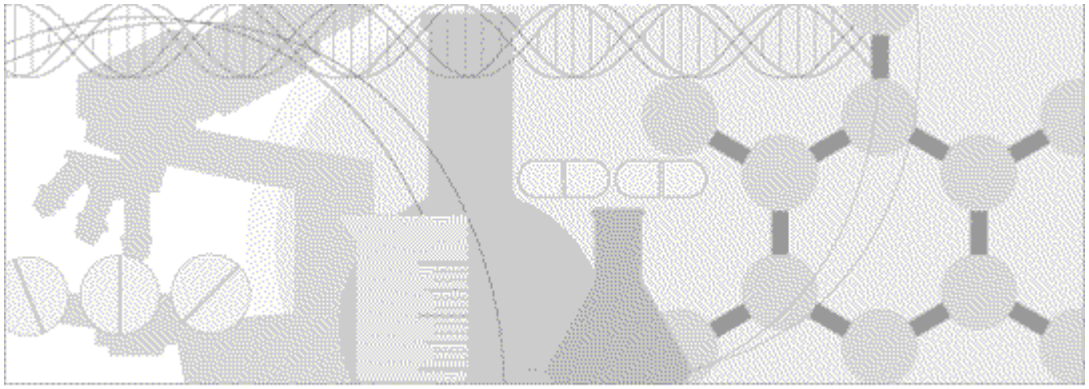
Installation Guide

Oracle® Health Sciences Central Designer Release 2.1.2.1



ORACLE

Part Number: E91372-01

Contents

CHAPTER 1

Architectural overview of the environment

In this chapter

Introduction to the Central Designer software

The Central Designer software consists of:

- **Central Designer server application**—Communicates with the client applications through web services.
- **Central Designer client application**—Provides a collaborative environment for designing clinical studies and deploying them to the InForm application.
- **Central Designer Administrator client application**—Provides an environment for setting up administrative information, such as users, roles, and system configuration information.

Physical architecture

The physical configuration of the Central Designer software includes:

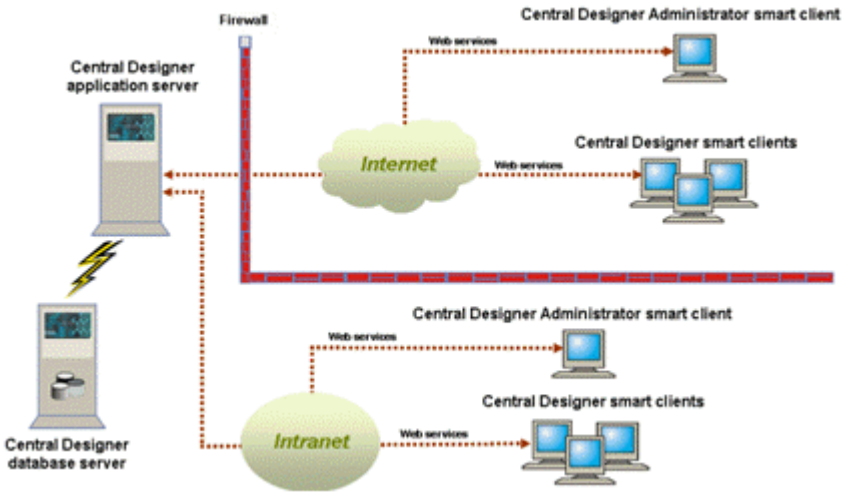
- A database server machine.
- One or more application server machines. For more information, see *Web farm capabilities* (on page 4).
- One or more client machines.

There are three configuration options for the Central Designer software.

Configuration	Description
Single-tier	The application server, database server, and client applications run on the same machine.
Two-tier	The application server and database server run on the same machine, and the client applications run on another machine.
Three-tier	The database server, application server, and client applications each run on a separate machine.

Notes:

- For optimum performance, Oracle recommends a three-tier configuration.
- If the application server and database server are on the same computer, you must install the Oracle Server software and Oracle Client software in the same home.



Web farm capabilities

You can expand the performance capabilities of the Central Designer application server by adding multiple servers in a farm configuration. This configuration is called a web farm. A web farm setup distributes requests from the client applications among multiple application servers. A web farm is useful for the following reasons:

- A large number of requests that might impact performance can be spread out among multiple application servers, thus improving performance.
- Multiple application servers allow for redundancy and failover protection.

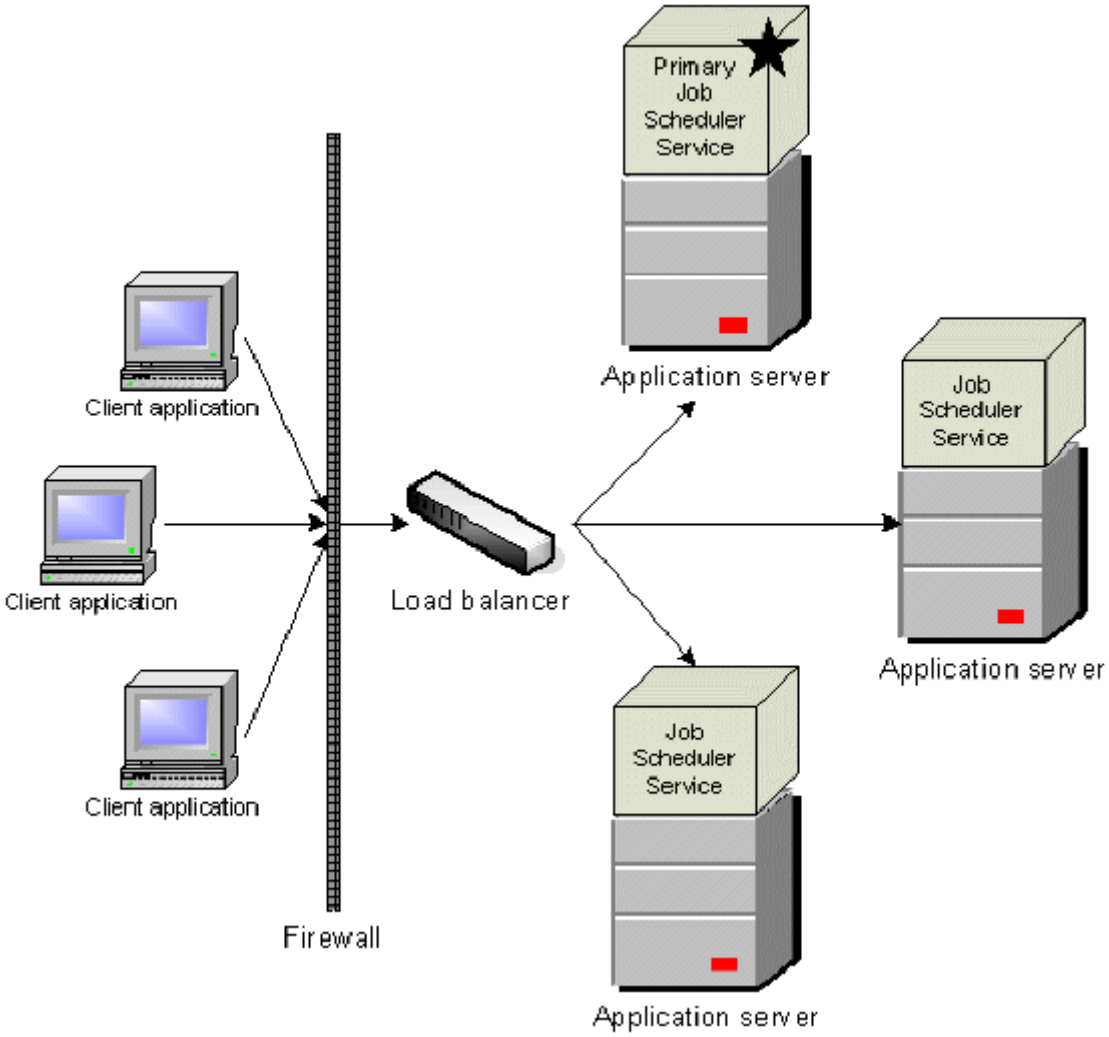
In a web farm configuration, all application servers can process any request. However, certain operations are run asynchronously using the Central Designer Job Scheduler. The Job Scheduler is installed on every application server, but only one Job Scheduler can process jobs, and only one service is enabled to process requests. The Job Scheduler service that processes all requests is called the primary Job Scheduler. You can change the primary Job Scheduler at any time. Oracle recommends setting the Job Scheduler on the most powerful machine in the web farm as the primary.

Note: You must use the same port number, which you specify during installation, for all application servers within a web farm. If one of the application servers uses a different port number, the Job Scheduler will not work if the machine is set to run the primary Job Scheduler. By default, the port number is 53000.

Illustration of a web farm configuration

The following tasks are performed in a web farm configuration:

- The client applications send requests through a firewall to a load balancer. The load balancer distributes requests among application servers.
- The job scheduler services on all of the application servers run; however, only the primary job scheduler processes requests. The other job scheduler services do not accept any requests. Examples of tasks that require the job scheduler service include importing and validation.
- All tasks that do not require the job scheduler service are distributed among the application servers.



Information that is stored in the database

Units information and report definitions are stored in the database and are used by all application servers in a web farm.

- You can export the units information to a file and then modify and import the file. You perform this task in the Central Designer Administrator application.
- If you have created custom reports, you must back up the Report configuration section of the

DesignerWebServices.config file before upgrading and then import it into the database.

For more information about working with this information, see the *Administrator Guide*.

About adding application servers

You can add additional application servers to a web farm environment at any time, even if you did not configure your first application server to support a web farm.

When you install a second application server, the installation recognizes the existing application server installation. The Job Scheduler service on the existing application server is set as the primary by default, but you can set the Job Scheduler for the second (or higher) application server as the primary during the installation of its application server.

You install additional application servers the same way that you install the first application server. The installation process configures the application server computers as a web farm. For more information, see *Installing the Central Designer application server* (on page 36).

Managing web farm capabilities

After a web farm is installed, you can manage it using the Central Designer Administrator software. You perform the following tasks in the Central Designer Administrator software:

- Viewing the servers that are in the web farm.
- Determining and changing the primary job scheduler.
- Working with Event Log messages for the web farm, including:
  - Viewing the messages.
  - Changing the default limit for the number of entries in the log.
  - Deleting all entries in the log.
- Modifying the file for report definitions.
- Modifying units information.

For more information, see the *Administrator Guide*.

CHAPTER 2

Checklists for software installation

In this chapter

Checklist—Planning the server installation

Use the following checklist to help plan the Central Designer application server and database server installations.

If you are upgrading, see *Upgrading the software to this release* (on page 49).

☑	Task	Information
❑	Determine if the setup is single-tier or multi-tier.	*Physical architecture* (on page 3).
❑	Make sure all system requirements, including .NET Framework requirements, have been met for the application server.	• *System requirements: Application servers* in the *Release Notes*. • *Verifying that the correct version of Microsoft .NET Framework is installed* (on page 19). • *Verifying that all required IIS roles are installed* (on page 20).
❑	Make sure all system requirements, including required Oracle database parameters, have been met for the database server.	• *System requirements: Database server* in the *Release Notes*. • *Install the Oracle database software on the database server* (on page 28).
❑	Register the .NET assemblies to the Global Assembly Cache (GAC).	• *Registering .NET assemblies* (on page 29). • Database patch Release Notes.
❑	On the database server, create the database and tablespaces.	The database and tablespaces must be created prior to installing the Central Designer software. *Create the database and tablespaces* (on page 29).
❑	On the database server, configure the Open Cursors setting.	*Configuring the Open Cursors setting for a database instance* (on page 30).
❑	On the database server, configure the Cursor Sharing setting.	*Configuring the Cursor Sharing setting for a database instance* (on page 30).
❑	On the database server, grant the appropriate rights to database administrators.	*Required rights for database administrators* (on page 30).
❑	Configure the application server for optimal performance.	*Configuring the application server for optimal performance* (on page 25).
❑	On the database server, configure the listener to accept connections for the new database.	*Configuring the listener to accept connections for the new database* (on page 30).
❑	Determine the security level to be used for communication between the client applications and the application server.	*Securing communication with Transport Layer Security (TLS)* (on page 69).
❑	Determine if you will implement a web farm.	*Web farm capabilities* (on page 4).

