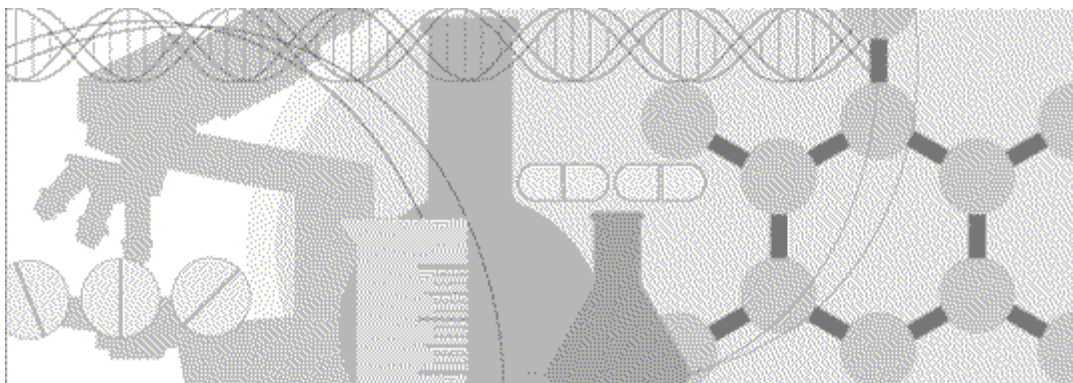


# CIS Installation Guide

Clintrial Integration Solution  
Release 4.6 SP1a



**ORACLE**

Copyright © 2002 - 2015, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

This documentation may include references to materials, offerings, or products that were previously offered by Phase Forward Inc. Certain materials, offerings, services, or products may no longer be offered or provided. Oracle and its affiliates cannot be held responsible for any such references should they appear in the text provided.

# Contents

<b>About this guide</b>	<b>v</b>
Overview of this guide.....	vi
Audience .....	vi
Related information.....	vii
CIS 4.6 SP1a documentation.....	vii
Training .....	viii
If you need assistance.....	ix
<b>Chapter 1 Overview of the Clintrial Integration Solution environment</b>	<b>1</b>
About the CIS environment .....	2
Overview of CIS architecture.....	3
Deployment scenarios and requirements .....	5
Study design configuration .....	6
Production configuration installed on separate computers .....	7
Production configuration for studies hosted by Phase Forward .....	8
Load-balancing configurations .....	9
CIS software load-balancing.....	10
<b>Chapter 2 Planning and prerequisites</b>	<b>11</b>
Overview of planning .....	12
Checklist—Prerequisites.....	13
Installing and configuring the Oracle database software.....	15
Updating the tnsnames.ora file .....	15
Setting initialization parameters .....	15
Creating tablespaces.....	17
Ensuring that LOGGING is enabled.....	17
Configuring registry settings for the Oracle client .....	20
Setting up Oracle XA transaction support on the Oracle server.....	20
Validating the database connection.....	21
Securing the CIS environment .....	22
Securing messages .....	22
Web policy for CIS and InForm Adapter software .....	22
Digital certificates.....	23
Setting up key certificates for SSL.....	24
Granting rights to the NETWORK SERVICE user for the private key.....	25
Setting the MTS timeout .....	26
<b>Chapter 3 Installing the CIS software</b>	<b>27</b>
Overview of the installation process .....	28
Canceling the installation process.....	28
Running the CIS 4.6 SP1a installation program.....	29
Selecting the installation process .....	29
Running the CIS installation for the first time.....	29
Running the CIS installation when upgrading from a previous version.....	46
Running the CIS installation for a load-balanced configuration or with existing database .....	47
<b>Chapter 4 After completing the CIS installation</b>	<b>63</b>
Securing the Service user name and password .....	64
Securing the predefined CIS user accounts.....	65

Updating the registry if CIS and the InForm software are installed on the same computer .....	66
Increasing the timeout period for ASP.NET.....	67
Changing database connection information .....	68
Changing the CIS database information .....	68
Changing the CIS administration database information .....	68
Managing certificates and applying full security.....	69
Using the Authentication Only option.....	69
Using the Authentication, Signing and Encryption option.....	72
Configuring CIS behind a Proxy server.....	74
Adding a service when there is more than one InForm Adapter service .....	75
Monitoring MS DTC logs .....	76

# About this guide

## In this preface

Overview of this guide.....	vi
Related information.....	vii
If you need assistance.....	ix

## Overview of this guide

This installation guide provides:

- An architectural and configuration overview of the CIS software and environment.
- A description of the prerequisites for installing the CIS software.
- Step-by-step instructions for installing, uninstalling, and upgrading the CIS software.

