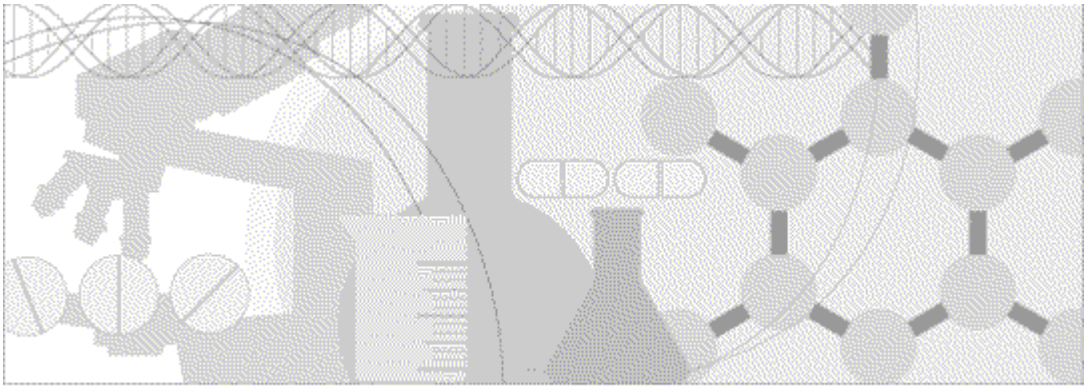
CIS Installation Guide

Clintrial Integration Solution
Release 4.6.2



ORACLE

Part Number E71108-02

Contents

About the documentation 45

CHAPTER 1

Overview of the Clintrial Integration Solution environment

In this chapter

About the CIS environment

The Clintrial Integration Solution (CIS) software is an application that allows users to integrate the features of the InForm software and the Clintrial software in a complete environment for study development and execution.

In a CIS integrated environment, you deploy integrated clinical studies on production servers that gather clinical data through the InForm software EDC interface and store the data in a Clintrial protocol database. The CIS software performs the following integration tasks between the Clintrial software and the InForm software:

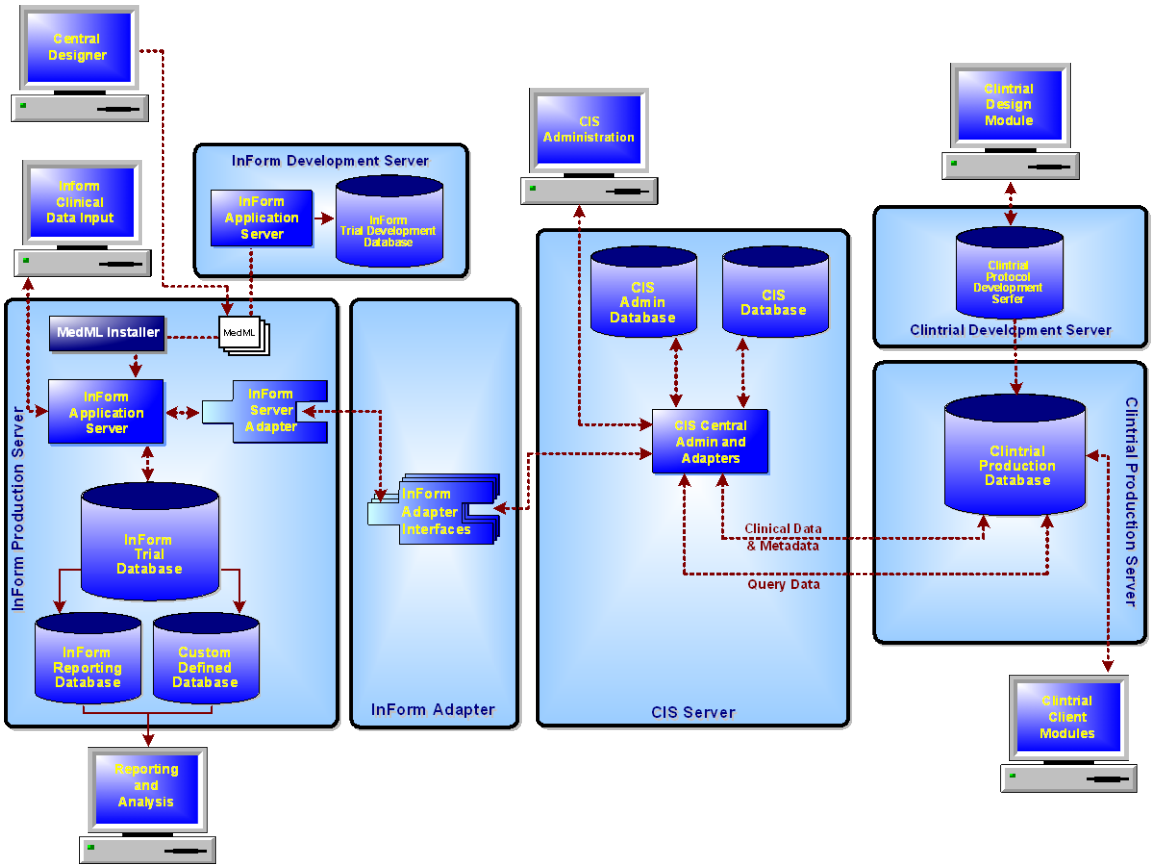
- Transfers and translates study metadata.
- Transfers clinical data.
- Transfers data validation information.

Overview of CIS architecture

The CIS architecture consists of the following components:

Purpose	InForm software	CIS	Clintrial software	InForm Adapter
Study design and implementation	• The Central Designer software.	n/a	Clintrial Design module	n/a
Run-time data entry and data management	• The InForm software. • Reporting and Analysis.	n/a	Clintrial client modules: Classify, Enter, Lab Loader, Manage, Multisite Distribution, Resolve	n/a
Database management (Oracle databases)	• InForm study database (development and production). • InForm reporting database. • Customer-defined database.	• CIS Admin database • CIS database	Clintrial study database (development and production)	The InForm Adapter database.
Data transfer administration	n/a	CIS Administration	n/a	n/a
Data transfer	n/a	n/a	n/a	The InForm Adapter software

All administration tasks are performed using the CIS Administration application with the Internet Explorer Web browser. The following diagram illustrates the components in the CIS environment.



