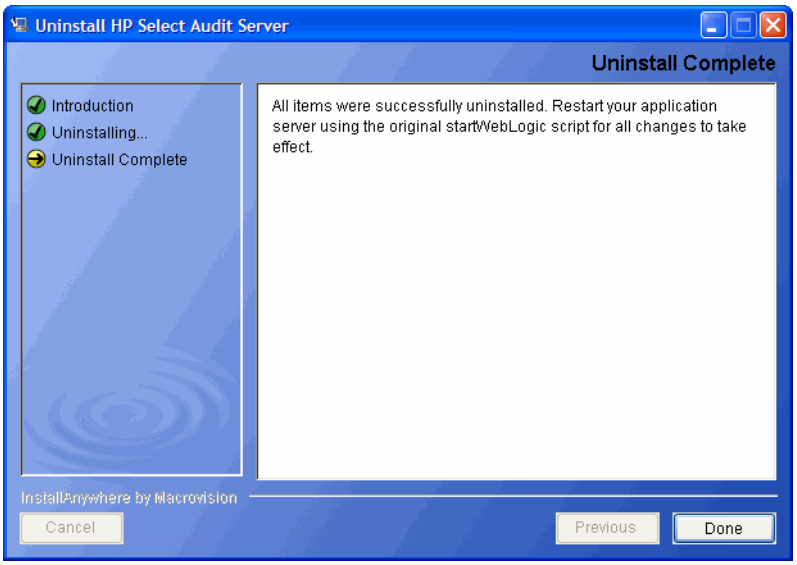
- Click **Yes** to uninstall the Report Library, including all custom reports and schedules permanently.
- Click **No** to leave any custom reports on disk to be restored later.

9 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.



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



10 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.

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

4 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 Unix:**

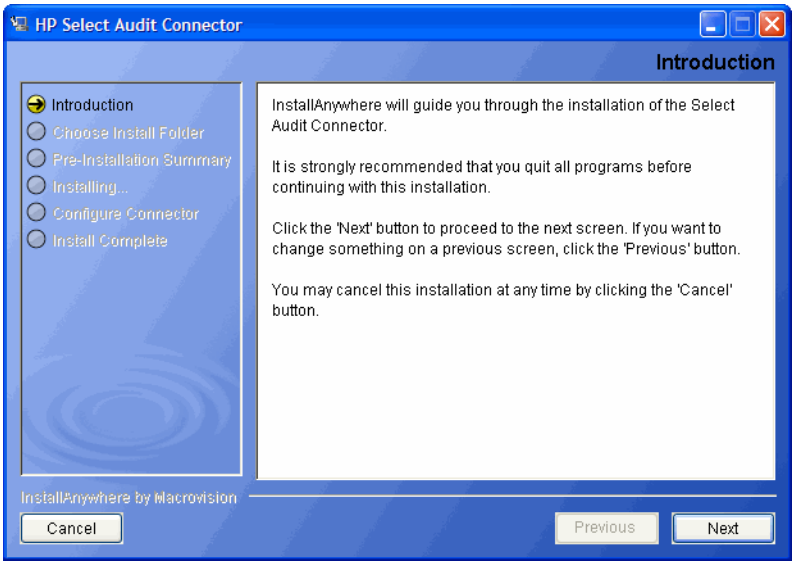
  Type the following command: `./SelectAuditConnectorInstall.bin`.

The connector installer should be run by the same user the connector process will be started as. If running the installer as root but registering the connector as a different user, follow the steps in the *HP Select Audit 1.1 Administration Guide* on manually configuring a connector.