☑	Task	Information
❑	Increase the default value of the MS DTC timeout on the application server.	*Increasing the Microsoft Distributed Transaction Coordinator timeout* (on page 25).
❑	Monitor the tablespace in the database.	If the tablespace becomes full, expand the tablespace by adding another data file.
❑	Make sure that the following services are running: • IIS Admin Service • World Wide Web Publishing Service	If the services are not running, the installation fails. The IIS Admin Service does not have to run for the duration of the installation. However, you must start it before you click the Next button on the Copying Files screen. **Note:** Do not use the **iisreset** command from the MMC or a command prompt after the installation or upgrade completes, or the IIS settings that were set by the installer are lost. Instead, use the **net start** command to start the services.
❑	Install a certificate for signing web service authorizations, and a certificate for signing deployment packages and InForm web service authorizations.	*Installing certificates for signing web service authorizations and deployment packages* (on page 14).
❑	If necessary, install the root certificate and intermediate certificate or certificates, and install the main certificate as the root certificate.	• *Installing root and intermediate certificates* (on page 16). • *Installing the main certificate as the root certificate* (on page 17).
❑	To secure the web server and prevent clickjacking on the http://<*server name*>/CentralDesignerInstall page, from which you install the Central Designer and Central Designer Administrator applications, configure the HTTP response header in IIS.	*Configuring the IIS HTTP response header setting* (on page 24).
❑	If you perform automated deployments to InForm studies hosted by Oracle Cloud for Industry (OCI), make sure the Microsoft Windows setting Automatic Root Certificates Update is turned on.	Automatic Root Certificates Update is turned on by default in Microsoft Windows 2008. For more information, see the Microsoft website (http://technet.microsoft.com).
❑	Install the application server.	• *Installing the Central Designer application server* (on page 36). • *Performing a silent installation* (on page 42).

☑	Task	Information
❑	Configure SMTP settings for sending email notifications related to automated deployment events.	*Configuring SMTP settings for automated deployment email notifications* (on page 45).
❑	Verify the installation of the application server.	*Verifying the installation of the application server* (on page 43).

Checklist—Planning the client installations

Use the following checklist to help plan the installations of the client applications.

The Central Designer and Central Designer Administrator applications are ClickOnce applications. You start a ClickOnce application by clicking a link from an Internet Explorer window.

When you click a link for either application, the Central Designer server checks whether the release that is installed on the server matches the files that are cached on your computer:

- If the server has been newly installed or has been upgraded after your last logon, the files that are necessary to run the application are cached on your computer, and then are used to open the application.
- If the server has not been updated since your last logon, the cached files on your computer are used to open the application.

☑ Task	Information
❑ Make sure all system requirements, including .NET Framework requirements, have been met for the client computers.	• *System requirements: Client computers* in the *Release Notes*. • ***Verifying that the correct version of Microsoft .NET Framework is installed*** (on page 19).
❑ (Optional; this step is informational only.) Check whether the Microsoft Internet Explorer browser uses a proxy server to connect to the Internet. The Central Designer software uses the same proxy server.	***Viewing Internet Explorer proxy settings*** (on page 21).
❑ Make sure the clocks on the application server computer, database server computer, and client computers are synchronized.	***Synchronizing clocks on server and client computers*** (on page 22).
❑ Start the client applications.	• ***Starting the Central Designer client*** (on page 46). • ***Starting the Central Designer Administrator client*** (on page 47).

CHAPTER 3

Planning your installation

In this chapter

Installing certificates for signing web service authorizations and deployment packages

You must install a certification for each of the following purposes:

- Signing the web service authorizations.
- Signing deployment packages and InForm web service authorizations on the Central Designer server.

Oracle recommends using certificates issued by trusted commercial Certificate Authorities.

Install certificates to the **LOCAL_MACHINE\MY** store. Each certificate in the certification path must be 2048 bytes. For more information about converting existing certificates, see the Microsoft support website.

To install a certificate:

1 Open the Microsoft Management console:
   a Open a Command Prompt window.
   b Enter **mmc**, and then press **Enter**.
2 Select **File > Add/Remove Snap-in**.

   The Add or Remove Snap-ins dialog box appears.
3 In the list of available snap-ins, select **Certificates**.
4 Click **Add**.

   The Add dialog box appears.
5 Click **Computer account**.
6 Click **Next.**
7 Click **Local Computer**.
8 Click **Finish**.
9 Click **OK**.
10 In the left pane of the console, select **Certificates (Local Computer)**.
11 Right-click the **Personal** folder.
12 Select **All Tasks > Import**.

   The Certificate Import Wizard appears.
13 Click **Next**.
14 Click **Browse**, and select the PFX file provided by the certificate vendor.

   You are prompted for a password.
15 Enter the password for the PFX file.
16 Click **Next** to accept the default options for the remaining wizard pages.
17 Click **Finish**.

The new certificate appears in the displayed list.

The Central Designer installation process grants Full Control to access the certificate private keys to the IIS AppPool\DefaultAppPool user and the NETWORK SERVICE user.

If a user other than the IIS AppPool\DefaultAppPool user is running the DefaultAppPool application pool, you must grant the user Full Control to access the private keys, or the user is unable to sign using the certificates.

To grant a user other than IIS AppPool\DefaultAppPool Full Control to the private keys, for each certificate:

1 In the left pane of the Microsoft Management console, select **Certificates (Local Computer) > Personal > Certificates**.

2 Right-click the certificate and select **All Tasks > Manage Private Keys**.

3 Click **Add** > **Locations**, and then select the computer name.

4 Click **Advanced** > **Find Now**, select the user, and grant them Full Control.

If the user does not appear in the search results, type the user name in the Select Users or Groups dialog box.

5 Click **OK**.

About installing root and intermediate certificates

You might need to install additional certificates for the following situations:

- When the main certificate you installed contains an intermediate certificate, a root certificate, or both in its certification path.
- When the PFX file you imported contains an intermediate certificate, a root certificate, or both embedded within it. In this case, the certificates might not have been installed in the correct locations.

Determining whether to install additional certificates

To check whether you need to install the additional certificates, double-click the main certificate and select the **Certification Path** tab. If you see:

- **Three or more certificates**—Install the root certificate and one or more intermediate certificates.

  For more information, see *Installing root and intermediate certificates* (on page 16).

- **Two certificates**—Install the root certificate.

  For more information, see *Installing root and intermediate certificates* (on page 16).

- **One certificate**—Install the main certificate from the PFX as the root certificate.

  For more information, see *Installing the main certificate as the root certificate* (on page 17).

Installing root and intermediate certificates

Perform this procedure for both the root certificate and one or more intermediate certificates.

1 Open the Microsoft Management console:

  a Open a Command Prompt window.

  b Enter **mmc**, and then press **Enter**.

2 Select **File > Add/Remove Snap-in**.

  The Add or Remove Snap-ins dialog box appears.

3 From the list of available snap-ins, select **Certificates**.

4 Click **Add**.

  The Add dialog box appears.

5 Click **Computer account**.

6 Click **Next**.

7 Click **Local Computer**.

8 Click **Finish**.

9 Click **OK**.

10 In the left pane of the console, select **Certificates (Local Computer)**.

11 Click the **Personal** folder.

12 Double-click the main certificate you previously imported and select the **Certification Path** tab.

13 Do one of the following:

- To install the root certificate, double-click the root certificate.
- To install the intermediate certificate, double-click the intermediate certificate and select the **Details** tab.

14 Click **Copy to File** and do the following:

a Deselect **Do not export the private key**.

b Select the default file type.

c Select **DER encoded binary**.

d Navigate to the location in which to save the certificate.

e Click **OK**.

15 In the left pane of the console, select one of the following:

- If you are installing an intermediate certificate, select **Intermediate Certification Authorities**.
- If you are installing the root certificate, select **Trusted root Certification Authorities**.

16 Right-click the **Certificates** folder and select **All Tasks > Import**.

The Certificate Import Wizard appears.

17 Click **Next**.

18 Select the CER file for the certificate you are installing, either the intermediate or root certificate.

19 Click **Next** to accept the default options for the remaining wizard pages.

Installing the main certificate as the root certificate

1 Open the Microsoft Management console:

a Open a Command Prompt window.

b Enter **mmc**.

2 Select **File > Add/Remove Snap-in**.

The Add or Remove Snap-ins dialog box appears.

3 In the list of available snap-ins, select **Certificates**.

4 Click **Add**.

The Add dialog box appears.

5 Click **Computer account**.

6 Click **Next**.

7 Click **Local Computer**.

8 Click **Finish**.

9 Click **OK**.

10 In the left pane of the console, select **Certificates (Local Computer)**.

11 Click the **Personal** folder.

12 Double-click the main certificate you imported and select the **Certification Path** tab.

13 To install the main certificate as the root certificate, double-click the main certificate.

14 Click **Copy to File** and do the following:

   a Deselect **Do not export the private key**.

   b Select the default file type.

   c Select **DER encoded** binary.

   d Navigate to the location in which to save the certificate.

   e Click **OK**.

15 In the left pane of the console, select **Trusted root Certification Authorities**.

16 Right-click the **Certificates** folder and select **All Tasks > Import**.

   The Certificate Import Wizard appears.

17 Click **Next**.

18 Select the CER file for the root certificate.

19 Click **Next** to accept the default options for the remaining wizard pages.

Verifying that the correct version of Microsoft .NET Framework is installed

For information about the required versions of Microsoft .NET Framework, see *Hardware and software requirements* in the *Release Notes*.

Note: If you have a version of .NET Framework prior to the required version for this release, you do not need to uninstall it before installing the required version.

- To find .NET Framework versions by viewing the registry:

  1 On the Start menu, click **Run**.

  2 In the Open field, enter **regedit.exe**.

  3 Click **OK**.

  4 In the Registry Editor, go to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP**.

  The installed versions are listed under the NDP subkey.

  If .NET Framework is installed, the folder contains folders whose names begin with v, followed by the .NET Framework version number. For example:

  - **v3.5**—indicates that .NET Framework 3.5 SP1 is installed.
  - **v4.0**—indicates that .NET Framework 4.0 is installed.

- To find .NET Framework versions by using Windows Explorer, paste the following text into the Windows Explorer address bar:

  - For 64-bit: **%systemroot%\Microsoft.NET\Framework64**.
  - For 32-bit: **%systemroot%\Microsoft.NET\Framework**.

  If .NET Framework is installed, the folder contains folders listing the installed versions.

- If a required version of .NET Framework is not installed, install it.

Verifying that all required IIS roles are installed

1. Select **Start** > **All Programs** > **Administrative Tools** > **Server Manager**.
2. Make sure the following **Web Server (IIS)** roles required by Central Designer are installed:
   - Web Server
     - Web Server\Common HTTP Features
     - Web Server\Common HTTP Features\Default Document
     - Web Server\Common HTTP Features\Directory Browsing
     - Web Server\Common HTTP Features\HTTP Errors
     - Web Server\Common HTTP Features\Static Content
     - Web Server\Application Development
     - Web Server\Application Development\.NET Extensibility
     - Web Server\Application Development\Application Initialization
     - Web Server\Application Development\ASP
     - Web Server\Application Development\ASP.NET
     - Web Server\Application Development\CGI
     - Web Server\Application Development\ISAPI Extensions
     - Web Server\Application Development\ISAPI Filters
     - Web Server\Application Development\Server Side Includes
     - Web Server\Health and Diagnostics
     - Web Server\Health and Diagnostics\HTTP Logging
     - Web Server\Security
     - Web Server\Security\Request Filtering
     - Web Server\Performance
     - Web Server\Performance\Static Content Compression
   - Management Tools
     - Management Tools\IIS Management Console
     - Management Tools\IIS Management Service
     - Management Tools\IIS Scripts and Tools
     - Management Tools\IIS 6 Management Compatibility
     - Management Tools\IIS 6 Management Compatibility\IIS 6 Metabase Compatibility
     - Management Tools\IIS 6 Management Compatibility\IIS 6 WMI Compatibility
     - Management Tools\IIS 6 Management Compatibility\IiS 6 Scripting Tools
     - Management Tools\IIS 6 Management Compatibility\IiS 6 Management Console

Viewing Internet Explorer proxy settings

1 Open Internet Explorer, and select **Tools** > **Internet Options**.

2 Select the **Connections** tab, and click one of the following:

- **If you are connecting via a local area network**—Click the **LAN Settings** button.
- **If you are connecting via a network connection**—Click the **Settings** button.

The proxy settings appear in the dialog box.

Synchronizing clocks on server and client computers

The clocks on the client computers, application server computer, and database server computer are not required to be in the same time zone, but they must be no more than 24 hours apart relative to the Coordinated Universal Time (UTC). Oracle recommends that the clocks be no more than 10 minutes apart.

Hardware networking switches

Some hardware networking switches change the incoming URL before passing the request to the Central Designer server. For example, if the address entered during a client installation is **https://abc.com**, a switch might change the URL in the following ways:

- A switch that performs hardware SSL/TLS processing might change the URL to **http://abc.com**.
- A switch that performs load balancing might change the URL to **http://PhysicalServer1**.

When the application server is installed in an environment that includes a hardware networking switch, the URL that you enter for the **Web server URL root** field must match the URL that the networking switch uses to address the application server. From the previous examples, the required URLs must be:

- In the first example, **http://abc.com**.
- In the second example, **http://PhysicalServer1**.

Note: The application server must be able to use the address that you enter for the **Web server URL root** field to address itself.

Configuring the IIS HTTP response header setting

To secure the web server and prevent clickjacking on the http://<*server name*>/CentralDesignerInstall page, from which you install the Central Designer and Central Designer Administrator applications, configure the HTTP response header in IIS.

1 Open the Internet Information Services (IIS) Manager.

2 In the Connections section on the left, expand the **Sites** folder.

3 Select **Default Web Site**.

4 In the Default Web Site Home pane, in the IIS section, double-click **HTTP Response Headers**.

5 In the Actions section on the right, click **Add**.

The Add Custom HTTP Response Header dialog box appears.