Deployment scenarios and requirements

When planning the deployment of the CIS software, you must determine how to configure the software components on the computers in your CIS environment. Consider the following deployment scenarios:

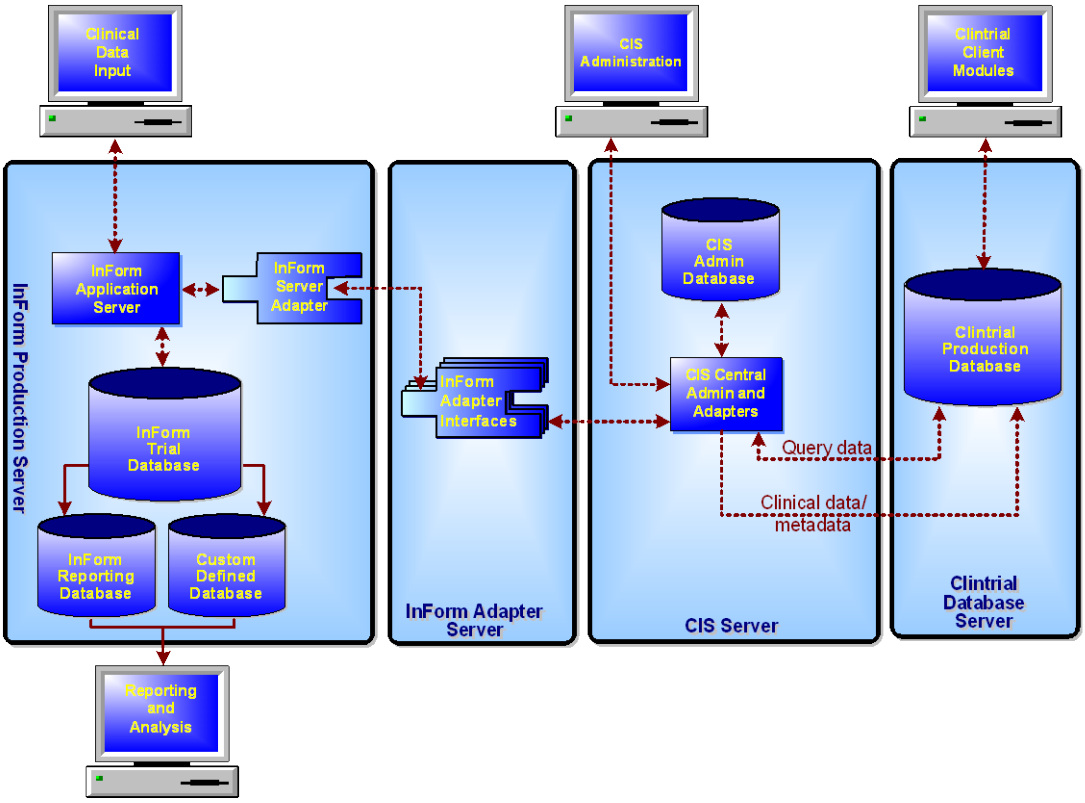
Environment	Where to get more information
A study design configuration in which the InForm Adapter software is installed on a separate computer.	Study design configuration.
A production configuration in which the InForm software, the CIS software, and the Clintrial software are installed on separate computers.	*Production configuration installed on separate computers* (on page 6).
A production configuration in which Oracle hosts the study.	*Production configuration for studies hosted by Oracle* (on page 7).

In addition, if your studies are large, consider employing a load-balancing strategy to distribute the processing load over multiple servers. Your load-balancing solution could be used in any deployment scenario. For more information, see *Load balancing configurations* (on page 8).

If you are installing multiple software components on the same computer, consider the installation and connectivity requirements for both the CIS software and the software that supports the CIS software. For more information, see the CIS *Release Notes*.

Production configuration for self-hosted studies

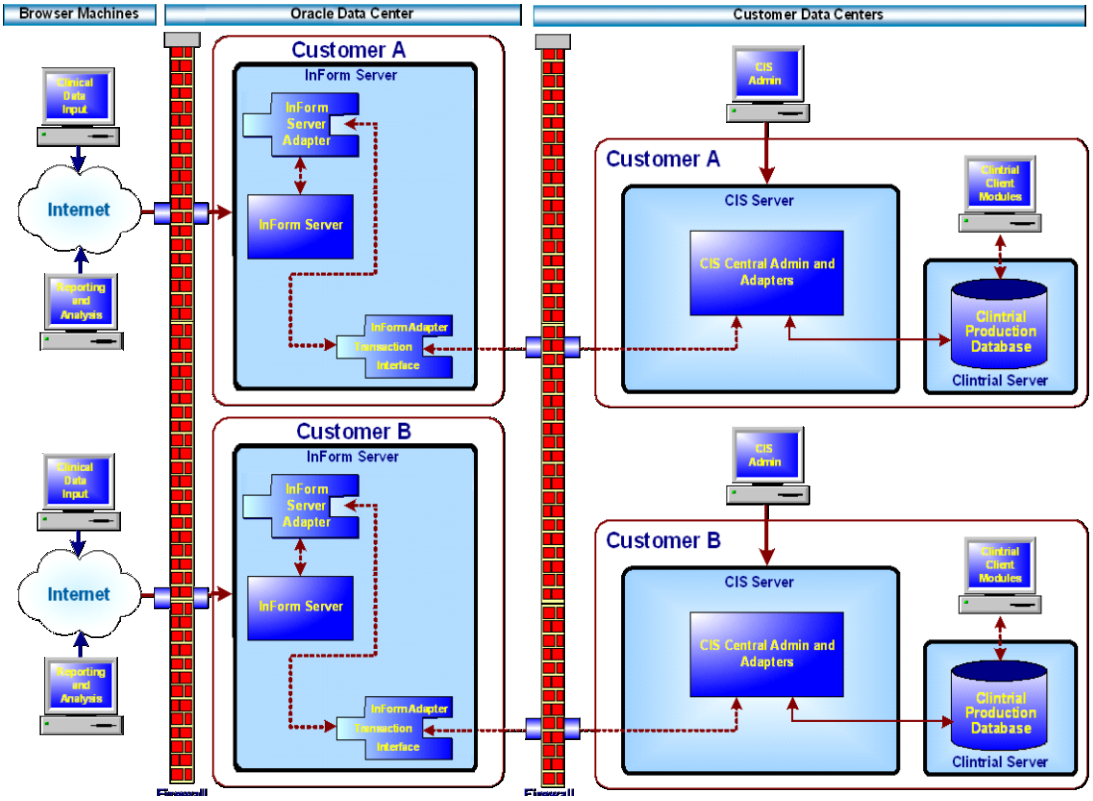
In a test and production environment, you can install the InForm components, the CIS components, and the Clintrial database on separate computers. This configuration is typically used by customers who host the InForm study.



Production configuration for studies hosted by Oracle

In a production environment in which Oracle hosts InForm studies, the following configuration is used:

- Each InForm server computer processes trials for only one customer. Studies for other customers are processed by separate InForm server computers.
- Multiple studies for a single customer can be hosted on one or more InForm server computers.
- Each InForm Adapter computer processes InForm server computers for only one customer. InForm server computers for other customers are hosted by separate InForm Adapter computers. One or more InForm Adapters can be registered with CIS.
- InForm and InForm Adapter can be installed on the same server computer.



Load-balancing configurations

As implemented in the CIS software, load-balancing is a process that:

- Distributes the processing of synchronization connections among multiple computers, so that more data can be processed in a shorter period of time.
- Provides fail-over capability by assigning the synchronization processing to another computer if one or more computers fail.

Note: Each synchronization is processed by only one computer at a time. Therefore, load balancing improves the performance of multiple synchronizations, not the performance of a single synchronization.