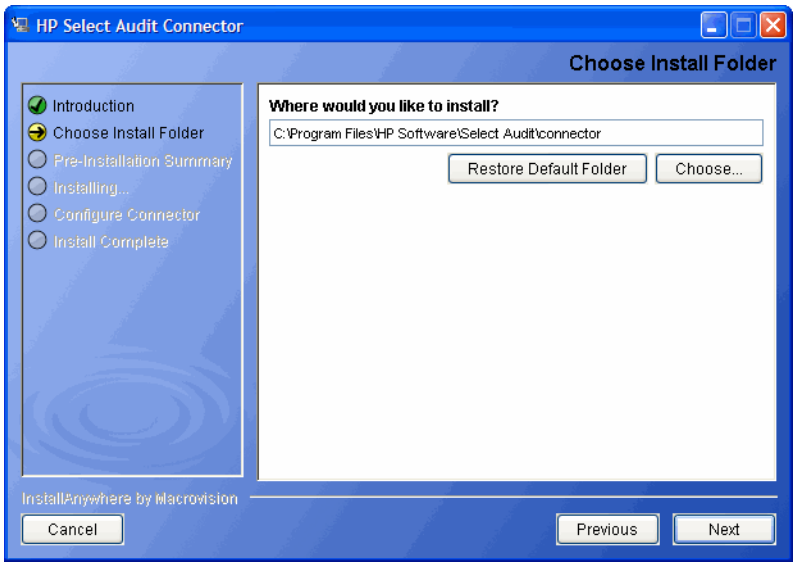
Also, to register the connector to run automatically on system startup, the root user should execute the `registerconnector.sh` script once the connector is installed.

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.



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



3 Do one of the following:

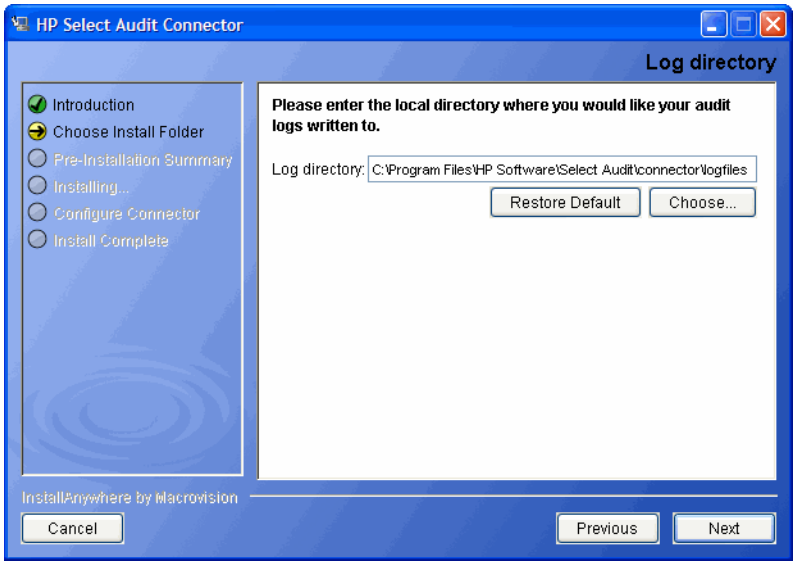
- If the default location is acceptable, proceed to step 4.
- If you want to select a different installation folder, click **Choose**, select a folder and then click **OK**. The new folder is shown in the **Where would you like to install Select Audit?** field.

If you choose the wrong folder, click **Restore Default** to restore the Select Audit defaults.

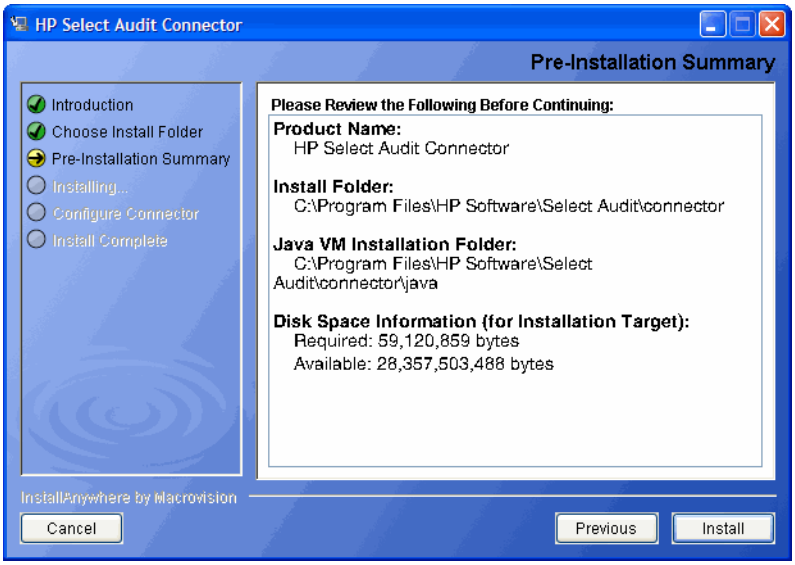
The following characters are not valid in file or folder names when specifying where to install the Audit Connector:

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

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.