6 Enter the following:

- **Name**—X-Frame-Options
- **Value**—SAMEORIGIN

7 Click **OK**.

Configuring the application server for optimal performance

Oracle recommends performing the following modifications on the Central Designer application server to optimize performance.

Use the /3GB startup switch feature for a 32-bit Microsoft Windows server

Using this startup switch, you can specify allocation details for memory and memory address space usage. Additionally, the switch allows the server to access 3 GB of address space instead of 2 GB, which is the default maximum for a 32-bit operating system.

Do not set the startup switch for a 64-bit Microsoft Windows server.

For more information, see the Microsoft documentation.

Configure the worker process recycling settings for Windows 2008

1 On the application server computer, select **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

2 Expand the tree for the local computer and select **Application Pools**.

3 Right-click **DefaultAppPool** and select **Recycling**.

4 Configure the following settings:

- Verify that only **Regular time intervals (in minutes)** is selected.
- Verify that a value of **1740** is entered for that setting.

Configure the worker process health settings for Windows 2008

1 On the application server computer, select **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

2 Expand the tree for the local computer and select **Application Pools**.

3 Right-click **DefaultAppPool** and select **Advanced Settings**.

4 Under **Process Model**, set **Shutdown time limit (seconds)** to match the timeout for the client application. (The default is 1200 seconds.)

Increase the default Microsoft Distributed Transaction Coordinator timeout

Oracle recommends that you increase the Microsoft Distributed Transaction Coordinator (MS DTC) timeout because the default Windows timeout setting of 60 seconds might be insufficient for some Central Designer processes.

1 Select **Start** > **Control Panel** > **Administrative Tools** > **Component Services**.

2 Open **Component Services** > **Computers**.

3 Right-click **My Computer**, and select **Properties**.

4 Select the **Options** tab.

5 Change the value of the **Transaction timeout (seconds)** field to **3600**. (The default is 60.)

6 Click **OK**.

7 Open **Control Panel > Services**.

8 Stop and restart all IIS services.

Use the performance tuning capabilities that are available with the Oracle database software

Open the Automatic Database Diagnostic Monitor (ADDM) from the Database Control home page or from Advisor Central.

This tool helps you diagnose problems, identify their causes, and make recommendations.

About acting on ADDM recommendations:

- Make configuration changes to the database or operating system as necessary.
- The SQL Tuning Advisor might recommend rewriting some SQL statements. However, the SQL statements cannot be rewritten.
- Add database indexes as needed.

> **Caution**: Take note of all new indexes. Before upgrading, you must drop them to ensure that they do not cause conflicts with new indexes that have been added to the product. After the upgrade is finished, you can add the indexes back.
>
> **Note**: Contact Oracle Global Support to forward SQL statement recommendations or request index changes in the product.

The most common configuration recommendations from ADDM are:

- SGA_TARGET
- PGA_AGGREGATE_TARGET
- DB_FILE_MULTIBLOCK_READ_COUNT
    - Reset to zero instead of using an explicit value.
    - Oracle automatically manages this parameter value if it is set to zero.

For more information, see the Oracle database software documentation.

CHAPTER 4

Preparing the database server

In this chapter

Prepare the database server

Before installing the Central Designer software, you must:

- Install and configure the Oracle database software on the database server.
- Create the necessary database instance and tablespaces.

Install the Oracle database software on the database server

After the database server requirements are met, you can install the Oracle database software. Use the Oracle database software installation documentation as needed. For more information about required Oracle database software versions, in the *Release Notes*, see:

- System requirements: Application servers.
- System requirements: Database server.
- System requirements: Client computers.

Note: If the application server and database server are on the same computer, you must install the Oracle Server software and Oracle Client software in the same home, or the Central Designer server installation will not work.

Mandatory configuration

Most of the default Oracle settings can be used for the Central Designer database. However, the following Oracle configuration must be used.

Page	Option	Value
Database Components	Oracle Text, a standard database component.	Selected. **Note:** The Oracle database software installation requires that you install Oracle Data Mining if you install Oracle Text. If you do not want to install Oracle Data Mining, you can install Oracle Text manually after completing the Oracle database installation. For more information, see the following My Oracle Support note: *Note: 970473.1 Manual installation, deinstallation and verification of Oracle Text 11gR2.*
	Oracle Java Virtual Machine (JVM)	Selected.
Character Sets	Database Character Set	AL32UTF8 - Unicode 4.0 UTF universal character set, UTF-8 compliant.
	National Character Set	AL16UTF16 - Unicode UTF-16 universal character set.
Parameters	CURSOR_SHARING parameter	For Oracle 11g—**FORCE**

Page	Option	Value
	OPEN_CURSORS parameter	For Oracle 11g—**500**

Additional configuration information

In production databases at Oracle, the DB_BLOCK_SIZE Oracle parameter is set to 16k (16384 bytes).

Registering .NET assemblies

You must register the .NET assemblies to the Global Assembly Cache (GAC) after the initial installation, and each time you apply a patch.

For .NET version 4:

- Oracle.ManagedDataAccess.dll

For .NET version 2 and version 4:

- Oracle.DataAccess.dll
- Oracle.Web.dll
- OracleDatabaseExtensions.dll

To add the assemblies to the GAC, do the following:

1 Open a command prompt as an Administrator.

2 Navigate to the directory that contains the assembly to add to the GAC.

3 Execute the following command:

```
oraprovcfg.exe/action:gac/providerpath:<assembly DLL>
```

For example:

```
oraprovcfg.exe/action:gac/providerpath:Oracle.DataAccess.dll
```

Create the database and tablespaces

After you install the Oracle database software, create the database instance and tablespaces. Make sure the Oracle server has sufficient space to accommodate the new tablespaces. The Central Designer software uses the following tablespaces by default.

Tablespace	Description	Minimum size
DESIGNER	Main data tablespace	100 MB. For Oracle 12c databases, a 16k (16384 bytes) block size is required. **Note:** Depending on usage, you might need to increase the MB size.

DESIGNER_BIGINDEX	Index tablespace	10 MB with 16k (16384 bytes) block size. **Note:** Do not create this tablespace for Oracle 12c databases.
SYSTEM	Main data tablespace	500 MB.
SYSAUX	Main data tablespace	250 MB.
TEMP	Temporary tablespace	Always present in the Oracle database.
UNDOTBS1	Main data tablespace	200 MB.

Note: The tablespace names provided are the default names. Any names can be used for the tablespaces.

If you use non-default names, you must specify them during the installation of the application server (by clicking Advanced on the Database Parameters page), so be sure you take note of them.

Configuring the listener to accept connections for the new database

After installing the Oracle database software, you must configure the listener to accept connections for the new database. For more information, see the Oracle database software documentation.

Configuring the Open Cursors setting for a database instance

When you create a database instance, you must set the Open Cursors setting correctly for your database version.

- For the Oracle 11g database version, set Open Cursors to **500** using the following SQL command:

```
ALTER SYSTEM SET open_cursors=500 SCOPE=BOTH;
```

Before you upgrade, ensure that the Open Cursors parameter is correctly set.

Configuring the Cursor Sharing setting for a database instance

When you create a database instance, you must set the Cursor Sharing setting properly for your database version. For the Oracle database version 11.2.0.3 or later, set Cursor Sharing to **FORCE**.

The following SQL command changes the Cursor Sharing setting:

```
ALTER SYSTEM SET cursor_sharing=<Setting> SCOPE=BOTH;
```

In the previous command, *Setting* can be SIMILAR or FORCE, depending on the version of the Oracle database software in your environment.

Before you upgrade, ensure that the Cursor Sharing parameter is correctly set.

Required rights for database administrators

During the installation of the Central Designer application server, you are prompted to specify user

names and passwords for:

- Database Administrator
- Database User

The installation uses the Database Administrator user name and password to create the Database User and grant that user rights to perform tasks for the Central Designer application. The default name for the Database Administrator is system, but it can be any user that you assign the rights to perform the following tasks.

Task	SQL	Automatically executed for
Create the Database User.	**CREATE USER &1 IDENTIFIED BY &2** **DEFAULT TABLESPACE &3;** **GRANT CONNECT TO &1;** **GRANT RESOURCE TO &1;** **GRANT CREATE VIEW TO &1;**	All supported Oracle database software versions.
Allow the Database User to create function indexes.	**GRANT QUERY REWRITE TO &1;** **GRANT CREATE SYNONYM TO &1;**	All supported Oracle database software versions.

Note: In Oracle 11g and 12c, the Database Administrator user does not have the right to allow the Database User to execute jobs. For more information on how to assign the Database Administrator the necessary rights, see ***Granting the EXECUTE on SYS.DBMS_JOB right to the database administrator*** (on page 31).

Granting the EXECUTE on SYS.DBMS_JOB right to the database administrator

The Database Administrator user does not have the right to allow the Database User to execute jobs in the Oracle 11g and 12c database software.

To grant the Database User the right to execute jobs, run the following SQL commands as a Database Super User:

GRANT EXECUTE on SYS.DBMS_JOB to <*Database Administrator user name***> WITH GRANT OPTION;**

In the previous command, *Database Administrator user name* can be System, or the user name you assigned to the Database Administrator user.

Due to a known issue in the 11.2.0.3 database software version, after you grant the right to execute jobs, you must revoke the right, and grant the right again. Run the following SQL commands as a

Database Super User:

1 **REVOKE EXECUTE on SYS.DBMS_JOB from <***Database Administrator user name***>**

2 **GRANT EXECUTE on SYS.DBMS_JOB to <***Database Administrator user name***> WITH GRANT OPTION;**

In the previous command, *Database Administrator user name* can be System, or the user name you assigned to the Database Administrator user.

You can then run the following SQL commands as the Database Administrator user you referenced in the previous step to assign a user the right to execute jobs:

GRANT EXECUTE on SYS.DBMS_JOB to &1;

Sample SQL

The following SQL commands are not run by the installation but show an example of what a database administrator needs to do to create the tablespaces. Database administrators must set up the tablespaces before installing the Central Designer software. Administrators should note the setting of the cache size before creating the _BIGINDEX tablespace.

```
CREATE TABLESPACE designer

LOGGING

DATAFILE 'D:\Oracle\oradata\dev1\DESIGNER.ora' SIZE 400M

AUTOEXTEND ON NEXT 1M;

ALTER SYSTEM SET db_16k_cache_size = 80M;

CREATE TABLESPACE designer_bigindex

LOGGING

DATAFILE 'D:\Oracle\oradata\dev1\DESIGNER_BIGINDEX.ora' SIZE 10M
REUSE

BLOCKSIZE 16384

EXTENT MANAGEMENT LOCAL SEGMENT SPACE MANAGEMENT AUTO;
```

CHAPTER 5

Installing and uninstalling the software

In this chapter

Before you begin

The latest information about the Central Designer application is on the Oracle Support self-service website, My Oracle Support. Before you install and use the Central Designer application, check My Oracle Support for the latest information, including *Release Notes* and *Known Issues*, alerts, white papers, bulletins, and patches.

For the latest Central Designer software, check the Oracle Software Delivery Cloud (https://edelivery.oracle.com).

Overview of installation and configuration

Before you start your installation, plan your work:

- *Checklist—Planning the server installation* (on page 8).
- *Checklist—Planning the client installations* (on page 11).

Overview of installing the application and database servers

Step		For more information, see
1	Install the Central Designer application server.	• *Preparing the database server* (on page 27). • *Installing the Central Designer application server* (on page 36).
2	Verify the installations.	• *Verifying the installation of the application server* (on page 43).

Overview of uninstalling

Step		For more information, see
1	Uninstall the application server.	• *Uninstalling the application server* (on page 44).

Note: The client applications are ClickOnce applications and are therefore not installed on users' computers. Therefore, you cannot uninstall the client applications.

Installing the Central Designer application server

1 Locate the **setup.exe** program.

The setup.exe program is available the Oracle Software Delivery Cloud (https://edelivery.oracle.com).

2 Double-click **setup.exe**.

The InstallShield Wizard prepares to install the application server.

A welcome page appears.