In addition to installing the CIS software described in this guide, you must install the InForm Adapter software. For more information, see the *InForm Adapter Installation Guide*.

## Audience

This guide is for:

- CIS administrators
- Database administrators
- System engineers

## Related information

### CIS 4.6 SP1a documentation

The CIS 4.6 SP1a documentation includes the documents in the following table. All documentation is available from the Phase Forward Download Center.

Item	Description	Part number
<i>Release Notes</i>	<ul style="list-style-type: none"> <li>New features, fixed issues, hardware and software requirements, and upgrade considerations.</li> </ul>	RN-CIS46-001-01a
<i>Known Issues</i>	<ul style="list-style-type: none"> <li>Known problems and workarounds (if available).</li> </ul> <p><b>Note:</b> The most current list of known issues is available on the Phase Forward Extranet.</p> <ul style="list-style-type: none"> <li>To sign in to the Extranet, go to <a href="http://www.phaseforward.com">www.phaseforward.com</a> and click <b>Customer Login</b>. Enter your email address and password, and navigate to the <b>Known Issues</b> section. Select a product, and then enter your search criteria.</li> </ul>	RN-CIS46-002-01a
<i>Administrator Guide</i>	<ul style="list-style-type: none"> <li>How to use the CIS administration tool (CIS Administration) to manage adapters, load-balanced machines, CIS protocols, and synchronization connections.</li> <li>Troubleshooting, data transfer and storage, and key database tables.</li> </ul> <p>This document is also available from the Documentation CD and the CIS Administration user interface.</p>	DC-CIS46-001-000
<i>Designer Guide</i>	<ul style="list-style-type: none"> <li>Integrated study design considerations.</li> </ul> <p>This document is also available from the Documentation CD.</p>	DC-CIS46-002-000
<i>Installation Guide</i>	<ul style="list-style-type: none"> <li>Product interoperability considerations.</li> <li>Procedures for installing, configuring, and upgrading the CIS Administration application.</li> </ul> <p>This document is also available from the Documentation CD.</p>	DC-CIS46-004-01a

Item	Description	Part number
Online Help	<ul style="list-style-type: none"> <li>• Field definitions.</li> <li>• How to perform the tasks that are available on each page of the CIS Administration user interface.</li> <li>• Concepts and procedures for performing synchronization and general administrative tasks with the CIS Administration software.</li> </ul> <p>This document is available from the CIS Administration user interface.</p>	DC-CIS46-003-000

---

## Training

In addition to the CIS training courses listed in the following table, the training courses for the following applications provide information about the software products used in a CIS environment:

- Clintrial software
- InForm software
- Central Designer software

For information about the following training offerings for CIS, contact Phase Forward.

Title	Description	Format
Clintrial Integration Solution Training	Teaches clinical study specialists to create and manage integrated and hybrid studies using CIS, the Clintrial software, and the InForm software.	Instructor-led training.
Hosting CIS Integrated Studies	Teaches database, network, and web professionals to set up and manage integrated studies, as well as perform general troubleshooting.	Instructor-led training.

---



## If you need assistance

If you are a Phase Forward customer with a maintenance agreement, you can contact the Global Support Center for assistance with product issues.