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



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

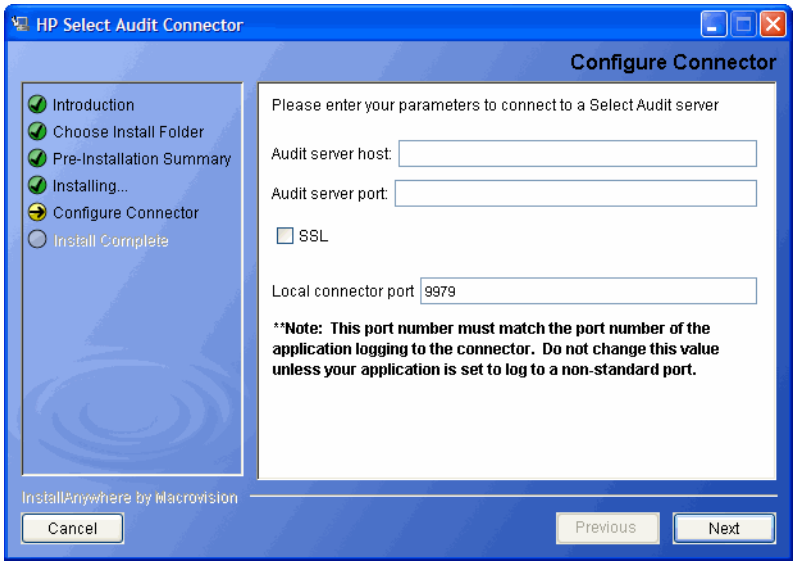
- The installation folder you chose for the Audit Connector installation.
- The installation location of the Java Virtual Machine that the Select Audit Install wizard has automatically installed. The Java Virtual Machine is required to run the connector application as well as the installer and uninstaller programs.
- 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.

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



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

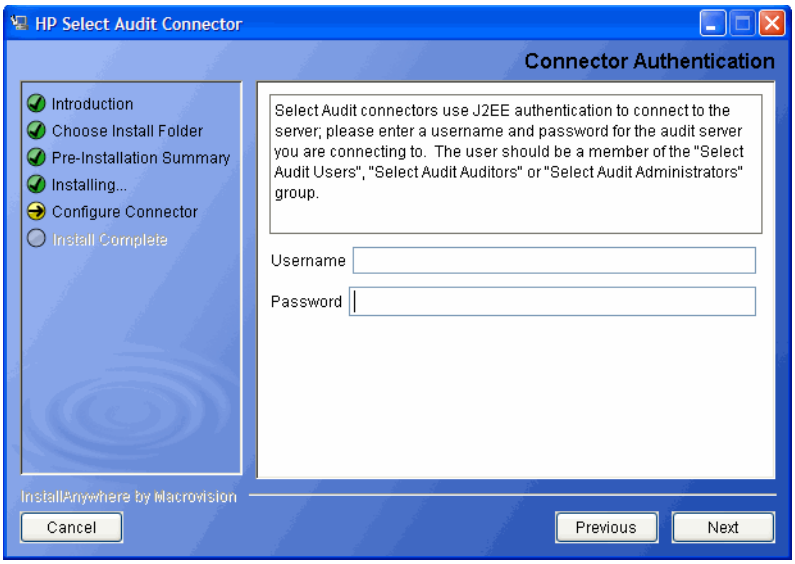
- Type the server host name in the **Audit server host** field.
- Type the server port number in the **Audit server port** field.
- Type the port number of the application logging to the Audit Connector in the **Local connector port** field.

  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.