3 Click **Next**.

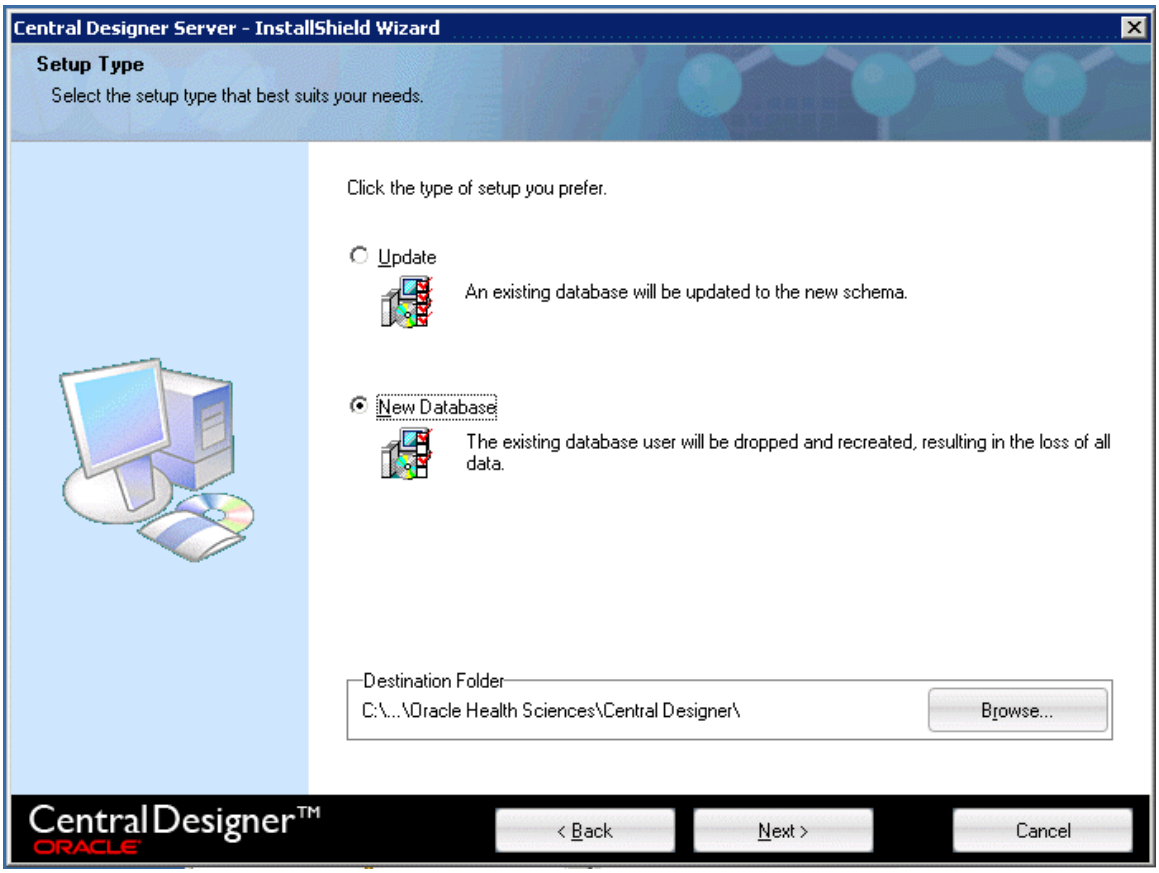
The Customer Information page appears.

4 Provide the following information:

- **User Name**—Your name.
- **Company Name**—The name of your company.
- **Company URL**—A unique identifier for your company data, typically your company URL (for example, http://www.mycompany.com).
- Select whether to install the application for anyone who uses the computer, or only for your user.

5 Click **Next**.

The following page appears.



6 Select **New Database**.

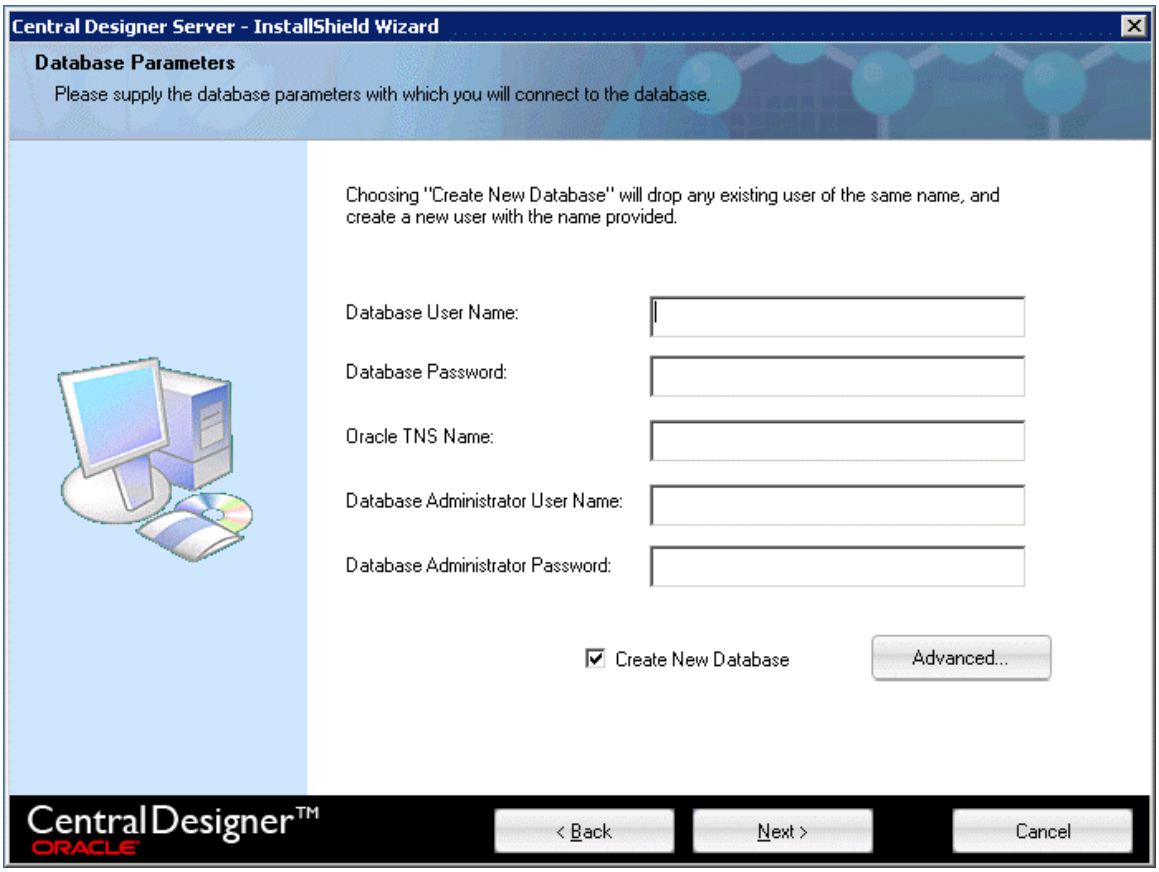
> **Note:** If you are installing the second or higher server in a web farm, do not select **New Database**. You must select **Update**.

7 In the **Destination Folder** area, specify the destination location for the installation. By default, the installation wizard installs the software in the *<PROGRAMFILESDIR>\Oracle Health Sciences\Central Designer* folder. *PROGRAMFILESDIR* is a system setting that is usually C:\Program Files. If you want to install to another location, click **Browse**, and select the location.

> **Note:** The instructions, paths, and Start Menu navigation in this guide assume you are installing to the default location. Oracle strongly recommends that you install the software to the default location.

8 Click **Next**.

The following page appears.



9 Fill in the fields in the page as follows.

Field	Description
Database User Name	The Oracle user name for the database user.
Database Password	The password for the database user. **Note:** The password must not contain any of the following characters: @ & ( ) [or].

Field	Description
Oracle TNS Name	Alias from the TNSnames.ora file. This TNS name is used to connect to the database instance.
Database Administrator User Name	The Oracle user account for the database administrator. This account is used to create the database user. **Note:** The user name cannot be a SYSDBA user account.
Database Administrator Password	The password for the database administrator. **Note:** The password must not contain any of the following characters: @ & ( ) [or].
Create New Database	Indicate whether to create a new database schema during installation. **Caution:** If you have an existing database schema and you select **Create New Database**, all existing information in your current database schema will be **deleted**.

Note: Do not use Oracle reserved words for user names or passwords.

10 If a new database was created and tablespaces were created with non-default names, you must specify the names of the tablespaces. The tablespaces that you specify must already exist. The installation does not create tablespaces.

a Click **Advanced**.

The Advanced Database Settings page appears.

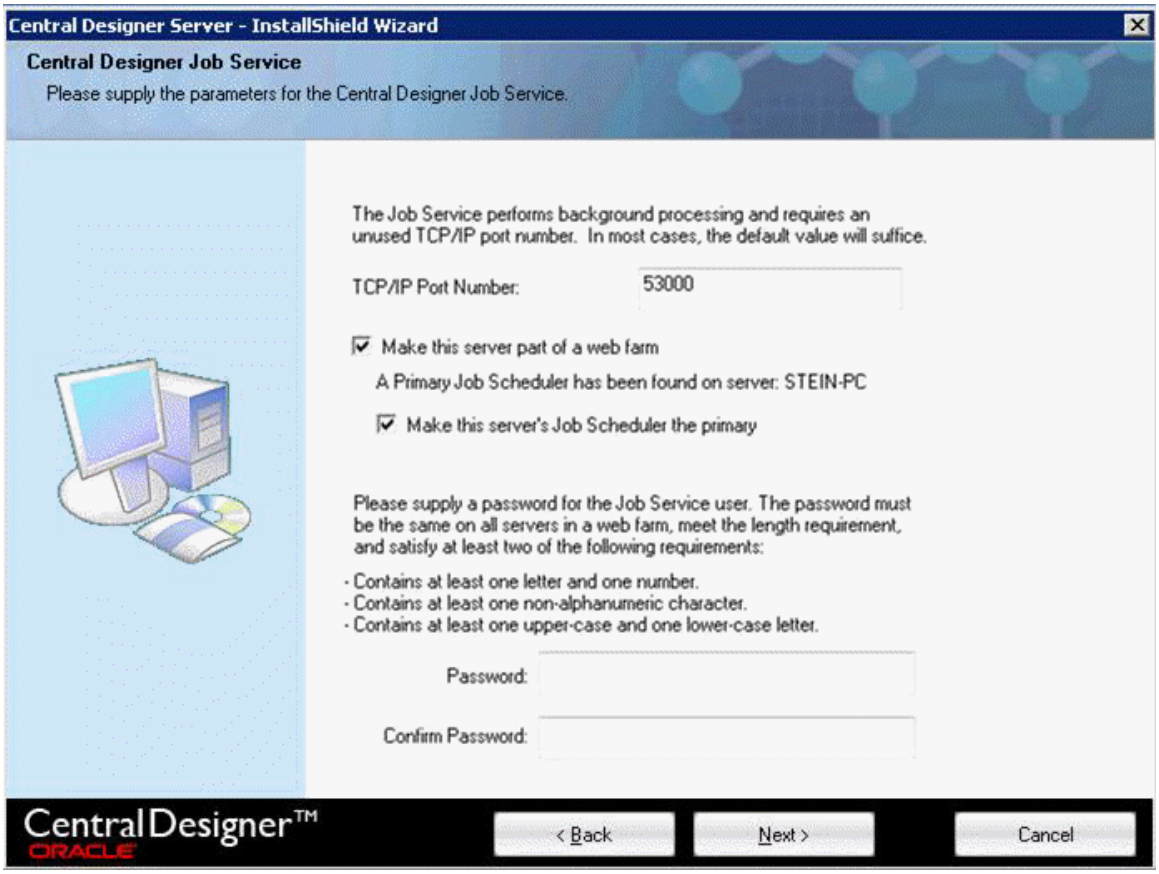
b Fill in the fields with the correct information, according to the following table.

c Click **OK** to return to the **Database Parameters** page.

Field	Description
Default Tablespace for new user	The first tablespace for the tables of the schema owner. For an Oracle 12c database, this tablespace must have a block size of 16k.
Large (16K) Tablespace for new user	A second tablespace with a block size of at least 16k. **Note:** This tablespace is not required for Oracle 12c databases.
Temp Tablespace for new user	The temporary tablespace for the tables of the schema owner.

11 Click **Next**.

The following page appears.



12 Enter the TCP/IP port number that the job service will use. The port must be unused. In most cases, you can use the default value.

> **Note:** If you are installing the server as part of a web farm, all of the servers can use the same port number, as long as the port is unused.

13 Optionally, to configure the Central Designer software to support a web farm, select **Make this server part of a web farm**. A web farm setup allows you to install the Central Designer server software on multiple application server computers. The installation is the same for all of the servers, and you must select this option for all servers in the web farm. For more information, see *Web farm capabilities* (on page 4).

After you select the checkbox, the installation checks the database to see if a primary Job Scheduler has been specified. Additional options appear, depending on whether you are installing the first or second (or higher) server.