If the CIS components are installed on a single server, the CIS software performs all load-balancing actions but distributes data only to the single server.

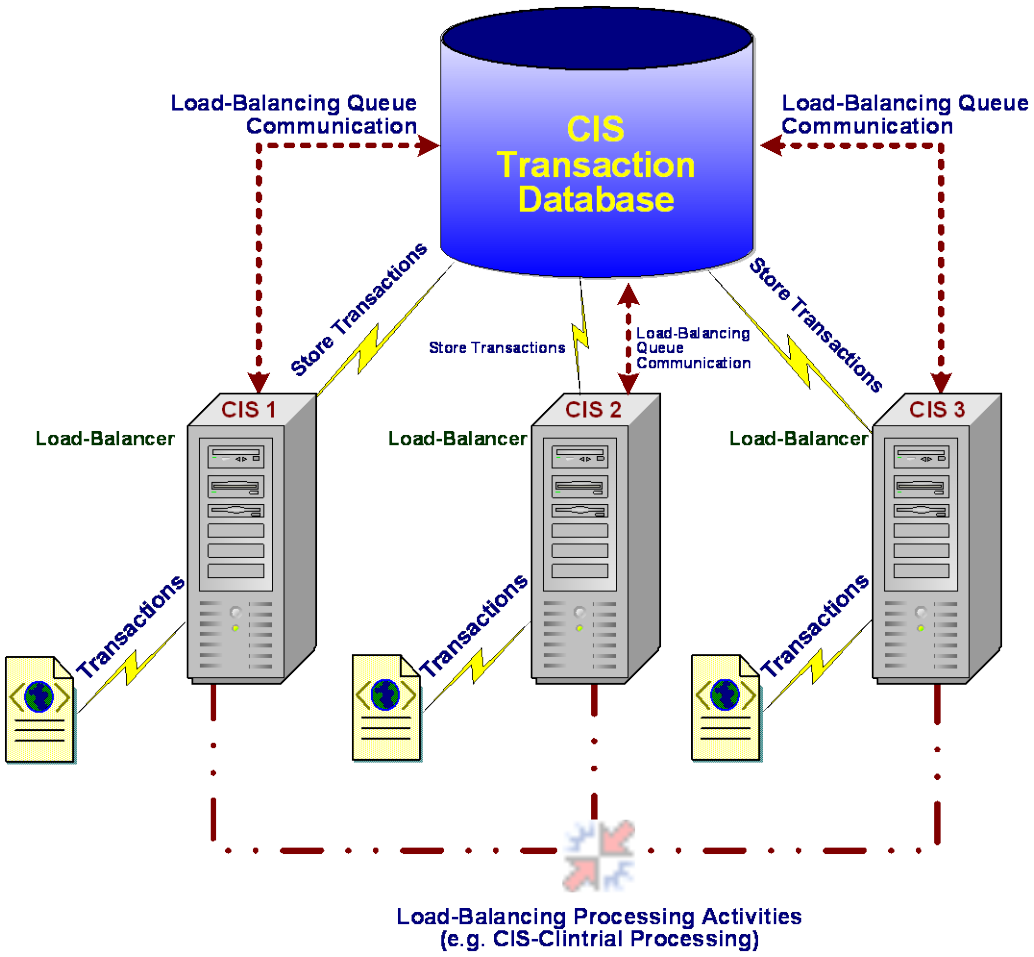
Note: Load-balancing manages synchronization loads only. The CIS Administration user interface should be accessed through a single application server, and should not be load-balanced. If CIS Administration is behind address translators, users should always be forwarded to a single application server.

CIS software load-balancing

To set up a CIS load-balancing configuration, install the CIS software on multiple computers, using the same CIS database credentials for each installation. This configuration provides the following benefits:

- Because the installations use the same CIS database, they share the same synchronization connections and distribute the load of processing those synchronizations among all the computers.
- This configuration provides redundancy. If one or more of the CIS computers fails, processing of synchronization connections continues as long as at least one CIS computer is online and running.

The following figure provides a high-level view of load processing in the CIS software load-balancing configuration.



CHAPTER 2

Planning and prerequisites

In this chapter

Overview of planning

Before installing the CIS software, consider the following installation dependencies and prerequisites:

- Hardware and software requirements.

  For more information, see the CIS *Release Notes*.

- Supported configurations.

  For more information, see ***Deployment scenarios and requirements*** (on page 5).

- Other prerequisites you must meet before you can install the CIS software on your computer.

  For more information, see ***Checklist - Prerequisites*** (on page 13).

Note: Software dependencies might determine which releases of some products you can use. For example, if you install all components of a CIS system on a single server, they must all use the same release of the Oracle software.

Checklist—Prerequisites

Before you install the CIS software, perform the following tasks in the order in which they are presented.

☑		Workflow step	Where to get more information
❑	1	Set up a new Windows 2008 R2 server on which to install the CIS 4.6.2 software.	Microsoft Windows documentation.
❑	2	Install and configure the Oracle software on the Clintrial, InForm, and CIS computers.	• Oracle documentation. • CIS *Release Notes* for: ▪ Minimum Oracle database patches required for the CIS database. ▪ Minimum Oracle software components required for the CIS Oracle client. • ***Installing and configuring Oracle database software*** (on page 15).
❑	3	Purchase and install an X.509 certificate. **Note:** Allow ample time to complete this step.	***Digital certificates*** (on page 20).
❑	4	Decide whether or not to enable TLS for communications between the CIS software and the InForm Adapter software.	
❑	5	Install the Clintrial software.	Clintrial *Getting Started*.
❑	6	Install the InForm software.	For InForm releases 4.6 and 4.7: *InForm Installation and Configuration*. For InForm release 5.0, and later: InForm *Installation Guide*.
❑	7	Install the InForm Adapter software on a development InForm software computer: 1 Install the InForm Server Adapter interface (ISA). 2 Install the Transaction and Central Administration interface for the CIS software. 3 Manually add information about the studies with which the InForm Adapter communicates.	InForm Adapter *Installation Guide*.

☑	Workflow step		Where to get more information
❑	8	Make sure that the InForm Adapter generates transaction XML. Perform this step well before installing the CIS software.	InForm Adapter *Installation Guide*.
❑	9	Set the MTS timeout to control the timeout period for the Microsoft Transaction server.	***Setting the MTS timeout*** (on page 24).
❑	10	Make sure that Microsoft .NET Framework release 4.5.2 is installed on the CIS server.	

Installing and configuring the Oracle database software

Before installing the Clintrial, InForm, or CIS software, install and configure the Oracle software on each computer in your CIS environment.

For information about setting up the Oracle software on the InForm Server, see the following InForm documentation as appropriate for your configuration:

- For InForm releases 4.6 and 4.7, see the *InForm Installation and Configuration Guide*.
- For InForm release 5.0 and higher, see the InForm *Installation Guide*.

For information about setting up the Oracle software on the Clintrial server, see the Clintrial *Getting Started* manual.