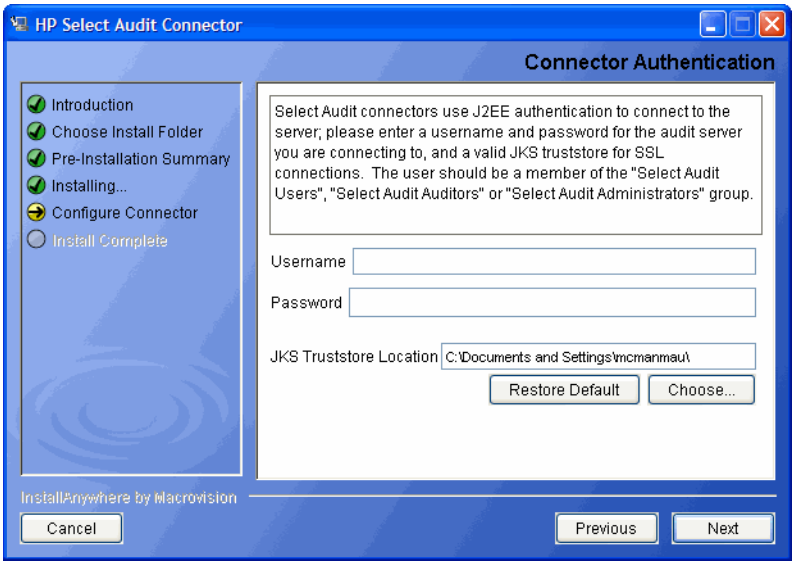
8 If you want to use an SSL connection, select the **SSL** check box.

  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.



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

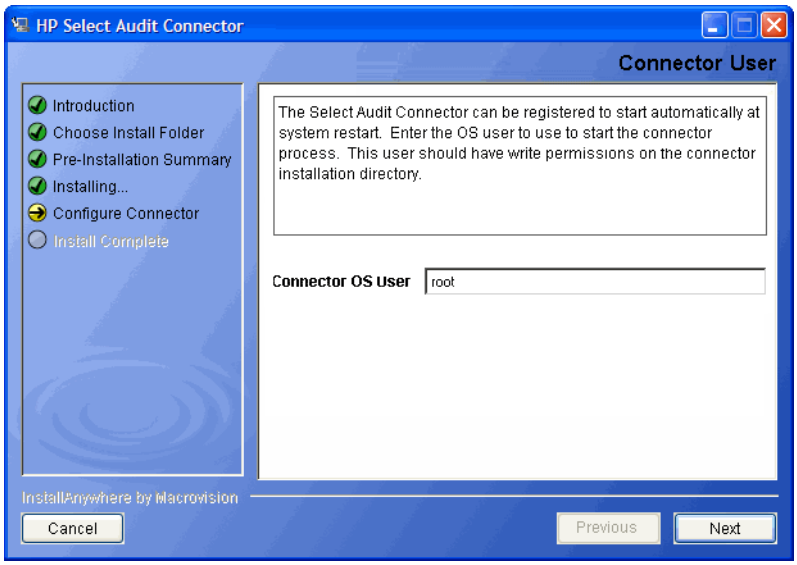


10 Type the **Username** and **Password** required to authenticate to the Audit Server.

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.



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.

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

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 1.1 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 HP-UX 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`.

Run `registerConnector.sh` as root to register the connector for automatic startup.

Installing the Connector in Console Mode

The installer can run in an interactive, text-only mode on Unix systems only, not Windows.

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.bin -i console
   ```

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

   The connector installer should be run by the same user the connector process will be started as.

3. Define Select Audit's installation folder by doing one of the following:
   - Typing the *absolute* path to the folder you wish to use.

   OR

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

     ```
     /opt/HP/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 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. The Select Audit Connector can be configured to start automatically at system restart. Type the OS user you want to use to start the Connector. This user should have write permissions on the Connector installation directory.

8 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`.

   Run `registerConnector.sh` as root to register the connector for automatic startup.

9 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:

```
CONNECTOR_OS_USER=root
INSTALLER_UI=silent
USER_INSTALL_DIR=C:\\Program Files\\HP Software\\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
```

Post-Installation Steps

Registering the Connector to Run at Startup (Unix)

A script is provided to register the connector to automatically run after a system restart. Before running this script, stop the connector using `<install_dir>/stopConnector.sh`

If `/var/run/SAudConnector` does not exist, manually kill the java process.

If the user to run the connector is different from the user that installed the connector, `chown` the entire installation directory to the connector user to ensure it has access to all files.

To register the connector, log in as `root` and execute the following script:

```
<install_dir>/registerConnector.sh
```

This script will create the PID directory under `/var/run` if it does not already exist, and set the ownership to the connector user. It then registers the connector process with the operating system for startup and starts the connector as the specified user.

For Windows systems, the connector is automatically registered as a Windows service to run at startup.

Uninstalling the Audit Connector

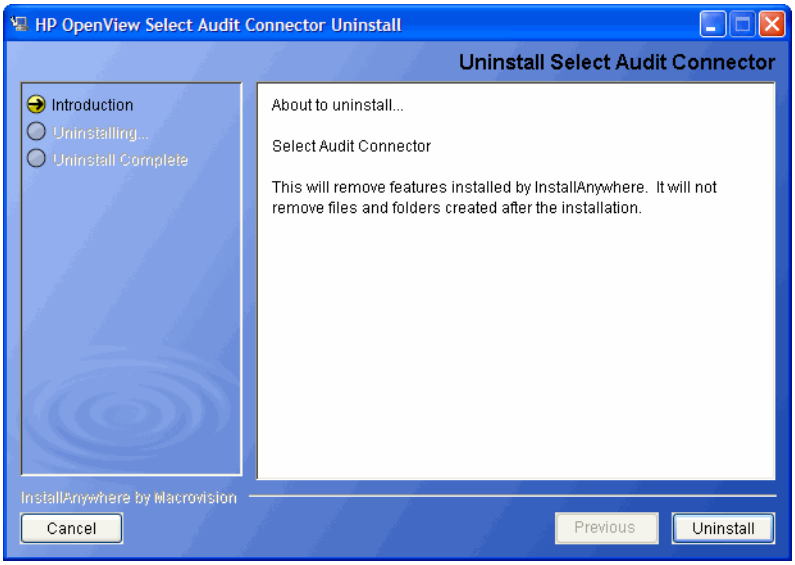
Audit Connector uninstaller executables are created on the machine where the Audit Connector is installed during the Connector installation. After installing the Audit Connector on Windows, there is an `Uninstall_Connector` folder under `C:\Program Files\HP Software\Select Audit` directory. This folder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

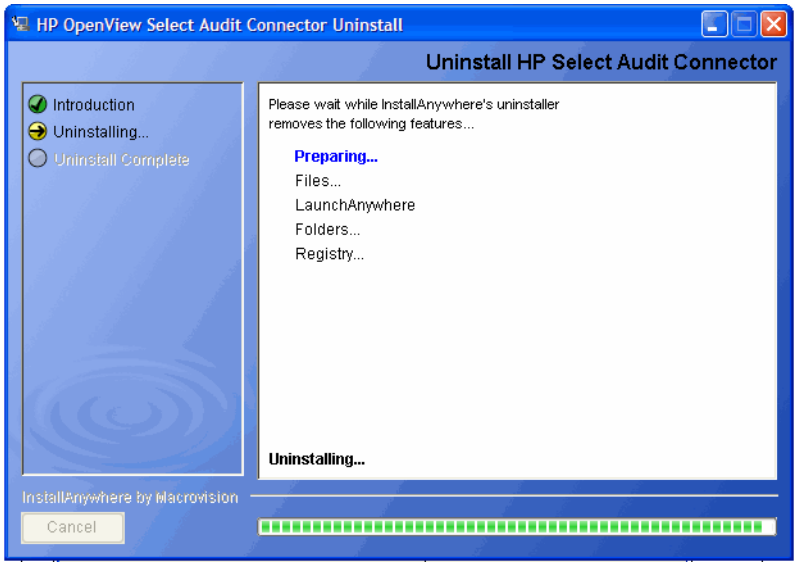
On Unix, under the connector installation directory `/opt/HP/SelectAudit/connector`, there is a `Uninstall_Connector` directory that contains the `Uninstall_Connector` binary.

To uninstall the Audit Connector

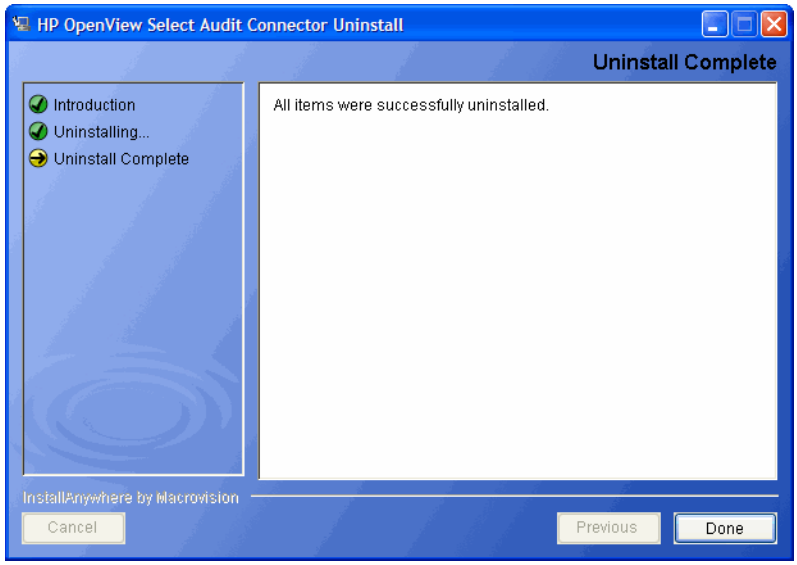
1. Run `Uninstall_Connector.exe` under the `C:\Program Files\HP Software\Select Audit\connector\Uninstall_Connector` directory. The **Uninstall Select Audit Connector Introduction** screen opens.



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



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



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.

5 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 users to collect all relevant system and application data in one easy step for submission to HP support for quick problem resolution

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.

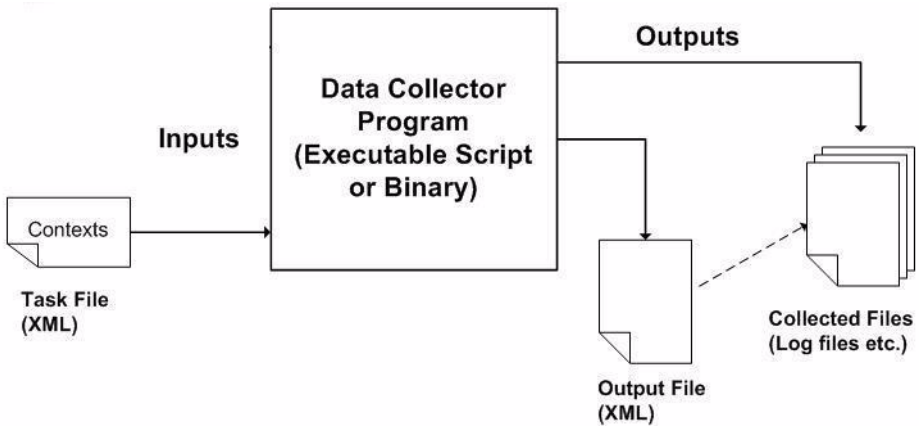
The Data Collector can be run on an installation of an audit server or connector.

The Data Collector is registered with the OS through a signed registration file at install time.

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 `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 9.

Figure 9 Data Collection Process



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 1.1 installer at the following location:

```
<install_dir>/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 `<install_dir>/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 installer performs when installing Select Audit.

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 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.

- 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 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 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 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>/data/ldap/conf/vde.prop` for each server. For managed servers, this must be done manually.

- It creates three JDBC data sources using the WebLogic APIs with the provided Oracle or Microsoft SQL Server database settings, targeted to the administration server and the target server or cluster.

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 an existing data source on the domain with the same name, it will be recreated using the database information entered in the installer.

- It creates the Select Identity data source only if Select Identity filtering is enabled at install time. This data source is used to connect to the Select Identity database which can be Oracle or Microsoft SQL Server.

Name	JNDI Name
SelectIdentityIntegrationDataSource	jdbc.IdentityIntegration

If there is an existing data source on the domain with the same name, it will be recreated using the database information entered in the installer.

To configure Select Identity filtering after the installation, this data source must be manually created.

- 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.

- Select Audit requires a WebLogic startup class to initialize its configuration module. It creates the startup class using WebLogic APIs.
- It stops the managed servers. If you are running a cluster, the installer will prompt you to shut down all managed servers so that configuration and classpath settings will be in effect.
- It restarts WebLogic. You are prompted to restart the administration server using the new startup script and one of the managed servers in the cluster, leaving any other managed servers stopped.
- It checks that the servers are running using the WebLogic APIs to verify that the servers are up and running.
- It creates the proxy data source using the WebLogic APIs to create 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 data source uses a custom JDBC driver, but connects to the same database as the main Select Audit data source. This is only used when Select Identity filtering is enabled.