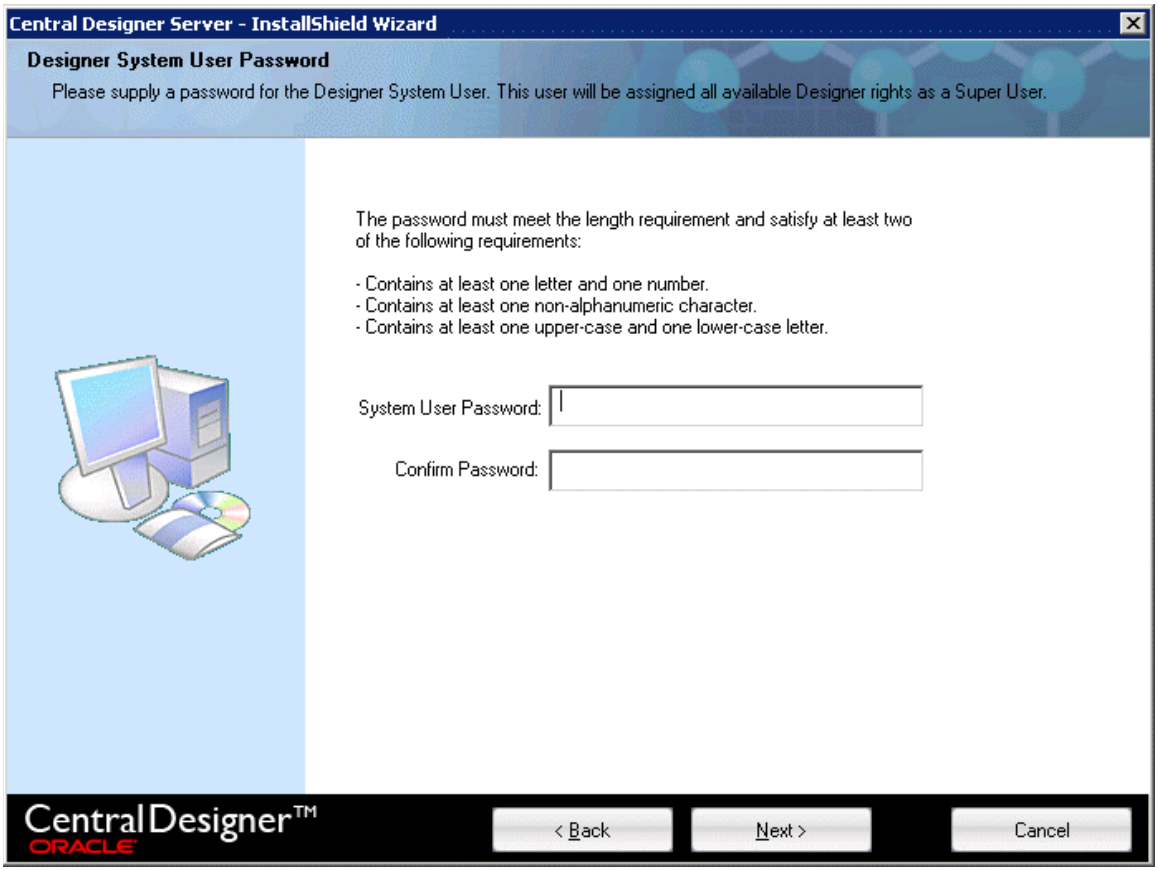
- If this installation is the first server in the web farm, the primary Job Scheduler has not been set yet. The installation automatically sets the Job Scheduler service on the server computer as the primary Job Scheduler. If you install additional application servers, you can change the primary Job Scheduler during the installations.
- If this installation is the second or higher server in the web farm, the primary Job Scheduler service has already been set, and the name of the computer that runs the primary Job Scheduler appears. To change the primary Job Scheduler, select **Make this server's Job Scheduler the primary**.

14 Specify a password for the Job Service user.

Note: Make sure that the user password meets the requirements listed on the page.

15 Click **Next**.

The following page appears.



16 Specify a password for the system user.

Note: Make sure that the user password meets the requirements listed on the page.

The Central Designer application installs the system user by default. You can configure the lockout time for the system user separately from all other users. By default, this user is assigned the superuser and DesignerAdministrator roles.

Note: The password that you specify for the system user is also used for the **archiveimporter** user. For more information about this user, see the ***Administrator Guide***.

17 Click **Next**.

The Network Parameters page appears.

18 In the **Web server URL root** field, enter the server address to which requests will come (for example, *http://ABCServer* or *https://ABCServer*). If you enabled Transport Layer Security (TLS), use *https*.

Note: When the application server is installed in an environment that includes a hardware networking switch, the URL that you enter for the **Web server URL root** field must match the URL that the networking switch uses to address the application server. For more information, see ***Hardware networking switches*** (on page 23).

As you enter a value in the Web server URL root field, the Public server URL root field is automatically updated with the same value. If you edit the value in the Public server URL root field, the field is no longer updated automatically when the Web server URL root field is updated.

19 Optionally, you can secure (encrypt and prevent tampering of) communications by using Transport Layer Security (TLS). For more information, see *Securing communication with Transport Layer Security (TLS)* (on page 69).

20 Optionally, if the application server computer is behind a proxy that rewrites the request URLs, in the **Public server URL root** field, enter the address that the client computer uses to access the application server (the public address of the server computer as seen by the client computer). This address will be added as the address of the server computer during installation of the client applications.

If the value for the **Public server URL root** field does not need to be different from the **Web server URL root** field, make sure that the values in both fields match.

21 Specify the certificate to use to sign web service authorizations:

a Click **Choose Certificate**.

The Choose Certificate dialog box appears.

b Select a certificate.

c Click **OK**.

The Issued to, Issuer, Expiration, and Friendly name fields are populated.

Note: On each Central Designer application server, an administrator must install the certificate that is used for signing web service authorizations to the LOCAL_MACHINE\MY store. The Central Designer installation process grants Full Control to access the certificate private keys to the IIS AppPool\DefaultAppPool user and the NETWORK SERVICE user.

If a user other than the IIS AppPool\DefaultAppPool user is running the DefaultAppPool application pool, you must grant the user Full Control to access the private keys, or the user is unable to sign using the certificates. For more information, see ***Installing certificates for signing web service authorizations and deployment packages*** (on page 14).

22 If the Central Designer application server is outside the network of the InForm application server. Specify the proxy URL or script used by the Central Designer application server to communicate with the InForm server during automated deployment:

- In the **Proxy URL** field, enter the web address for the proxy server.
- In the **Proxy Script** field, enter the web address for the proxy configuration script.

23 Click **Next**.

The Client Installation Configuration page appears.

24 In the Environment Name field, enter the name for your Central Designer instance.

The environment name appears on the web page to which you navigate to start the Central

Designer application.

25 Click **Next**.

The InForm Deployment page appears.

26 Specify the certificate to use to sign deployment packages and InForm web service authorizations:

a Click **Choose Certificate**.

The Choose Certificate dialog box appears.

b Select a certificate.

c Click **OK**.

The Issued to, Issuer, Expiration, and Friendly name fields are populated.

Note: For studies hosted by Oracle Cloud for Industry, the certificate must be issued by a trusted commercial Certificate Authority.

27 Click **Next**.

The Start Copying Files page appears.

28 Review the installation settings. To change any settings, click **Back**. If you are satisfied with the settings, click **Next**.

The installation begins. The Setup Status page appears, showing the status of the installation.

When the installation is complete, the InstallShield Wizard Complete page appears.

29 Click **Finish**.

Note: If the IIS worker process is running under any user other than NETWORK SERVICE or IIS AppPool\DefaultAppPool, you must grant the user read permission to the HKEY_LOCAL_MACHINE\SOFTWARE\OracleHS\CentralDesigner registry key after the installation.

Performing a silent installation

To create a setup.iss response file that contains all the installation parameters:

1 In a command prompt window, enter the path of the Central Designer setup.exe program followed by /r to run the installation in record mode.

The InstallShield Wizard appears.

2 Follow the wizard steps.

3 When you reach the Start Copying Files page, the setup.iss file is created in the Windows directory (by default C:\Windows).

To perform a silent installation:

1 Copy the setup.iss file to the same directory as the Central Designer setup.exe program.

2 In a command prompt window, enter the path of the setup.exe program followed by /s.

The silent installation is performed.

Verifying the installation of the application server

1 Verify that the job service is installed and running:

   a Open the **Control Panel**.

   b Open **Administrative Tools** > **Services**.

   c Verify that the **Oracle Central Designer Job Scheduler** service exists and is running.

2 Verify that the Web site has been added to the Internet Information Services (IIS) Manager directory:

   a Open the **Control Panel**.

   b Open **Administrative Tools** > **Computer Management**.

   c Open **Services and Applications** > **Internet Information Services (IIS) Manager** > **Web Sites** > **Default Web Site**. Verify that **CentralDesigner** is listed in the virtual directories.

3 Review the **installer.log** file. This log contains messages that were generated during installation. It is available in the following location:

   \Program Files\Oracle Health Sciences\Central Designer

Uninstalling the application server

Note: For Central Designer environments that run on the Windows 7 or Windows 2008 operating system, stop the job scheduler and IIS services before you perform this procedure.

1 Open **Control Panel** > **Add or Remove Programs**.

2 Select **Central Designer Server**, and click **Change/Remove**.

A confirmation dialog box appears.

3 Click **Yes**.

The Setup Status page appears, informing you of the status of the uninstall.

The Uninstall Complete page appears.

4 Click **Finish**.

5 Delete the Central Designer directory.

Configuring SMTP settings for automated deployment email notifications

The Central Designer application can send email notifications for the following automated deployment events:

- Deployment request is created, approved, or rejected.
- Deployment is started.
- Deployment is completed successfully or with failures.
- Deployment request is cancelled.
- Deployment is cancelled.

To set up Central Designer to send email notifications:

1 Install the SMTP server feature in Microsoft Windows. For more information, see the Microsoft documentation for your operating system.

2 Verify that you can send email from the SMTP server.

3 After you install the Central Designer application server, configure the Central Designer web site to send email.

   a Select **Start** > **Administrative Tools** > **Internet Information Services (IIS) Manager**.

   b Expand <*machine_name*> > **Sites** > **Default Web Site**.

   c Select CentralDesigner.

   d In the Features View, double-click **SMTP E-mail**.

   The SMTP E-mail page appears.

   e Enter a dummy address as the email address from which messages are sent (for example, *designer@mycompany.com*).

   f Select **Deliver e-mail to SMTP server**.

   g Select **Use localhost**.

   h Select the same authentication settings that are configured for the SMTP server.

   i Click **Apply**.

Note: Every time you install the Central Designer application, you must reconfigure the SMTP email settings for the Central Designer web site.

Starting the Central Designer client application

The client applications are ClickOnce applications, and you do not need to install them to start them, as you would for applications using a traditional Windows installer.

1 Using Internet Explorer, navigate to the following address:

http://<*server name*>/CentralDesignerInstall

In the previous address, <*server name*> is the name of the application server computer.

2 Click the **Start Central Designer Client** link.

The application files are downloaded to a cache and the application is installed. The installation might take some time.

After the installation is complete, the application opens, and you can log on.

Starting the Central Designer Administrator client application

The client applications are ClickOnce applications, and you do not need to install them to start them, as you would for applications using a traditional Windows installer.

1 Using Internet Explorer, navigate to the following address:

http://<*server name*>/CentralDesignerInstall

In the previous address, <*server name*> is the name of the application server computer.

2 Click the **Start Central Designer Administrator** link.

The application files are downloaded to a cache and the application is installed. The installation might take some time.

After the installation is complete, the application opens, and you can log on.

CHAPTER 6

Upgrading the software to this release

In this chapter

About upgrading the application server

Use these instructions to upgrade to this release from any previous release.

When you upgrade, you must:

- Choose whether to update the existing database or create a new database.

  Caution: Unless you choose the update option, your existing database will be deleted.

- Provide the database and user parameters that you entered when you created the new database and database user.

Time considerations

Because the upgrade updates every study in the database, upgrading from an earlier release could take some time, so plan your upgrade carefully. For example, Oracle expects that upgrading a database with 150 studies could take 10 - 15 hours or longer.

Checklist—Planning an upgrade

☑	Task		Information
❑	1	Export the Central Designer database user.	**Caution:** You **must** perform this step. If the upgrade is not successful, you might need to restore the database to attempt to install again. Depending on the size of the database, this process could take several hours. **Note:** Use the following command to export a user: exp designer@db1_dev1 file=file_to_export.dmp buffer=99999 In this example, the user has the following information: • **User name**—designer • **Database**—db1_dev1: **Note:** When you execute this command, you are prompted for the user password.
❑	2	If you are upgrading to an Oracle 12c database, create a new database instance with a 16k block size for the DESIGNER tablespace.	*Create the database and tablespace* (on page 29).
❑	3	If you are migrating to a new database, import the database user into the destination database server.	Use the following command to import a database user into the destination database server: imp designer@db1_dev1 fromuser=designer touser=designer file=file_to_export.dmp In this example, the user has the following information: • **User name**—designer • **Database**—db1_dev1 **Note:** When you execute this command, you are prompted for the user password.