Your maintenance agreement indicates the type of support you are eligible to receive and describes how to contact Phase Forward. Additionally, the Phase Forward website lists the toll-free support number for your product, location, and support level:

<http://www.phaseforward.com/support>

In the event that our toll-free telephone service is interrupted, please use either of the following methods to contact the Global Support Center:

- Email  
customer.support@phaseforward.com
- Telephone

In the US: 781-902-4900

Outside the US: +44 (0) 1628 640794

Phase Forward also provides assistance with User Management, Site Assessment, and Provisioning. Please refer to your Master Services Agreement and individual Statement of Work to determine if you are eligible to use these services.



## CHAPTER 1

# Overview of the Clintrial Integration Solution environment

### In this chapter

About the CIS environment.....	2
Overview of CIS architecture .....	3
Deployment scenarios and requirements.....	5
Load-balancing configurations .....	9

## 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:

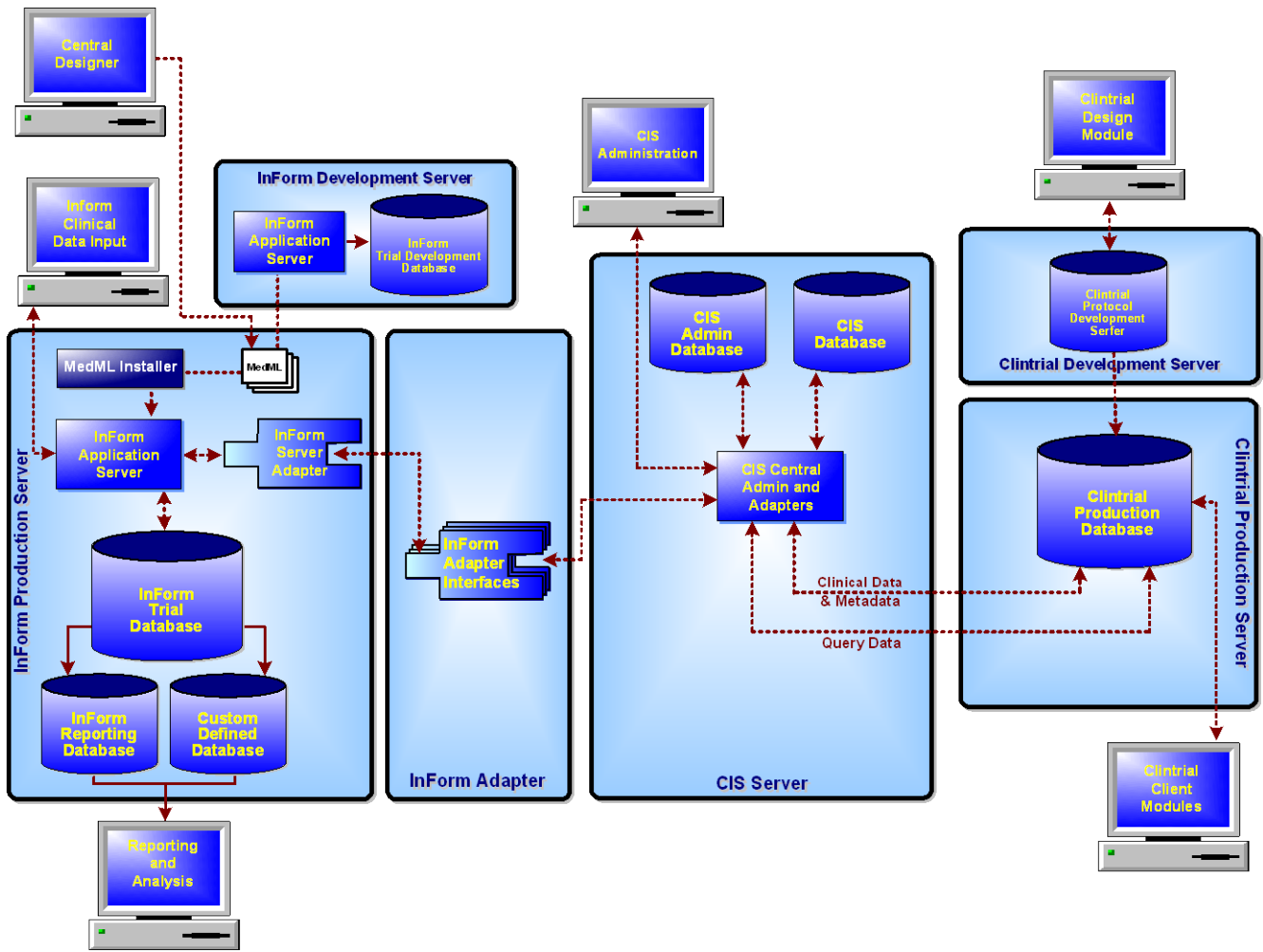
- Transfers and translates study metadata.
- Transfers clinical data.
- Transfers data validation information.