Name	JNDI Name
SelectAuditProxyDataSource	jdbcproxy/SAudDataSource

  If there is an existing data source on the domain with the same name, it will be recreated using the database information entered in the installer.
- It deploys the report server application. Using WebLogic APIs, the installer deploys the application to the given server or cluster. Any existing application with the same name will be undeployed.

Name	Type
SelectAuditReporting	Web Application Module

- If deploying to a cluster, you will be prompted to restart the remaining managed servers.
- It deploys the Select Audit server and Select Audit workflow engines applications. Using WebLogic APIs, the installer deploys the applications to the given server or cluster. Any existing applications with the same name will be undeployed.

Name	Type
SelectAuditServer	Application
SelectAuditWorkflow	Application

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.

Index

A

appenders, setting for logging, 61

Audit Connector
- described, 13
- installation modes, 67
- installing, 67
- installing in Console mode, 74
- installing in Default mode, 68
- installing in Silent mode, 75
- Select application configuration, 67
- uninstalling, 76

Audit Server
- described, 13
- post-installation steps, 59
- WebLogic installation, 41
- WebLogic, uninstalling, 62

C

clustered environments
- data collector, 80
- pre-installation steps, 39

coexistence, Select Audit and Select Identity, 29

configuration requirements, Select applications, 67

D

Data Collector
- clustered environments, 80
- collection process, 79
- data collected, 80
- described, 79

defaults
- installation directory, Select Audit, 69
- restoring, 45, 69

disk space, minimum requirements, 11

H

hardware requirements, 11

HP-UX
- minimum requirements, 11
- platform availability, 11
- pre-installation steps, 38
- setting printenv, 14
- setting printev, 14

I

installation
- Connector installer mode overview, 67
- order, 39
- prerequisites, 42
- system requirements, 11

installation modes
- Console, 74
- Default, 68
- overview, 67
- Silent, 75

installers, described, 13

integration, Select Identity, 26

J

Java Virtual Machine install location, 74

L

links, symbolic, 14

Linux
- minimum requirements, 11
- platform availability, 11

load balancing, enabling in WebLogic, 60

log4j
- appenders, setting, 61
- configuring, 60
- enabling, 60

logging
- configuring, 60
- enabling, 60
- setting appenders, 61

M

memory, minimum requirements, 11

MSSQL
MS SQL2000 database server configuration, 16
MS SQL2005 database server configuration, 19
new database instance, 15
XA configuration, 15

O

operating systems
minimum requirements, 11
platform availability, 11
Oracle
database schema setup, 16
new database instance, 14

P

platforms. *See* operating systems
post-installation steps
configuring log4j, 60
configuring UTF-8 fonts, 61
enabling load balancing in WebLogic, 60
roles, adding users, 26
running the connector at startup (Unix), 75
pre-installation steps
clustered environments, 39
database schema setup, 16
DBA user, 14
HP-UX, 38
MSSQL database instance, 15
new database instances, 14
Oracle database instance, 14
overview, 14
printenv, path to, 14
processor, minimum requirements, 11

R

registry entries, creating, 14
requirements
registry entries, 14
system, summary, 11
roles, adding users, 26

S

Select Audit
Connector installation, 68, 74, 75
Connector installation modes, 67
Control Panel impact, 14
default installation directory, 69
HP-UX installation, 38
installation order, 39
operating systems available, 11
platform availability, 11
pre-installation steps, 14
Select Identity coexistence, 29
Select Identity integration, 26
system requirements, 11
Select Identity
integration, 26
Select Audit coexistence, 29
Self-Healing Services, 79 to 82
data collected, 80
data collection process, 79
data collector, 79
described, 79
using, 81
software requirements, 11
Solaris
minimum requirements, 11
platform availability, 11
symbolic links, 14
system requirements for installation, 11

U

UTF-8 fonts, configuring, 61

V

video card, minimum requirements, 11
VNC, 67

W

WebLogic
Audit Server installation, 41
Audit Server, uninstalling, 62
installation described, 83
load balancing, 60
Windows
minimum requirements, 11
platform availability, 11

X

XA configuration, 15

X-Windows, 67


invent


Java™
COMPATIBLE