☑	Task		Information
❑	4	If you are migrating to the Oracle 12c database version, re-map the tablespaces.	Use the following command to import a database user into the destination database server: imp designer@db1_dev1 fromuser=designer touser=designer REMAP_TABLESPACE=DESIGNER_BIGINDEX:DESIGNER file=file_to_export.dmp In this example, the user has the following information: • **User name**—designer • **Database**—db1_dev1 **Note:** When you execute this command, you are prompted for the user password.
❑	5	Make sure that the Cursor Sharing setting for the database instance is set properly.	*Configuring the Cursor Sharing setting for a database instance* (on page 30).
❑	6	Make sure that the following services are running: • IIS Admin Service • World Wide Web Publishing Service	If the services are not running, the installation fails. The IIS Admin Service does not have to run for the duration of the installation. However, you must start it before you click the Next button on the Copying Files screen. **Note:** Do not use the **iisreset** command from the MMC or a command prompt after the installation or upgrade completes, or the IIS settings that were set by the installer are lost. Instead, use the **net start** command to start the services.
❑	7	Configure the application server for optimal performance.	*Configuring the application server for optimal performance* (on page 25).
❑	8	Unlock statistics for specific tables.	Unlock statistics for the following tables: IC_OBJECT IC_OBJECT_REVISIONS IC_OBJECT_BACK_REFERENCES IC_OBJECT_FORWARD_REFERENCES IC_BLUEPRINT_OBJECT_MAP The upgrade process drops non-primary key indexes on the tables affected by the upgrade and recreates the indexes at the end of the process. If the index was originally defined with the COMPUTE STATISTICS clause, the recreation also attempts to COMPUTE STATISTICS. If statistics are locked, this process fails.

☑	Task		Information
❑	9	Make sure that: • The database UNDO_MANAGEMENT initialization parameter is set to AUTO. • The UNDO and TEMP tablespaces are set to autoextend.	These settings are necessary for a successful upgrade.
❑	10	If you added any new indexes to the database, you must drop them before upgrading to ensure that they do not cause conflicts with new indexes that have been added to the product.	After the upgrade is finished, you can add the indexes back.
❑	11	If you upgrade from release 2.1.1.3 or earlier, install a certificate for signing deployment packages and InForm web service authorizations.	*Installing certificates for signing web service authorizations and deployment packages* (on page 14).
❑	12	If necessary, install the root certificate and intermediate certificate or certificates, and install the main certificate as the root certificate.	*Installing root and intermediate certificates* (on page 16). *Installing the main certificate as the root certificate* (on page 17).
❑	13	Export custom reports definitions from the Central Designer Administrator application.	*Upgrading custom reports definitions* (on page 60).
❑	14	Update data mappings with the PhysicalMappingType property set to All.	*Updating data mappings with PhysicalMappingType set to All* (on page 56).
❑	15	(Recommended) Run the **DetectStudiesWithUnitsWithSpaces.sql** script to determine if any studies contain unit names with spaces.	A validation check produces an error if a unit name contains a space. *Running the DetectStudiesWithUnitsWithSpaces.sql script* (on page 55).
❑	16	If you upgrade to this release from a release prior to Central Designer 2.0, run the **DetectMisconnectedGlobalConditions.sql** script to identify errors in the way global conditions are referenced by study objects in a study workflow.	*Running the DetectMisconnectedGlobalConditions.sql script* (on page 56).

☑	Task		Information
❑	17	If you upgrade from a release prior to Central Designer 2.0, run the **DetectInvalidCodeListItems.sql** script to identify codelist items of types that are incompatible with the type of their parent codelist.	*Running the DetectInvalidCodeListItems.sql script* (on page 56).
❑	18	(Optional) If you upgrade to this release from a release prior to Central Designer 2.0, run the **TestForOverflow.sql** script to identify values that exceed 1000 characters in certain columns and need to be truncated.	*Running the TestForOverflow.sql script* (on page 56).
❑	19	If you perform automated deployments to InForm studies hosted by Oracle Cloud for Industry (OCI), make sure the Microsoft Windows setting Automatic Root Certificates Update is turned on.	Automatic Root Certificates Update is turned on by default in Microsoft Windows 2008. For more information, see the Microsoft website (http://technet.microsoft.com).
❑	20	Run the application server installation to upgrade the application server.	*Upgrading the application server* (on page 61).
❑	21	If you dropped indexes from your database before upgrading, add them back in after you finish upgrading.	No additional information.
❑	22	If the IIS worker process is running under any user other than NETWORK SERVICE or IIS AppPool\DefaultAppPool, you must grant the user read permission to the HKEY_LOCAL_MACHINE\SOFTWARE\OracleHS\CentralDesigner registry key after you upgrade the Central Designer application server.	No additional information.
❑	23	After you upgrade the Central Designer application server, recompile user-defined functions and sign and secure user-defined function assemblies as needed.	*Upgrading user-defined functions* (on page 57).
❑	24	Re-import custom reports definitions.	*Upgrading custom reports definitions* (on page 60).

☑	Task		Information
❑	25	If you upgrade to this release from release 2.0 or 2.0.1, recompile all user-defined function assemblies to reference the latest version of Oracle.Designer.ExternalFunctions.dll (found in the Central Designer\bin folder of the installation directory) and re-import them into any study or library that contains function objects that reference the assemblies.	No additional information.
❑	26	Configure SMTP settings for sending email notifications related to automated deployment events.	*Configuring SMTP settings for automated deployment email notifications* (on page 45).
❑	27	If the web service authorization and deployment authorization certificates have expired, upgrade them. **Note:** If the certificates are current, you can skip this step.	*Updating certificates without reinstalling the Central Designer software* (on page 68).
❑	28	Inform users that they can resume using the client applications.	*Starting the Central Designer client application* (on page 46). *Starting the Central Designer Administrator client application* (on page 47).

Running the DetectStudiesWithUnitsWithSpaces.sql script

A SQL script called **DetectStudiesWithUnitsWithSpaces.sql** generates a report that identifies the unit names with spaces and the study projects that contain unit names with spaces. Oracle recommends that you run this script because a validation check produces an error if a unit name contains a space.

Run the script before upgrading the application server. If the script finds units with spaces and study projects that use the units, perform the following steps:

1 In any affected study, run validation to determine the items that refer to the units with spaces in their names.

2 Modify the units file to remove the spaces from the unit names that appear in the output file.

3 Using **Control Panel** > **Administrative Tools** > **Services**, restart the Job Scheduler service (Oracle Central Designer Job Scheduler).

4 Restart the client applications.

5 In any affected study, modify the items to use the unit names that do not contain spaces.

The script and a readme file (DetectStudiesWithUnitsWithSpaces.Readme) are available on the product ZIP file in the **InstallSupport** directory.

Running the DetectMisconnectedGlobalConditions.sql script

In releases of the Central Designer application prior to release 2.0, in certain scenarios, global conditions were incorrectly removed from study objects in study workflow. Run the **DetectMisconnectedGlobalConditions.sql** script before upgrading the application server from a release prior to 2.0 to detect global conditions that are not connected correctly to study objects in the study workflow.

The script and a readme file (DetectMisconnectedGlobalConditions.Readme) are available on the product ZIP file in the **InstallSupport** directory.

Running the DetectInvalidCodeListItems.sql script

To be used in a rule, a codelist item must have the same data type as its parent codelist. If the data types do not match, when you upgrade from a release prior to 2.0, the data types of the codelist items are changed to the data types of their parent codelists. Changes in data type could have an impact on study reporting database extracts when new Central Designer 2.1 deployments are executed.

A SQL script called **DetectInvalidCodeListItems.sql** generates a report that identifies codelist items of types that are incompatible with the type of their parent codelist.

Run the script before upgrading the application server to assess the impact of data type changes on studies that are upgraded. The script and a readme file (DetectInvalidCodeListItems.Readme) are available on the product ZIP file in the **InstallSupport** directory.

Running the TestForOverflow.sql script

The **TestForOverflow.sql** script checks whether any value in the following columns is more than 1000 characters:

- IC_APPROVALMEANING.MEANINGNAME
- IC_APPROVALPOLICY.POLICYNAME
- IC_BASELINE.DESCRIPTION
- IC_COLLABORATIONOBJECT.SUMMARY
- IC_DEPLOYMENT.DESCRIPTION
- IC_FILESTORE.DESCRIPTION
- IC_VERBATIM_TYPE.VERBATIM_TYPE_DESCRIPTION
- IC_VERBATIM_TYPE.VERBATIM_TYPE_NAME

Run this script before **upgrading the application server from a release prior to 2.0** . Truncate any values that exceed 1000 characters before upgrading to the current release of the Central Designer software.

The script is available on the product ZIP file in the **InstallSupport** directory.

Updating data mappings with PhysicalMappingType set to All

If a study contains a data mapping for which PhysicalMappingType is set to All and you use the data

mapping for both CDD and CIS, you must use the existing data mapping for one purpose only and create a new data mapping for the other purpose.

Because creating a new database for CDD is simpler, Oracle recommends using the existing data mapping for CIS and creating a new CDD data mapping and, if necessary, a new CDD database.

To modify the existing data mapping and create a new data mapping:

1 To determine whether your database contains any data mappings for which PhysicalMappingType is set to All, before you upgrade, run the **DetectStudiesWithPhysicalMappingAll.sql** script, which is available in the **InstallSupport** directory on the product ZIP file.

2 For each data mapping for which PhycialMappingType is set to All, change the PhysicalMappingType property of the data mapping from All to CIS.

   The CIS data mapping continues to work as expected, and you are able to perform resynchronizations with the CIS database.

3 Create a new CDD data mapping.

4 Copy the data sets in the CIS data mapping and paste them into the CDD data mapping.

   The RefNames of the data sets and their data series are appended with _1.

5 If you deployed the study to the InForm application in an earlier release:

   - Remove the _1 appended text from the aliases of the data sets and data series in the CDD data mapping.

     Caution: Do not update the RefNames, or you will not be able to perform a CIS resynch after you deploy again to the InForm application.

6 Deploy the study to the InForm application.

7 Set up the new CDD database.

Note: After you create a new data mapping for either CDD or CIS, you cannot perform a resynchronization with either the CDD or CIS database. You must create a new database for the new data mapping type.

Upgrading user-defined functions

If a study contains a user-defined function that performs a task such as reading from or writing to a file, accessing the database or the registry, making web service calls, running an external application, sending an email, or using the event log directly, the assembly for the user-defined function must be signed with a strong named signature that is valid and trusted in order for the function to work in the InForm application.

To ensure that the user-defined functions and assemblies in your study projects and library projects are secure, Oracle recommends that you sign user-defined function assemblies using a strong named, valid and trusted signature.

Note: For InForm studies hosted by Oracle Cloud for Industry, all user-defined function assemblies that require signing must be signed by Oracle Services prior to deployment.

In addition, user-defined functions that use the Log4Net application must use the Central Designer Log4Net wrapper or must be recompiled to use Log4Net version 1.2.10.0. For more information

about the Log4Net wrapper, see the *Rules Reference Guide*.

Identifying user-defined functions and assemblies to update

To identify study and library projects that contain user-defined functions that need to be recompiled or assemblies that need to be secured and signed, run the ValidateCustomFunctionAssemblies.exe file after you upgrade the application server.

Note: User-defined functions that refer to an unsupported Log4Net version must be recompiled or reconfigured to use the Central Designer Log4Net wrapper. For more information about the Log4Net wrapper, see the *Rules Reference Guide*.

1 Locate the ValidateCustomFunctionAssemblies.exe file on the product ZIP file, in the **InstallSupport** directory.

2 Copy the file and paste it to the bin folder in the directory in which you installed the Central Designer application.

3 In a command prompt window, enter one of the following:

- To view assemblies that reference the wrong Log4Net version, enter **ValidateCustomFunctionAssemblies L**.
- To view assemblies with missing, invalid or untrusted signatures, enter **ValidateCustomFunctionAssemblies S**.
- To view assemblies with invalid references to ExternalFunctions.dll, enter **ValidateCustomFunctionAssemblies I**.
- To view all of the above, enter **ValidateCustomFunctionAssemblies**.

4 When prompted, specify the following:

- **System username**—system
- **System password**—Password that you specified on the Database System User Password page during the Central Designer application installation.
- **Path for the output file, including file name**—Location in which to save the output file that lists the study and library projects with user-defined functions that must be updated. For example, **C:\Output\ValidateAssemblies.txt**.

A list of user-defined functions is generated.

Securing and signing user-defined function assemblies

To secure and sign assemblies for user-defined functions, create a key pair, extract the public key, and place the key file on the following servers:

- Central Designer application server. If you are using the Central Designer application in a web farm environment, place the key on all the application servers in the web farm.
- All InForm application servers where studies using the assembly will be deployed.

Note: For InForm studies hosted by Oracle Cloud for Industry, all user-defined function assemblies that require signing must be signed by Oracle Services prior to deployment.

For specific instructions and information about creating and signing an assembly with a strong

named signature, see the *Rules Reference Guide* and the documentation for the tool that you use to create the strong name.

Recompiling user-defined function assemblies

The names of assemblies for user-defined functions have been changed in release 2.0. Therefore, you must recompile all user-defined function assemblies after upgrading from a Central Designer release prior to 2.0.

The following table lists the name changes.

Name in releases prior to 2.0	Name in releases 2.0 and later
PhaseForward.Designer.ExternalFunctions.dll	Oracle.Designer.ExternalFunctions.dll
PhaseForward.Designer.PrebuiltFunctions.dll	Oracle.Designer.PrebuiltFunctions.dll

1 When recompiling, replace references to PhaseForward.Designer.ExternalFunctions.dll with Oracle.Designer.ExternalFunctions.dll.