## Overview of CIS architecture

The CIS architecture consists of the following components:

Purpose	InForm software	CIS	Clintrial software	InForm Adapter
Study design and implementation	<ul style="list-style-type: none"> <li>The Central Designer software.</li> </ul>	n/a	Clintrial Design module	n/a
Run-time data entry and data management	<ul style="list-style-type: none"> <li>The InForm software.</li> <li>InForm Reporting and Analysis.</li> </ul>	n/a	Clintrial client modules: Classify, Enter, Lab Loader, Manage, Multisite Distribution, Resolve	n/a
Database management (Oracle databases)	<ul style="list-style-type: none"> <li>InForm study database (development and production).</li> <li>InForm reporting database.</li> <li>Customer-defined database.</li> </ul>	<ul style="list-style-type: none"> <li>CIS Admin database</li> <li>CIS database</li> </ul>	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.	<b><i>Study design configuration</i></b> (on page 6).
A production configuration in which the InForm software, the CIS software, and the Clintrial software are installed on separate computers.	<b><i>Production configuration installed on separate computers</i></b> (on page 7).
A production configuration in which Phase Forward hosts the study.	<b><i>Production configuration for studies hosted by Phase Forward</i></b> (on page 8).

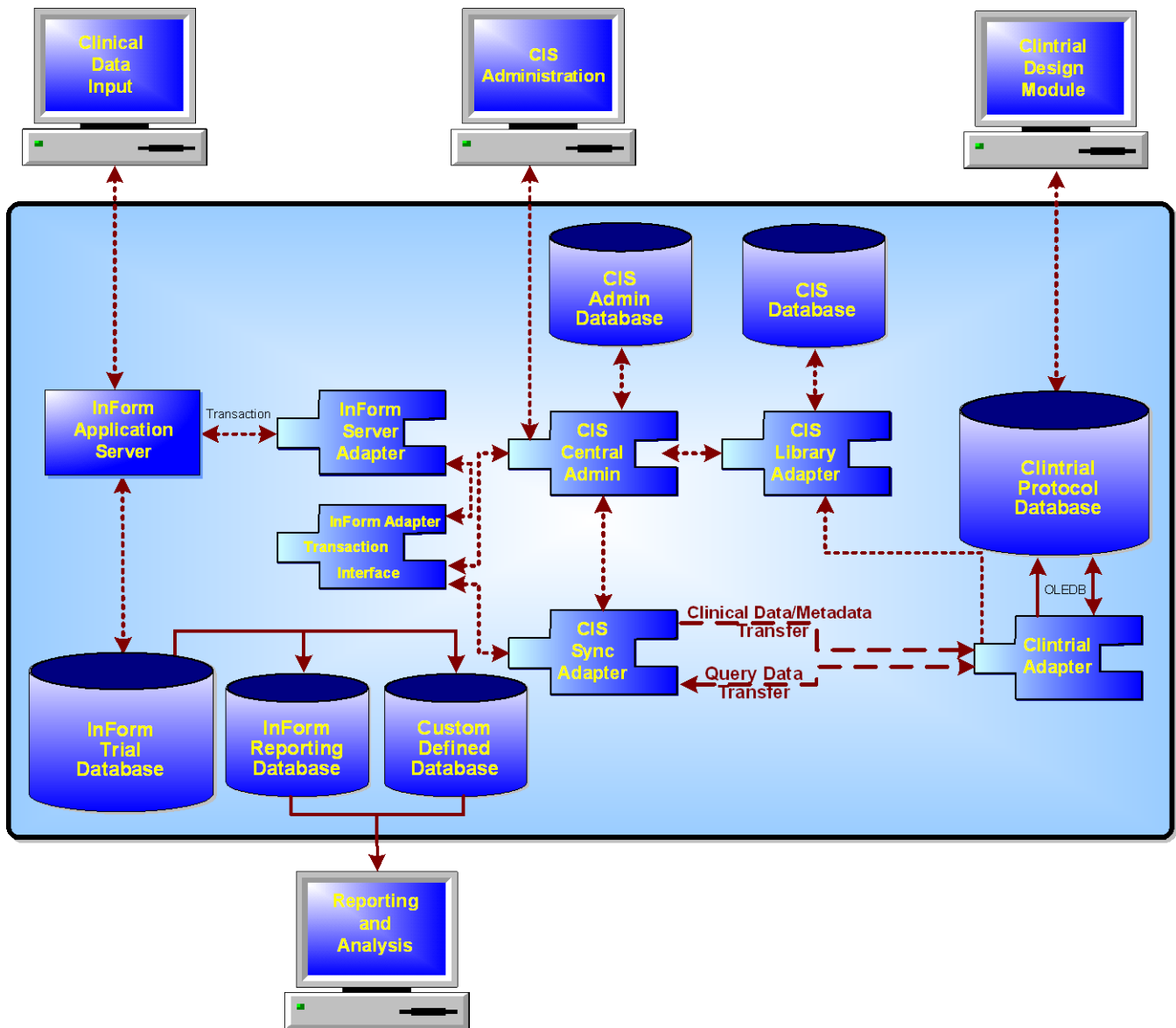
In addition, if your studies are large, consider employing a load-balancing strategy to distribute the processing load over multiple servers. Your load-balancing solution could be used in any deployment scenario. For more information, see ***Load balancing configurations*** (on page 9).