Note: The following Oracle Database patch is required for the Clintrial database server if it is running Oracle 11.2.0.4:

- For a Linux Clintrial database server—Patch number 16305657 (OBJECTS LOCKED FOR INCORRECT DURATION WHEN SQL RUN FROM PLSQL).
- For a Windows Clintrial database server—Patch number 22839608 (WINDOWS DB BUNDLE PATCH 11.2.0.4.160419).

If you are migrating from a Windows 2003 environment running an earlier release of the CIS software, or upgrading to this release, see the CIS *Release Notes*.

Note: The CIS 4.6.2 release supports only the AL32UTF8 CHARACTER_SET and the AL16UTF16 NATIONAL_CHARACTER_SET.

Updating the tnsnames.ora file

When creating an Oracle instance, you must add entries to the tnsnames.ora Oracle network configuration file. The tnsnames.ora file contains network configuration parameters that enable the Oracle Client to connect with the database server by using an alias. This file is located in the ORACLE_HOME/network/admin directory.

When you make your entries for the CIS software, the TNSnames entries in the tnsnames.ora file for the CIS databases and the Clintrial databases must be the same on all CIS computers. Therefore, you cannot have a different alias on each CIS computer.

Setting initialization parameters

Oracle recommends that you set the db_block_size parameter to 16K (16384 bytes).

Oracle recommends that you use Automatic Memory Tuning.

Required parameters when Automatic Memory Tuning is on

Set the following required initialization parameters.

Parameter	Production servers	Development servers
SGA_MAX_SIZE*	584M	584M
SGA_TARGET	Equal to or less than SGA_MAX_SIZE	Equal to or less than SGA_MAX_SIZE
CHARACTER_SET	AL32UTF8	AL32UTF8
NATIONAL_CHARACTER_SET	AL16UTF16	AL16UTF16

* SGA_MAX_SIZE can be set based on the system available resource. It can be set up to 80% of the system memory for a dedicated server.

Required parameters when Automatic Memory Tuning is off

You can turn off Automatic Memory Tuning by setting SGA_TARGET to 0. If SGA_TARGET is set to 0, you must set the following initialization parameters:

Parameter	Production servers	Development servers
SGA_Target	0	0
DB_CACHE_SIZE	17000	17000
SHARED_POOL_SIZE	102400000	35000000
CHARACTER_SET	AL32UTF8	AL32UTF8
NATIONAL_CHARACTER_SET	AL16UTF16	AL16UTF16

Running required scripts for instance creation

Run the catalog.sql, catproc.sql, and dbmspool.sql scripts during instance creation. These scripts create all the necessary stored procedures and views for the CIS application. Remember to run these scripts for both production and development environments.

The scripts are located in:

```
%ORACLE_HOME%\RDBMS\ADMIN
```

Oracle Corporation also recommends running the UTLRP.SQL script after creating an Oracle instance.

Creating tablespaces

The CIS installation requires two tablespaces, one permanent and one temporary, on the CIS computer:

- The permanent tablespace houses the CIS schema.
- The temporary tablespace is used for temporary data storage.

The names of the tablespaces can be anything that meets your naming conventions. When you install CIS, you indicate the names of the tablespaces you created.

Note: When you create the tablespaces, make sure that the LOGGING option is enabled for BLOB and CLOB objects. For more information, see ***Ensuring that LOGGING is enabled*** (on page 17).

You can use the following script as a model for creating the tablespaces. For larger studies, you might need to increase the size of the tablespaces.

```
CREATE TABLESPACE permanent_tablespace_name
DATAFILE 'PATH\permanent_tablespace_name_01.dbf' SIZE 200m
AUTOEXTEND ON NEXT 10m
DEFAULT STORAGE (
   INITIAL 128K
   NEXT 128K
   MINEXTENTS 1
   MAXEXTENTS UNLIMITED
   PCTINCREASE 0);

CREATE TEMPORARY TABLESPACE temp_tablespace_name
TEMPFILE 'PATH\temp_tablespace_name_01.dbf' SIZE 350m
EXTENT MANAGEMENT LOCAL UNIFORM SIZE 1m;
```

Ensuring that LOGGING is enabled

The installation for CIS references a permanent and a temporary tablespace in which to create the CIS database users. You specify the tablespace names when you run the installation.

When the tablespaces are created, the Oracle LOGGING option for LOB storage (BLOB and CLOB data types) **must** be enabled. LOGGING enabled is the default setting:

- When LOGGING is enabled, Oracle generates full rollback from data pages in the case of media failure.
- When the option is set to NOLOGGING, transactions could fail to commit or roll back if storage media fails.

If you have already created tablespaces with the NOLOGGING setting and have installed the CIS software:

- If you have installed the CIS software but have not performed a synchronization, or if you do not need to keep any data that you have synchronized, follow the instructions in *Dropping and re-creating tablespaces with the option set to LOGGING* (on page 18).
- If you have synchronized data and want to retain the data in the CIS database, change the LOB storage option to LOGGING for the TRANSACTION_DATA column of the *protocol_name*.INF_TRANSACTIONDATA table for each protocol that has been created by CIS synchronization.

Dropping and re-creating tablespaces with the option set to LOGGING

If you have installed the CIS software and created tablespaces with the Oracle LOB storage option set to NOLOGGING and you have not synchronized, or you do not need to keep any data that you have synchronized in the CIS database:

1 Uninstall the CIS software. For more information, see *Uninstalling the CIS software* (on page 34).

2 Drop the Oracle tablespaces for the CIS database users.

3 Re-create the Oracle tablespaces for the CIS users with the Oracle LOB storage option set to LOGGING.

4 Reinstall the CIS software. For more information, see *Installing the CIS software* (on page 25).

Configuring registry settings for the Oracle client

Make sure that the following registry settings are in place for the Oracle client. All values are located in

```
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\MSDTC
```

Key	Name	Data value
MtxOCI (for Oracle 11g)	OracleOciLib	oci.dll
	OracleSqlLib	orasql11.dll
	OracleXaLib	oraclient11.dll
XADLL (For Windows 2008)	mtxoci.dll	Path to the mtxoci.dll file (the [SystemFolder])
SECURITY (For Windows 2008)	NETWORKDTCACCESS	1
	NETWORKDTCACCESSADMIN	1
	NETWORKDTCACCESSINBOUND	1
	NETWORKDTCACCESSOUTBOUND	1
	NETWORKDTCACCESSTRANSACTIONS	1
	XATRANSACTIONS	1

Setting up Oracle XA transaction support on the Oracle server

Perform the following procedure on the CIS database server on each Clintrial database server instance that CIS uses.

1 Log on to Oracle as SYSDBA. For example, type:

```
sqlplus sys/sys_user_password@connection_string as sysdba
```

2 Run the xaview.sql script and create the V$XATRANS$ view:

```
@ORACLE_HOME\RDBMS\ADMIN\xaview.sql
```

3 Grant SELECT access to public:

```
Grant select on v$xatrans$ to public;
Grant select on sys.dba_pending_transactions to public;
```

4 Log on to Oracle as SYS:

```
sqlplus sys/sys_user_password@connection_string
```

5 Set the JOB_QUEUE_PROCESSES parameter. To find the current value, type:

```
select value from v$parameter where name = 'job_queue_processes';
```

If the value does not exist or is less than 1, set the value to a number that is 1 or greater.