2 Additionally, recompile assemblies that reference PhaseForward.Designer.PrebuiltFunctions.dll, replacing the reference with Oracle.Designer.PrebuiltFunctions.dll.

3 Import each recompiled function assembly into any study or library that contains function objects that reference the assembly.

After you import, any other studies or libraries use the new versions of the assemblies when validating and creating deployment packages.

Upgrading custom reports definitions

If you have defined custom reports, you must export the XML report definition file before performing an upgrade. After the upgrade, you must re-import the report definitions.

1 In the Central Designer Administrator application, export the XML report definition file. For more information, see the *Administrator Guide*.

2 Upgrade the Central Designer software.

3 Modify the XML file exported in the first step, replacing any instances of **assembly="PhaseForward.Designer.ServerCore"** with **assembly="Oracle.Designer.ServerCore"**.

4 Re-import the report definitions on each Central Designer application server:

   a Copy the updated custom reports definition file to the following location, overwriting the existing file:

   ```
   <designer_root>\
   DBSchema\_Last\Datainstaller\DesignerReportsDefinitions.xml
   ```

   In the previous location, <*designer_root*> is the root directory of the Central Designer installation.

   b From the <designer_root>\bin directory, run the UpdateReports.bat file.

   The UpdateReports.bat file updates the definitions of the custom reports in the database.

Upgrading the application server

1 Export the Central Designer database user.

Caution: You **must** perform this step. If the upgrade is not successful, you might need to restore the database to attempt to install again.

To export a user with the following information:

- **User name**—designer
- **Database**—db1_dev1

Use the following command:

```
exp designer@db1_dev1 file=file_to_export.dmp buffer=99999
```

Note: When you execute this command, you are prompted for the user password.

2 Locate the **setup.exe** program.

The setup.exe program is available the Oracle Software Delivery Cloud (https://edelivery.oracle.com).

3 Double-click **setup.exe**.

The InstallShield Wizard prepares to install the application server.

You are prompted to delete the previous installation of the application server.

4 Click **Yes**.

A welcome page appears.

5 Click **Next**.

A message about the upgrade appears.

6 Review the message, and click **Continue**.

The Customer Information page appears.

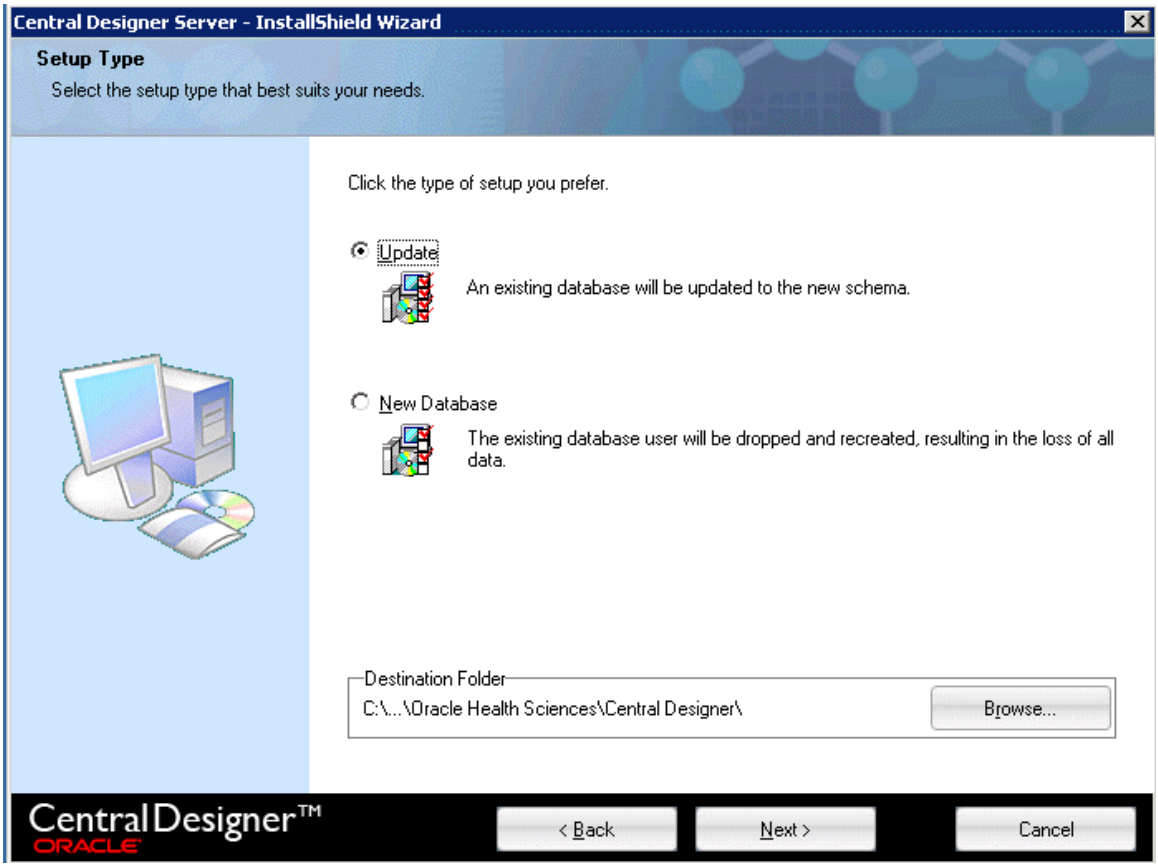
7 Fill in the fields. You should provide the same values that were entered during the initial installation of the application server.

- **User Name**—Your name.
- **Company Name**—The name of your company.
- **Company URL**—A unique identifier for your company data, typically your company URL (for example, http://www.mycompany.com).

Note: You must enter the company URL that you specified during the original Central Designer installation.

8 Click **Next**.

The following page appears.



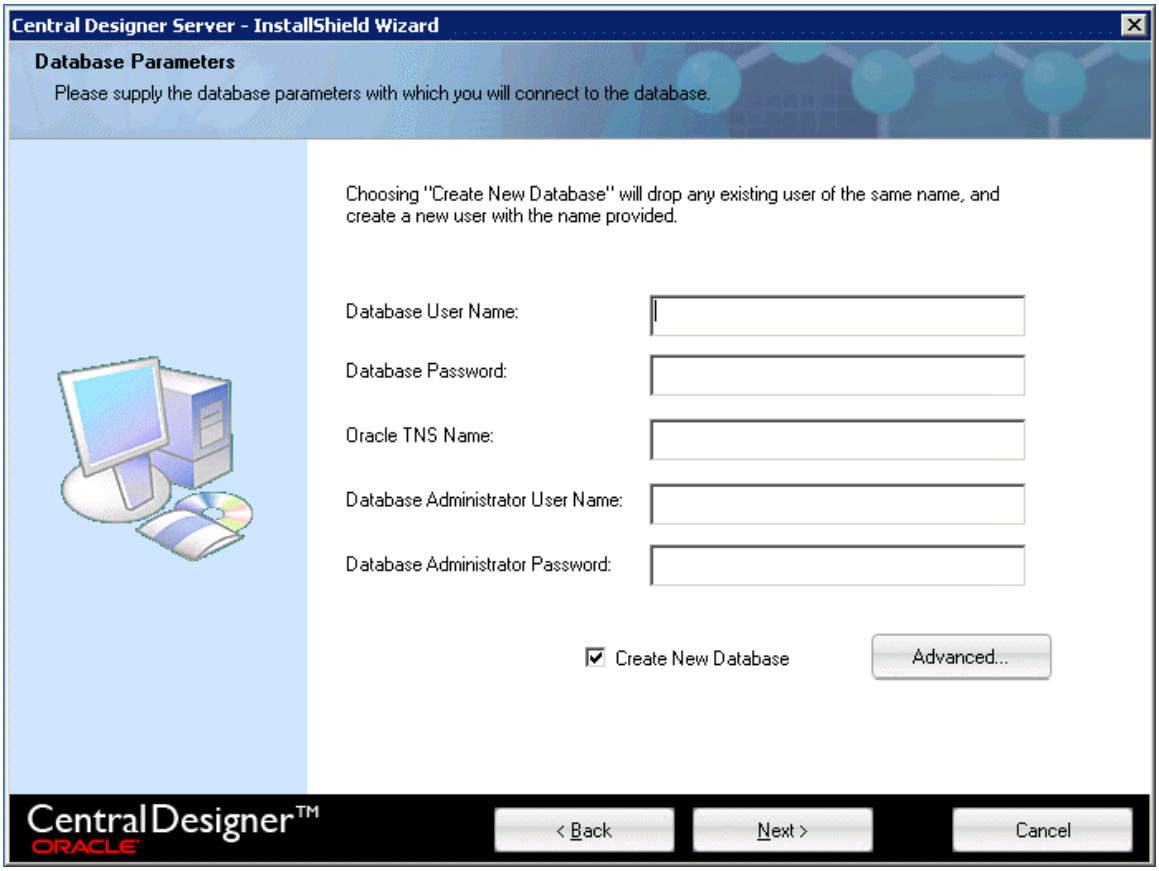
9 Select **Update**.

10 In the **Destination Folder** area, specify the destination location for the installation. By default, the installation wizard installs the software in the <*PROGRAMFILESDIR*>*Oracle**Central Designer*\ folder. *PROGRAMFILESDIR* is a system setting that is usually C:\Program Files. If you want to install to another location, click **Browse**, and select the location. You **must** choose the location to which the application server was initially installed.

Note: The instructions, paths, and Start Menu navigation in this guide assume you are installing to the default location. Oracle strongly recommends that you install the software to the default location.

11 Click **Next**.

The following page appears.



Because you are upgrading, the Create New Database checkbox is grayed out.

12 Fill in the following fields. You **must** provide the values that you created when you set the Oracle TNS name (typically set when you create the database) and the database user name and password (set when you created the Central Designer user in the new database).

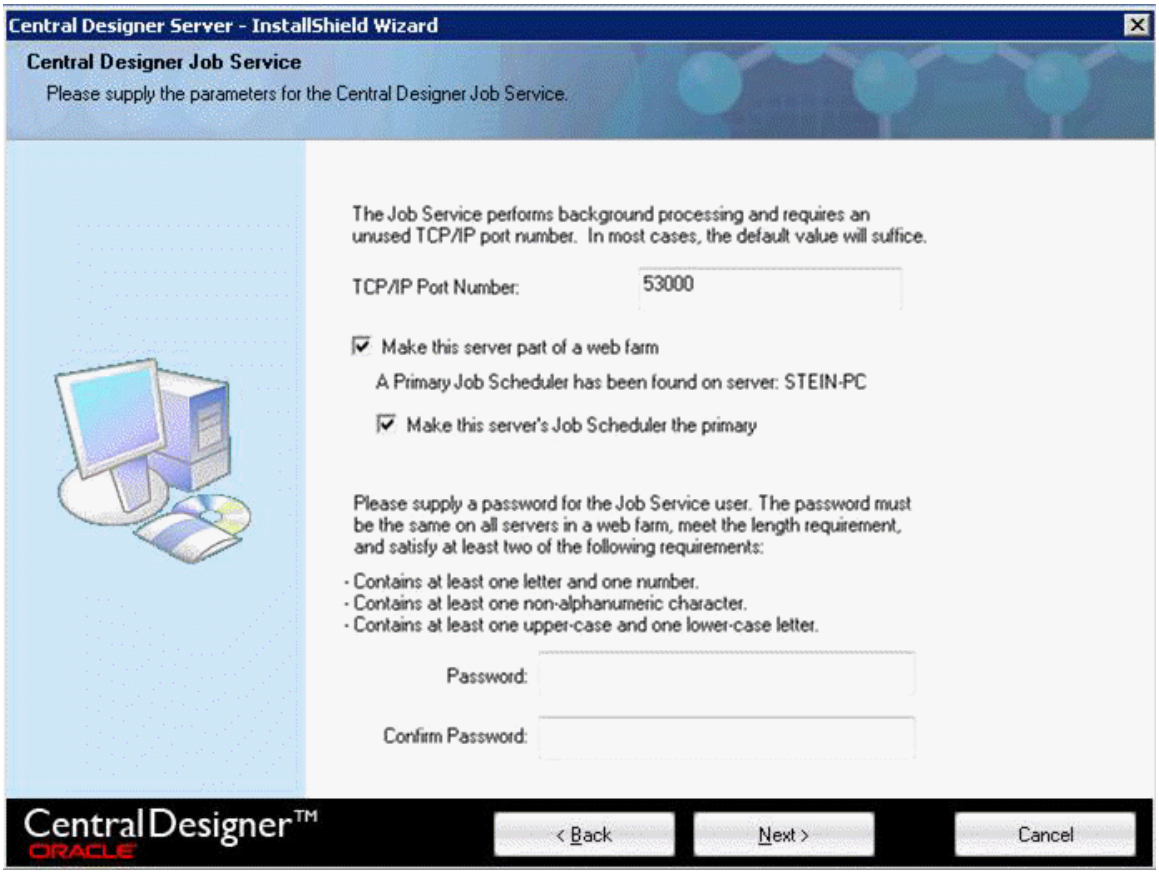
Field	Database
Database User Name	The Oracle user name for the Central Designer database user. **Note:** The password must not contain any of the following characters: @ & ( ) [or].
Database Password	The password for the Central Designer database user.
Oracle TNS Name	Alias from TNSnames.ora file. This TNS name is used to connect to the Central Designer database instance.
Database Administrator User Name	The Oracle user account for the database administrator. This account is used to create the database user. If you provide a database administrator user name different from the one in your original database, you must enter the new user name. **Note:** The user name cannot be a SYSDBA user account.