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 4.6 SP1a *Release Notes*.

## Study design configuration

In a design environment, you can install all the required software on one computer. A design environment does not impose the same guidelines as a test or production environment. In the following configuration, all of the components are installed on a single computer. If all the components are on one server, the InForm and Clintrial database instances must use the same Oracle software version.

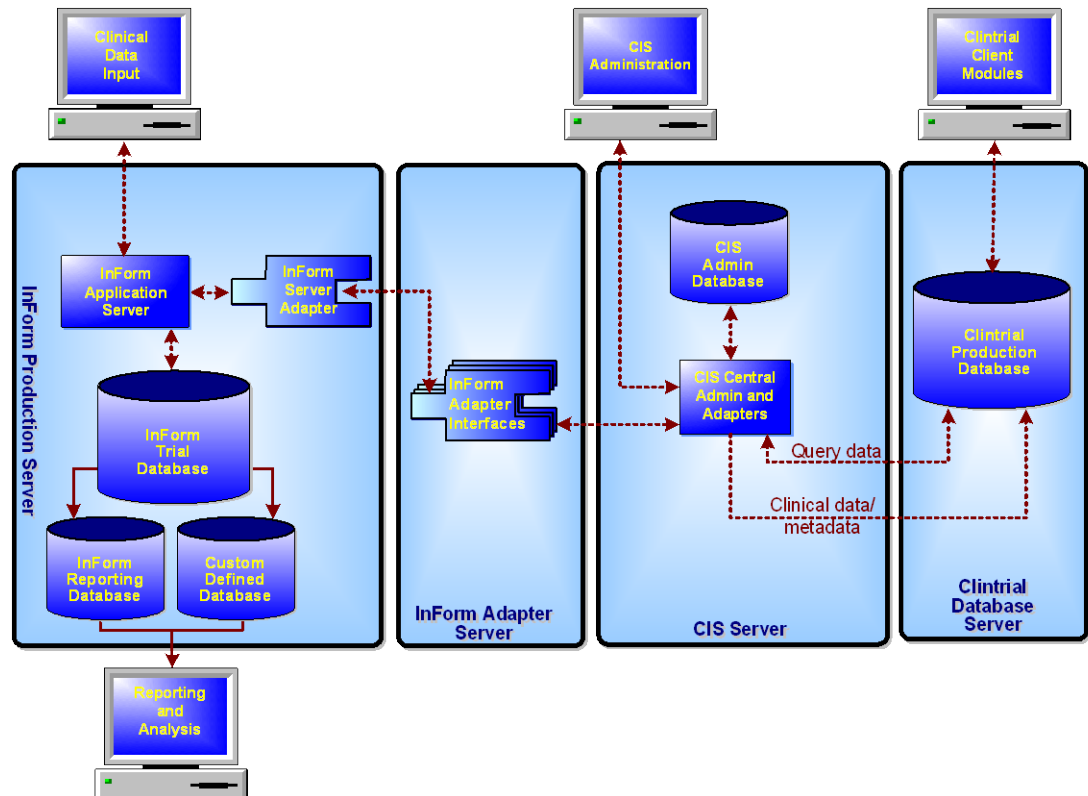
**Note:** Installing all components on a single computer is supported only for the InForm 5.0 software.