Perform the following procedure on the database client machine:

1 Log on to Oracle as SYSDBA. For example, type:

```
sqlplus sys/sys_user_password@connection_string as sysdba
```

2 Run the oramtsadmin.sql script:

```
@ORACLE_HOME\oramts\admin\oramtsadmin.sql
```

Validating the database connection

- From the application server, open a command prompt and issue the command

```
sqlplus system/system_password@alias_in_tnsnames.ora
```

If the test is successful, an SQL prompt appears, and a connection is established to the database server as the user system.

If the test is unsuccessful, you receive an ORA-error. For help with troubleshooting errors, Consult your DBA.

Note: Problems with connections can sometimes be attributed to the database server containing a single Ethernet card with two nodes. Disabling one of the ports from the card usually solves the problem. For help with resolving errors, consult your system administrator.

Securing the CIS environment

Digital certificates

The CIS software and the InForm Adapter software use a X.509 digital certificate to secure messages between the web services in your product environment.

Note: Digital certificates must be issued by a recognized Certificate Authority. Oracle does not accept customer-created certificates.

Before you install the CIS software, obtain a X.509 digital certificate from a third-party vendor and install it. You must specify the name of the certificate during the CIS installation. You can change the X.509 digital certificate after you install the CIS software.

Oracle recommends the use of single-certificate security which allows you to use the customer X.509 certificate on both the CIS and InForm Adapter servers.

- The private key stays on the CIS server.
- The public key of this certificate goes to the InForm Adapter server.

Setting up key certificates for TLS

To enable TLS, follow these steps to set up a key certificate on each server where the CIS software is installed.

- Create the key certificate.
- Install the key certificate.
- Verify that the certificate is installed correctly.

Creating and setting up a key certificate in IIS

1 Open **Internet Information Services (IIS) Manager**.

2 Open the **<***machine_name***>** node.

3 Go to the **IIS Group > Feature View** and double-click **Server Certificates**.

4 From the resulting **Actions** view, select **Create Certificate Request**.

The Request Certificate Wizard appears.

5 Enter the necessary information on the **Distinguished Name Properties** page, and click **Next**.

6 On the **Cryptographic Service Provider Properties** page, leave all default values, and click **Next**.

7 Click **Browse**.

8 Enter the file name and folder location for the certificate request.

9 Click **Finish**.

Installing a key certificate on the server machine in IIS

1 Open your browser and go to the security certificate server URL:

http://<*Windows_2008_security_certificate_server*>/<*certificate _request_page*>.

2 Click **Request a certificate**.

3 Click **Advanced certificate request**.

4 Copy all the text from the certreq.txt file to the first text field of the saved request.

5 Click **Submit**.

6 Select **Base 64 encoded**.

7 Click **Download certificate**.

8 Save the .cer certificate in a folder that you can access later.

9 Open **Internet Information Services (IIS) Manager**.

10 Open the <*machine_name*> node.

11 Go to the **IIS Group > Feature View**, and select **Server Certificates**.

12 From the **Actions** view, select **Complete Certificate Request**.

13 Select the .cer certificate file you downloaded, and enter a **Friendly name**.

14 Click **OK**.

The certificate appears on the Server Certificates page, and in the Microsoft Management Console (under the Certificates Snap-in > Personal Store).

Verifying that the certificate is installed correctly

1 Open a browser window.

2 Type:

`https://<`*`machine_name`***`>.<`***`domain_name`***`>.com`**

The Security Alert window appears.

3 Verify that the date and name for the certificate are valid.

Creating a private key for the certificate

1 Open the Microsoft Management console:

a Open a Command Prompt window.

b Type **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 Expand **Certificates (Local Computer)** > **Personal** > **Certificates**.

11 Right-click the certificate and select **All Tasks** > **Export**.

12 Click **Next**.

13 Select **Yes, export the private key**, and click **Next**.

14 Click **Next**.

15 Enter a password in the two fields, and click **Next**.

16 Enter a file name with a .pfx extension, and click **Next**.

17 Click **Finish**.

Importing the private key to an application server

1 Open the Microsoft Management Console and add the Certificates snap-in. For more information, see *Creating a private key for the certificate* (on page 21).

2 Expand **Certificates (Local Computer)** > **Personal**.

3 Right-click **Certificates**, and select **All Tasks** > **Import**.

4 Click **Next**.

5 Enter the password you specified when you created the private key, and click **Next**.

6 Browse to the private key file with the .pfx extension, and click **Next**.

7 Click **Next**.

8 Click **Finish**.

Granting rights to the NETWORK SERVICE user for the private key

The NETWORK SERVICE user must have read and write access to the private key on the installed certificate.

1 Open the Microsoft Management Console and add the Certificates Snap-in. For more information, see *Creating a private key for the certificate* (on page 21).

2 Expand **Certificates (Local Computer)** > **Personal** > **Certificates**.

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

4 Add the NETWORK SERVICE user to the list of groups and user names.

5 Select the NETWORK SERVICE user and grant it **Full Control** rights.

6 Click **OK**.

Configuring registry settings for TLS 1.2

If TLS 1.2 is enabled on the InForm Adapter computer or on the address translator (in a load-balanced configuration, for example), configure the following registry settings to enable TLS 1.2 on the CIS application server:

- In HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols, create the following keys and subkeys:

Key	Subkey	Entries
SSL 2.0	Client	• DisabledByDefault=1 • Enabled=0
	Server	• DisabledByDefault=1 • Enabled=0
SSL 3.0	Client	• DisabledByDefault=1 • Enabled=0
	Server	• DisabledByDefault=1 • Enabled=0
TLS 1.0	Client	• DisabledByDefault=1 • Enabled=0
	Server	• DisabledByDefault=1 • Enabled=0
TLS 1.1	Client	• DisabledByDefault=1 • Enabled=0
	Server	• DisabledByDefault=1 • Enabled=0
TLS 1.2	Client	• DisabledByDefault=0 • Enabled=1
	Server	• DisabledByDefault=0 • Enabled=1

- In HKLM\SOFTWARE\Microsoft\.NetFramework\v4.0.30319, create a key called SchUseStrongCrypto with the DWORD value=1.

Setting the MTS timeout

Oracle recommends that you increase the default Microsoft Transaction Server (MTS) timeout to a minimum of 300 seconds.

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

2 Click **Component Services**.

3 Double-click the **Computers** folder.

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

5 Select the **Options** tab.

6 In the **Transaction timeout (seconds)** field, enter 300.

7 Click **OK**.

CHAPTER 3

Installing the CIS software

In this chapter

Overview of the installation process

During the CIS software installation, you must:

- Provide required information for each database user.
- Provide the name of a X.509 digital certificate to use for the CIS software.