Field	Database
Database Administrator Password	The password for the database administrator. If you provide a database administrator password different from the one in your original database, you must enter the new password. **Note:** The password must not contain any of the following characters: @ & ( ) [or].

Note: Do not use Oracle reserved words for user names or passwords.

13 Click **Next**.

The following page appears.



14 Enter the TCP/IP port number that the job service will use. The port must be unused. In most cases, you can use the default value.

Note: If you are installing the server as part of a web farm, all of the servers can use the same port number, as long as the port is unused.

15 Optionally, to configure the Central Designer software to support a web farm, select **Make this server part of a web farm**. A web farm setup allows you to install the Central Designer server software on multiple application server computers. The installation is the same for all of the servers, and you must select this option for all servers in the web farm. For more information, see *Web farm capabilities* (on page 4).

After you select the checkbox, the installation checks the database to see if a primary Job Scheduler has been specified. Additional options appear, depending on whether you are installing the first or second (or higher) server.

- If this installation is the first server in the web farm, the primary Job Scheduler has not been set yet. The installation automatically sets the Job Scheduler service on the server computer as the primary Job Scheduler. If you install additional application servers, you can change the primary Job Scheduler during the installations.
- If this installation is the second or higher server in the web farm, the primary Job Scheduler service has already been set, and the name of the computer that runs the primary Job Scheduler appears. To change the primary Job Scheduler, select **Make this server's Job Scheduler the primary**.

16 Specify a password for the Job Service user.

Note: Make sure that the user password meets the requirements listed on the page.

17 Click **Next**.

The Network Parameters page appears.

18 In the **Web server URL root** field, enter the address of the server on its local network (the server address to which requests will come, for example, *http://ABCServer* or *https://ABCServer*). If you enabled Transport Layer Security (TLS), use *https*. Unless you made changes that would cause the server address to have changed, use the address that you entered for the last installation.

Note: When the application server is installed in an environment that includes a hardware networking switch, the URL that you enter for the **Web server URL root** field must match the URL that the networking switch uses to address the application server.

As you enter a value in the Web server URL root field, the Public server URL root field is automatically updated with the same value. If you edit the value in the Public server URL root field, the field is no longer updated automatically when the Web server URL root field is updated.

19 Optionally, you can secure (encrypt and prevent tampering of) communications by using Transport Layer Security (TLS). For more information, see *Securing communication with Transport Layer Security (TLS)* (on page 69).

20 Optionally, if the application server computer is behind a proxy that rewrites the request URLs, in the **Public server URL root** field, enter the address that the client computer uses to access the application server (the public address of the server computer as seen by the client computer). This address will be added as the address of the server computer during installation of the client applications.

If the value for the **Public server URL root** field does not need to be different from the **Web server URL root** field, make sure that the values in both fields match.

21 Specify the certificate to use to sign web service authorizations:

a Click **Choose Certificate**.

The Choose Certificate dialog box appears.

b Select a certificate.

c Click **OK**.

The Issued to, Issuer, Expiration, and Friendly name fields are populated.

Note: On each Central Designer application server, an administrator must install the certificate that is used for signing web service authorizations to the LOCAL_MACHINE\MY store. The Central Designer installation process grants Full Control to access the certificate private keys to the IIS AppPool\DefaultAppPool user and the NETWORK SERVICE user.

If a user other than the IIS AppPool\DefaultAppPool user is running the DefaultAppPool application pool, you must grant the user Full Control to access the private keys, or the user is unable to sign using the certificates. For more information, see ***Installing certificates for signing web service authorizations and deployment packages*** (on page 14).

22 If the Central Designer application server is outside the network of the InForm application server, specify the proxy URL or script used by the Central Designer application server to communicate with the InForm server during automated deployment:

- In the **Proxy URL** field, enter the web address for the proxy server.
- In the **Proxy Script** field, enter the web address for the proxy configuration script.

23 Click **Next**.

The Client Installation Configuration page appears.

24 In the Environment Name field, enter the name for your Central Designer instance.

The environment name appears on the web page to which you navigate to start the Central Designer application.

25 Click **Next**.

The InForm Deployment page appears.

26 Specify the certificate to use to sign deployment packages and InForm web service authorizations:

a Click **Choose Certificate**.

The Choose Certificate dialog box appears.

b Select a certificate.

c Click **OK**.

The Issued to, Issuer, Expiration, and Friendly name fields are populated.

Note: For studies hosted by Oracle Cloud for Industry, the certificate must be issued by a trusted commercial Certificate Authority.

27 Click **Next**.

The Start Copying Files page appears.

28 Review the installation settings. To change any settings, click **Back**. If you are satisfied with the settings, click **Next**.

The installation begins. The Setup Status page appears, showing the status of the installation.

When the installation is complete, the InstallShield Wizard Complete page appears.

29 Click **Finish**.

Upgrading the client applications

Because the client applications are ClickOnce applications, you do not need to upgrade them. Simply start the applications as you always do. For more information, see:

- *Starting the Central Designer client application* (on page 46).
- *Starting the Central Designer Administrator client application* (on page 47).

Updating certificates without reinstalling the Central Designer software

When the web service authorization and deployment authorization certificates expire, you can install renewed certificates without reinstalling the Central Designer software.

The procedure updates the configuration files of both the web server and the job scheduler with the certificates you select and adds access to the private keys for the certificates to NETWORK SERVICE and DefaultAppPool users.

1 Open a command window.

2 Navigate to the <Designer Install Dir>\bin directory.

3 Enter **Oracle.Designer.CertificateManager.exe** and press **Enter**.

A prompt to select the web services authorization certificate appears.

4 Click **OK**.

The Certificate Browser appears.

5 Select the web services certificate, and click **OK**.

A prompt to select the for deployment authorization certificate appears.

6 Click **OK**.

The Certificate Browser appears.

7 Select the deployment authorization certificate, and click **OK**.

Messages appear that indicate the progress of the tool.

CHAPTER 7

Securing communication with Transport Layer Security (TLS)

In this chapter

About communication security

You can secure (encrypt and prevent tampering of) communications by using Transport Layer Security (TLS) and, optionally, by signing authorization information issued by the application server.

With Transport Layer Security, all web traffic between the client applications and the web server is encrypted and tamper resistant. You configure TLS through IIS with an X.509 certificate obtained using your company certificate store or a third party application.

Oracle recommends that you enable TLS. For more information about enabling TLS, refer to the Microsoft documentation about configuring TLS for your operating system.

Note: When you start the client applications, enter the address of the application server, including the correct protocol (either HTTP or HTTPS). If you enable TLS, the address of the application server must begin with HTTPS.

CHAPTER 8

Getting started

In this chapter

Getting started

Logging on to the Central Designer Administrator application

An administrator must log on to the Central Designer Administrator application and create user accounts before other users can log on and use the Central Designer application.

1 Using Internet Explorer, navigate to the following address:

http://<*server name*>/CentralDesignerInstall

In the previous address, <*server name*> is the name of the application server computer.

2 Click the **Start Central Designer Administrator** link.

A dialog box appears, indicating that the application is starting.

The logon window appears.

3 Enter the following information:

- **User name**—system.
- **Password**—Password you set during the server installation.

4 If the web browser connects to the network through a proxy server that requires authentication, click **Proxy Settings** to enter the user name, the password, and the domain used to authenticate the connection to the proxy server.

5 Click **Log On**.

The application opens.

Oracle recommends:

- Changing the password of the system account after you log on to the Central Designer Administrator application.

  For more information, see *Changing your password in the Central Designer Administrator application* (on page 72).

- Deactivating or terminating the system user after you create and activate users.

  For more information, see the *Administrator Guide*.

Changing your password in the Central Designer Administrator application

1 In the Users view, right-click a user name, and

- Select **Change Password**.

  or

  Press **Ctrl+P**.

A dialog box appears.

2 Enter the new password twice for confirmation, and click **OK**.

Logging on to the Central Designer application

You can log on after an administrator creates a user account for you.

1 Using Internet Explorer, navigate to the following address:

http://<*server name*>/CentralDesignerInstall

In the previous address, <*server name*> is the name of the application server computer.

2 Click the **Start Central Designer Client** link.

A dialog box appears, indicating that the application is starting.

The logon window appears.

3 Enter your user name and password.

4 If the web browser connects to the network through a proxy server that requires authentication, click **Proxy Settings** to enter the user name, the password, and the domain used to authenticate the connection to the proxy server.

5 Click **Log On**.

Note: When a user account is created in the Central Designer Administrator application, the administrator can require the user to change the password after logging on the first time. You might be prompted to change your password.

Changing your password in the Central Designer application

If the administrator who created your user account requires that you change your password, you are prompted when you start the application to change your password.

To change your password because it is required:

1 Log on to the Central Designer application.

The Change Password dialog box appears.

2 Enter your old and new passwords. You must enter your new password twice.

3 Click **OK**.

To change your password at any time after logging on:

1 Select **File > Change Password**.

The Change Password dialog box appears.

2 Enter your old and new passwords. You must enter your new password twice for confirmation.

3 Click **OK**.

Logging off

- Select **File** > **Exit**.

If you have unsaved changes, you are prompted to save them.

Overview of configuring the Central Designer software

In the Central Designer Administrator application, you create and manage administrative components such as users, roles, locales, and security settings.

Some tasks in the Central Designer application cannot be performed until the administration information is set up correctly in the Central Designer Administrator application.

Other types of administration, including administering studies and libraries, are performed in the Central Designer application.

Creating a sample deployment package using the sample study

The Central Designer installation package contains a sample study and units file. You can import the files into the Central Designer application and then deploy the sample study to the InForm application using a manual deployment. Perform the following steps to create a sample deployment package.

Step	Task	More information
1	Import the DesignerUnit.xml file into the Central Designer Administrator application. This file updates custom units of measurement.	***Exporting and importing a units file*** in the *Administrator Guide*. The DesignerUnit.xml file is located in the Central Designer installation package in the InstallSupport\Sample Trial folder.
2	Set up locales in the Central Designer Administrator application, and include the following locales for the sample study: • English (United States) • Japanese (Japan) • Czech (Czech Republic) • Spanish (Mexico)	***Adding and removing a locale*** in the *Administrator Guide*.
3	Import the CSML for the sample study into a new study project.	***Importing study objects*** in the *User Guide*. The CSML for the sample study is located in the Central Designer installation package in the InstallSupport\Sample Trial folder.
4	Add the locales from step 2 to the study.	***Choosing the supported locales for a study*** in the *InForm Design Guide*.
5	Select all the dictionary types and all their verbatim types on the Coding tab.	***Associating dictionary types with verbatim types for a study or library*** in the *InForm Design Guide*.
6	Validate the study to create a baseline, and choose to ignore the warnings.	***Validating a study and creating a baseline*** in the *InForm Design Guide*.
7	Create a deployment package.	***Creating a deployment package*** in the *InForm Design Guide*.
8	Save the deployment package to the local computer.	***Saving a deployment package to the file system*** in the *InForm Design Guide*.

Step	Task	More information
9	Copy the deployment package and the public key to a location that is accessible to the InForm server.	No additional information.
10	Perform additional steps in the InForm application to finish setting up the study.	InForm *Installation Guide*.

CHAPTER 9

Troubleshooting

In this chapter

Troubleshooting

What should I do if an error occurs during the server installation?

Errors during server installation can be caused by several issues, including issues with the database user name and with the installation of the Oracle database software.

To troubleshoot:

- Read the installer.log file.

  The installer.log file contains information about the installation, including any errors that occurred. The default location of the file on the application server computer is C:\Program Files\Oracle Health Sciences\Central Designer.

- If the application server and database server are on the same computer, you must install the Oracle Server software and Oracle Client software in the same home, or the Central Designer server installation will not work.

What should I do if when I try to start Central Designer an error occurs indicating ASP.NET is not installed?

If an authentication failed error occurs when you start Central Designer or Central Designer Administrator and the error message indicates ASP.NET is not installed, ASP.NET may not be registered with IIS.

Run the following command to register ASP.NET:

- For 32-bit: **%systemroot%\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe –i**
- For 64-bit: **%systemroot%\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe –i**

About the documentation

Where to find the product documentation

The product documentation is available from the following locations:

- My Oracle Support (*https://support.oracle.com*)—Release Notes and Known Issues.
- Oracle Help Center (*https://docs.oracle.com/cd/E91616_01/index.htm*)—The most current documentation set.

Documentation accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website (*http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc*).

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support or Support Cloud. For information, visit *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs* or visit *http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info* if you are hearing impaired.