In addition to installing the CIS software, you must install the InForm Adapter software for your environment. The InForm Adapter software provides interfaces to communicate with the InForm software using web services. For more information, see the InForm Adapter *Interfaces Guide*.

A complete CIS installation requires two database users for different components of the CIS software:

- CIS Sync and Clintrial Adapter schemas are owned by one user.
- The CIS Administration schema is owned by a separate user. The CIS Administration schema must not be owned by the same user as the other schemas.

The installation program checks for prerequisite software. If any prerequisites are missing, the installation stops and displays a list of missing software. For more information, see ***Planning the CIS software installation*** (on page 11) and the System Requirements in the CIS *Release Notes*.

Canceling the installation process

You can use the **Cancel** button to stop the installation process at any time during the installation. When you cancel an installation:

- Any changes you make to CIS are removed and the system returns to the state it was in before you began the installation.
- Database changes are *not* removed, and any changes you make to the database user or tables are kept.

Running the CIS 4.6.2 installation program

Selecting the installation process

Select the appropriate process.

Purpose of this installation	For more information, see
You already have a CIS 4.6.1.5 or earlier installation on a Windows 2003 server, and you are migrating to a Windows 2008 server to install CIS 4.6.2.	The CIS 4.6.2 *Release Notes*.
You already have a CIS 4.6.2 installation, and you are migrating to a different server, or reinstalling CIS on the same server.	*Running the CIS installation with an existing database* (on page 30).
You are creating a new CIS 4.6.2 installation.	*Running the CIS installation for the first time* (on page 27).
You are adding a CIS 4.6.2 load-balanced server. CIS 4.6.2 is already installed on another server, and you want the server you are currently installing to share a database with the existing server.	*Running the CIS installation for a load-balanced configuration* (on page 32).

Running the CIS installation for the first time

Starting the installation

1 Run one of the following batch files:

- **SetupWithLogFiles.bat**—Recommended. This batch file creates log files in the root directory of your installation directory and in C:\. If the installation generates an error, Oracle can use these log files to diagnose the problem.

  Note: After you complete the installation and use the log files to diagnose problems if necessary, delete the log files, because they can contain unencrypted information such as passwords.

- **Setup.bat**—Runs the same series of commands, but does not write the log files that SetupWithLogFiles.bat creates.

The installation begins and the Welcome page appears.

2 Click **Next**.

The Installation Scenario page appears.

3 Select **New install of CIS 4.6.2** and then click **Next**.

The Customer Information page appears.

Providing customer information

1 Enter the following information:

- **User Name**—User that is installing the CIS software.
- **Organization**—Organization that is installing the CIS software.

2 Select whether to install the CIS application for the current Windows user, or for all users.

3 Click **Next**.

The Setup Type page appears.

Choosing the setup type

1 Select the setup type:

- **Typical**—Installs the CIS software to the default location, typically C:\Program Files\Phase Forward.
- **Custom**—Allows you to specify the directory in which to install the CIS software.

2 Click **Next**.

3 If you selected Custom, optionally view the space requirements or change the installation directory, and click **Next**.

The CIS Administration Database Setup page appears.

Setting up the CIS administration database for the first time

1 Enter the database connection information for the CIS administration database user that is created by this installation:

- **CIS Administration Database Instance Name**—Oracle TNS name. The Oracle TNS name must not be greater than 16 characters.
- **CIS Administration Database User**—Database user name and password. The user name that you enter for the CIS Administration database must not be the same as the CIS database user name.

2 Click **Next**.

The CIS Administration Database Account Creation page appears.

3 Enter the following information:

- **Oracle System Username**—Name of an Oracle System user for an existing account.
- **Oracle System Password**—Password for the Oracle System user.
- **Default tablespace**—Name of the default tablespace reserved for the CIS administration database.
- **Temporary tablespace**—Name of the temporary tablespace reserved for the CIS administration database during installation.

Note: If the user name and password you typed on the previous screen already exist, a message appears after you click Next and indicates that the installation will drop (destroy all existing data for that user) and re-create the administration database user.

4 Click **Next.**

The CIS Database Setup page appears.

Setting up the CIS database for the first time

1 Enter the database connection information for the CIS database user that is created by this installation:

- **CIS Database Instance Name**—Oracle TNS name. The Oracle TNS name must not be greater than 16 characters. The default is the database instance you entered for the CIS Administration Database instance.
- **CIS Database User**—Database user name and password. The user name that you enter for the CIS database must not be the same as the CIS Administration database user name.

Note: If the user name and password you typed on this screen already exist, then on the next page, CIS Database Account Creation, after you enter the Oracle System user name, a message appears and indicates that the installation will drop (destroy all existing data for that user) and re-create the CIS Database User.

2 Click **Next**.

The CIS Database Account Creation page appears.

3 Enter the following information:

- **Oracle System User**—Name of an Oracle system user for an existing account. The default is the user name you entered for the CIS administration database account.
- **Oracle System Password**—Password for the Oracle system user. The default is the password you entered for the CIS administration database account.
- **Default tablespace**—Name of the default tablespace reserved for the CIS database. The default is the name you entered for the CIS administration database tablespace.
- **Temporary tablespace**—Name of the temporary tablespace reserved for the CIS database during installation. The default is the name you entered for the CIS administration database temporary tablespace.

Note: If the user name and password you typed on the previous screen already exist, a message appears after you click Next and indicates that the installation will drop (destroy all existing data for that user) and re-create the CIS Database user.

4 Click **Next**.

The Certificate Name page appears.

Selecting a certificate

1 Enter the name of the X.509 certificate you installed for securing communication with InForm Adapter. Enter the name as it appears in the Microsoft Management Console, under Personal Store in the Certificates snap-in.

2 Click **Next**.

The Ready to Install the Program page appears.

Running the installation

- Click **Install**.

  The installation checks for the presence of all of the required software. If any components are missing, the installation stops and lists the missing components.

  Note: If Command Prompt windows appear during the installation, do not click them. Closing these windows interrupts the installation process.

  The InstallShield Wizard Completed page appears when the installation is complete.

Running the CIS installation with an existing database

If you are upgrading to this release or migrating to a new server, you can install CIS with an existing database.

For more information, see the *Release Notes*.

Starting the installation

1 Run one of the following batch files:

- **SetupWithLogFiles.bat**—Recommended. This batch file creates log files in the root directory of your installation directory and in C:\. If the installation generates an error, Oracle can use these log files to diagnose the problem.

  Note: After you complete the installation and use the log files to diagnose problems if necessary, delete the log files, because they can contain unencrypted information such as passwords.

- **Setup.bat**—Runs the same series of commands, but does not write the log files that SetupWithLogFiles.bat creates.

The installation begins and the Welcome page appears.

2 Click **Next**.

The Installation Scenario page appears.

3 Select **Install CIS 4.6.2 with existing database**, and then click **Next**.

The Customer Information page appears.

Providing customer information

1 Enter the following information in the specified fields:

- **User Name**—User that is installing the CIS software.

  Note: If you are updating from a previous version of the CIS software, you must use the same user name that you used in the original installation.

- **Organization**—Organization that is installing the CIS software.

2 Select whether to install the CIS application for the current Windows user, or for all users.

3 Click **Next**.

The Setup Type page appears.

Choosing the setup type

1 Select the setup type:

- **Typical**—Installs the CIS software to the default location, typically C:\Program Files\Phase Forward.
- **Custom**—Allows you to specify the directory in which to install the CIS software.

2 Click **Next**.

3 If you selected Custom, optionally view the space requirements or change the installation directory, and click **Next**.

The CIS Administration Database Setup page appears.

Setting up the CIS administration database for an existing database

1 Enter the database connection information for the CIS Administration database user that is created by this installation:

- **CIS Administration Database Instance Name**—Oracle TNS name. The Oracle TNS name must not be greater than 16 characters.
- **CIS Administration Database User**—Database user name and password. These fields are pre-populated, because you have already installed the initial CIS server. Note that the Create Oracle User and Schema checkbox is unavailable.

2 Click **Next.**

The CIS Database Setup page appears.

Setting up the CIS database for an existing database

1 Enter the database connection information for the CIS database user that is created by this installation:

- **CIS Database Instance Name**—Oracle TNS name. The Oracle TNS name must not be greater than 16 characters.
- **CIS Database User**—CIS Database username and password. Note that the Create Oracle User and Schema checkbox is not enabled. These fields are pre-populated, because you have already installed the initial CIS server.

2 Click **Next**.

The Ready to Install the Program page appears.

Running the installation

- Click **Install**.

  The installation checks for the presence of all of the required software. If any components are missing, the installation stops and lists the missing components.

  Note: If Command Prompt windows appear during the installation, do not click them. Closing these windows interrupts the installation process.

  The InstallShield Wizard Completed page appears when the installation is complete.

Running the CIS installation for a load-balanced configuration

To install the CIS software in a load-balanced configuration:

1 Install the first server using the process for a first-time installation.

  For more information, see *Running the CIS installation for the first time* (on page 27).

2 Install additional servers using the process for a load-balancing installation.

  For each additional server:

  a Start the installation. For more information, see *Starting the installation* (on page 30).

  b On the Installation Scenario page, select **Add CIS 4.6.2 load-balanced server**, and then click **Next**.

  c Continue with the process for an installation with an existing database. For more information, see *Providing customer information* (on page 30).

For more information about load balancing in the CIS environment, see *Load balancing configurations* (on page 8).

Shutting down the Sync Job Scheduler

In a load-balanced configuration, the PhaseForward CIS Sync Job Scheduler service is installed on all the servers, but should be running only on the first CIS server (that is, the server with the full installation).

The installation program installs and starts the service on all the servers.

In a load-balanced configuration, you must manually stop and disable the service on the second and subsequent servers.

1 Open the services applet:

  a Select **Start > Control Panel**.

  b Click **Administrative Tools**.

  c Double-click **Services**.

2 Right-click the PhaseForward CIS Sync Job Scheduler service and select **Stop**.

3 Right-click the PhaseForward CIS Sync Job Scheduler service again and select **Properties**.

4 Change the startup type to **Disabled**.

5 Click **OK** to confirm.

6 Close the windows.

Opening port 9000 in the firewall

In a load-balanced configuration, you must open port 9000 in the firewall software on all application servers that are behind a firewall.

To open port 9000 in the Windows Firewall:

1 Select **Start** > **Control Panel** > **Windows Firewall** > **Advanced settings**.

2 Select **Inbound Rules** > **New Rule**.

The New Inbound Rule Wizard appears.

3 Select **Port**, and click **Next**.

4 In the **Specific local ports** field, enter 9000, and click **Next**.

5 Select the defaults on all the pages of the wizard. Enter a rule name on the last page, and click **Finish**.

Uninstalling the CIS software

1 Open a Windows command prompt from the Teardown folder located in the installation directory (by default C:\Program Files\Oracle\Clintrial Integration Solution\Teardown).

2 Run the following command:

teardown

A confirmation window appears.

3 Click **Yes**.

The uninstallation process starts.

Note: Do not click Cancel before the uninstallation is completed.

When the uninstallation is completed, the following log files are created:

- UnInstall-CTAdapter.log
- UnInstall-CISSync.log
- UnInstall-CentralAdmin.log

CHAPTER 4

After completing the CIS installation

In this chapter

Securing the Service user name and password

During the installation, the Service user is created to support synchronizations. The default user name and password for this user is Service. To secure your CIS environment, Oracle recommends that you change this user password for your specific environment. You must change the password for the Service user on the following pages and in the following order:

1 **Profile tab of the Edit User page**—Select the Service User from the Users tab to change the password.

2 **Settings tab of the CIS Synchronization Adapter page**—Change the password for the Sync user.

For more information, see the *CIS Administrator Guide*.

Securing the predefined CIS user accounts

As installed, CIS includes the following predefined user accounts:

- CAAdmin
- CISAdmin
- CISPower
- CISUser

The default password for the predefined user accounts is the user name. To secure your CIS environment, Oracle recommends that you change the passwords for these accounts. For more information, see ***Editing a user profile*** in the *CIS Administrator Guide*.

After you have created accounts for all of your users and have verified that those accounts are associated with the correct rights, you can disable the predefined user accounts. For more information, see ***Changing the activation state of a user*** in the *CIS Administrator Guide*.

Note: Do not disable the Service account.

Increasing the timeout period for ASP.NET

If a web service request runs longer than the default timeout period for ASP.NET, the following message might appear:

```
Attempted to access an unloaded AppDomain
```

Such a timeout could occur during synchronization.

To resolve this issue, increase the value for **responseDeadlockInterval** in the **machine.config** file on each server. The default value is 3 minutes. This is a global value that applies to all ASP.NET applications. For more information about setting the value, see the Microsoft documentation.

Note: Oracle recommends that you do **not** change the **responseDeadlockInterval** value unless you receive the error as described.

Changing database connection information

If you need to change any of the following information, you must also update the CIS server with the changes:

- Oracle instances.
- CIS database user name.
- CIS database password.
- CIS administration user name.
- CIS administration password.

Usually, you would change this information if the Oracle password is changed.

Important: If your configuration uses a pool of load-balanced CIS servers sharing the same CIS database, you must make the changes on every load-balanced server.

Changing the CIS database connection information

1 Log off from CIS Administration.

2 Stop all CIS services on all load-balancing machines:

- PhaseForward CIS Sync Job Scheduler
- PhaseForward CIS SyncService

3 In the Oracle database software, change the password for the CIS Database User.

4 Log on to a CIS server.

5 Open a Windows command prompt from the root of the installation directory.

6 Enter the following command:

```
UpdateCISPassword Instance User Password
```

For example, if your user is CISDB, the following command changes the CIS password to NEWPASSWORD for the Oracle instance DEV5.WORLD:

```
UpdateCISPassword DEV5.WORLD CISDB NEWPASSWORD
```

7 Start the CIS services.

8 Restart IIS by entering the following command from a Windows command prompt:

```
iisreset
```

Important: If your configuration uses a pool of load-balanced CIS servers sharing the same CIS database, you must make the changes on every load-balanced server.

Important: Any attempt to log in to CIS Administration after the password change might lock the CIS database user, causing an error to occur when you log in. To unlock the user, run the following SQL*Plus command as Oracle system user:

alter user *user* **account unlock**

Changing the CIS administration database connection information

1 Log off from CIS Administration.

2 In the Oracle database software, change the password for the CIS Administration Database User.

3 Log on to a CIS server.

4 Open a Windows command prompt from the root of the installation directory.

5 Type the following command:

```
UpdateCAPassword Instance User Password
```

For example, if your password is CISADMINDB, the following command changes the CIS password to NEWPASSWORD for the Oracle instance DEV5.WORLD:

```
UpdateCAPassword DEV5.WORLD CISADMINDB NEWPASSWORD
```

6 Restart IIS by entering the following command from a Windows command prompt:

```
iisreset
```

Important: If your configuration uses a pool of load-balanced CIS servers sharing the same CIS database, you must make the changes on every load-balanced server.

Important: Any attempt to log in to CIS Administration after the password change might lock the CIS administration database user, causing an error to occur when you log in. To unlock the user, run the following SQL*Plus command as Oracle system user:

alter user *user* **account unlock**

Changing the certificate used for communication with InForm Adapter

1 Set up a certificate. For more information, see *Setting up key certificates for TLS* (on page 20).

2 Open the following files:

- **Web.config**, located in < *InstallationFolder* >\Central Admin.
- **PhaseForward.CISSynchAdapter.CISSyncProcessor.exe.config**, located in< *InstallationFolder* >\CISSync\bin.

3 In the appSettings section of each file, replace the value attribute that contains the name of the old certificate (CIS_old_cert_name) with the name of the new certificate (CIS_new_cert_name). Enter the name as it appears in the Microsoft Management Console, under the Personal Store in the Certificates snap-in.

For example:

```
<appSettings>
  <!-- Added for CIS 4.6.2 (WCF). Will be modified via installer. Must be changed if cert name changes -->
  <add key="cert" value="CIS_new_cert_name" />
</appSettings>
```

4 Save the files.

Configuring CIS behind a Proxy server

If your environment has the CIS software placed behind a Proxy server, you must update the following configuration files:

- *installation_path***Program Files\Phase Forward\Clintrial Integration Solution\CentralAdmin\web.config**
- *installation_path***Program Files\Phase Forward\Clintrial Integration Solution\CISSync\web.config**
- *installation_path***Program Files\Phase Forward\Clintrial Integration Solution\CTAdapter\web.config**
- *installation_path***Program Files\Phase Forward\Clintrial Integration Solution\CISSync\bin\PhaseForward.Platform.JobScheduler.exe.config**
- *installation_path***Program Files\Phase Forward\Clintrial Integration Solution\CISSync\bin\PhaseForward.CISSynchAdapter.CISSyncProcessor.exe.config**

To update the files:

1 Add the default proxy details immediately before the <configuration> tag. This is typically the last tag in the files.

2 Provide the default proxy settings as shown in the following example, with the *proxyaddress* attribute set to the actual address of the proxy server:

```
<system.net>
   <defaultProxy>
      <proxy usesystemdefault="false"
      proxyaddress="http://165.140.4.22:8080" bypassonlocal="true" />
   </defaultProxy>
</system.net>
```

If you do not update the CIS configuration files, you might experience connection problems. For example, the error "The underlying connection was closed: The remote name could not be resolved" might appear in the event log.

The error information includes the operation that was taking place at the point where the connection could not be acquired.

Monitoring MS DTC logs

To avoid running out of space, monitor Microsoft Distributed Transaction Coordinator (MS DTC) logs. These logs are written to frequently; for example, the Oracle software writes trace files to the MS DTC logs. If there are system problems, the logs can quickly reach their maximum size.

Oracle recommends the following:

- Move the logs from their default location (%SystemRoot%\SYSTEM32\MSDTC) to another drive.
- Expand the log file capacity to 64 MB or higher.
- Clear the logs as needed.

To perform these activities, use the tools in the Microsoft Component Services window:

1 Stop the MS DTC service by issuing the following command in a Windows command window:

```
net stop MSDTC
```

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

3 Expand **Component Services**.

4 Expand **Computers**.

5 Expand **My Computer**.

6 Expand **Distributed Transactions**.

7 Right-click **Local DTC** and select **Properties**.

To do this:	Follow these steps:
Move MS DTC logs	On the Logging tab, in the Location field, specify the directory in which to store the MS DTC logs.
Expand the log capacity	On the Logging tab, in the Capacity field, increase the capacity to at least 64 MB. For production machines, or if you encounter problems at this level, increase the capacity to 100 MB or higher.

8 Click **OK**.

9 Restart the MS DTC service by issuing the following command in a Windows command window:

```
net start MSDTC
```

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 Technology Network** (http://www.oracle.com/technetwork/documentation/hsgbu-154445.html)—The most current documentation set, excluding the *Release Notes* and *Known Issues*.

If the software is available for download, the complete documentation set is available from the Oracle Software Delivery Cloud (https://edelivery.oracle.com).

All documents may not be updated for every CIS release. Therefore, the version numbers for the documents in a release may differ.

Documentation accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at 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. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

CIS 4.6.2 documentation

Item	Description	Part number	Last updated
Release Notes	The *Release Notes* document presents information about new features, enhancements, and updates for the current release.	E71106-01	4.6.2
Known Issues	The *Known Issues* document presents information about known issues for the current release.	E71107-01	4.6.2
Installation Guide	The *Installation Guide* provides procedures for installing, configuring, and upgrading the CIS Administration software. It also includes product interoperability considerations.	E71108-02	4.6.2
Secure Configuration Guide	The *Secure Configuration Guide* provides an overview of the security features provided with the Oracle® Health Sciences CIS application, including details about the general principles of application security, and how to install, configure, and use the CIS application securely.	E69249-02	4.6.2
Administrator Guide	The *Administrator Guide* explains how to use the CIS administration tool (CIS Administration) to manage adapters, load-balanced machines, CIS protocols, and synchronization connections. It includes troubleshooting, data transfer and storage information, and key database tables.	DC-CIS46-001-000	4.6 SP0
Designer Guide	The *Designer Guide* presents Integrated study design considerations.	DC-CIS46-002-000	4.6 SP0

Item	Description	Part number	Last updated
Online Help	The online Help includes field definitions, instructions for performing the tasks on each page of the CIS Administration user interface, and concepts and procedures for performing synchronization and general administrative tasks with the CIS Administration application.	DC-CIS46-003-000	4.6 SP0
Third Party Licenses and Notices	The *Third Party Licenses and Notices* document includes licenses and notices for third party technology that may be included with the CIS software.	E59144-01	4.6.1.4