## Production configuration installed on separate computers

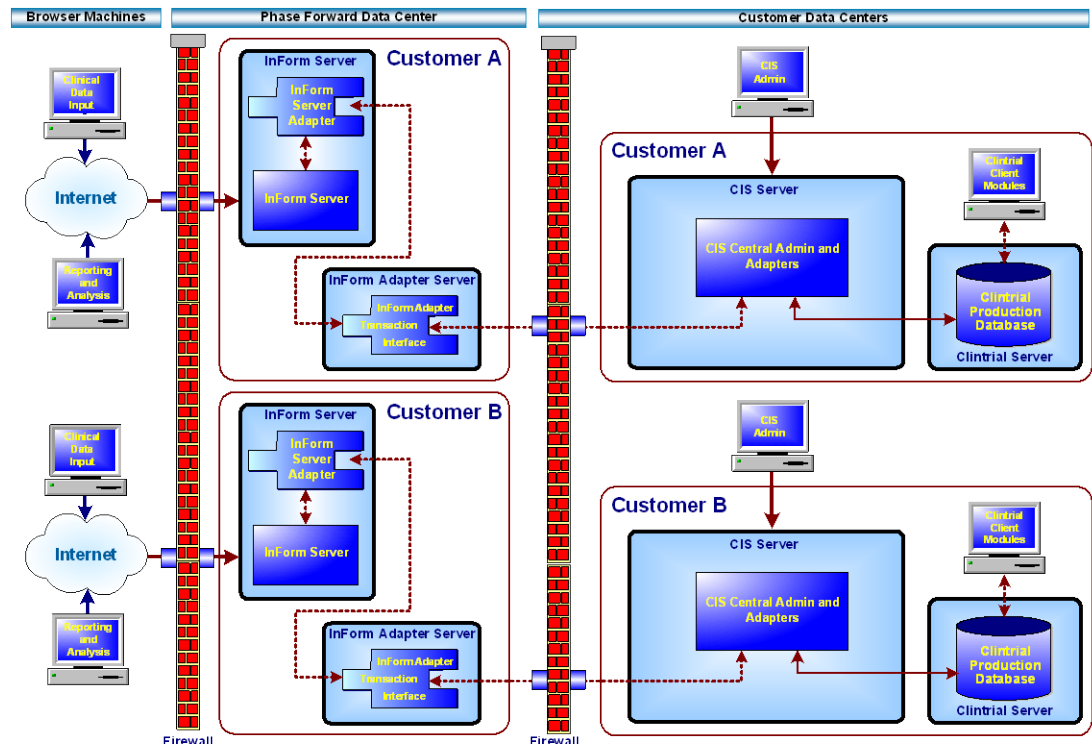
In a test and production environment, you can install the InForm components, the CIS components, and the Clintrial database on separate computers. This configuration is typically used by customers who host the InForm study.



## Production configuration for studies hosted by Phase Forward

In a production environment in which Phase Forward 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.



## 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.

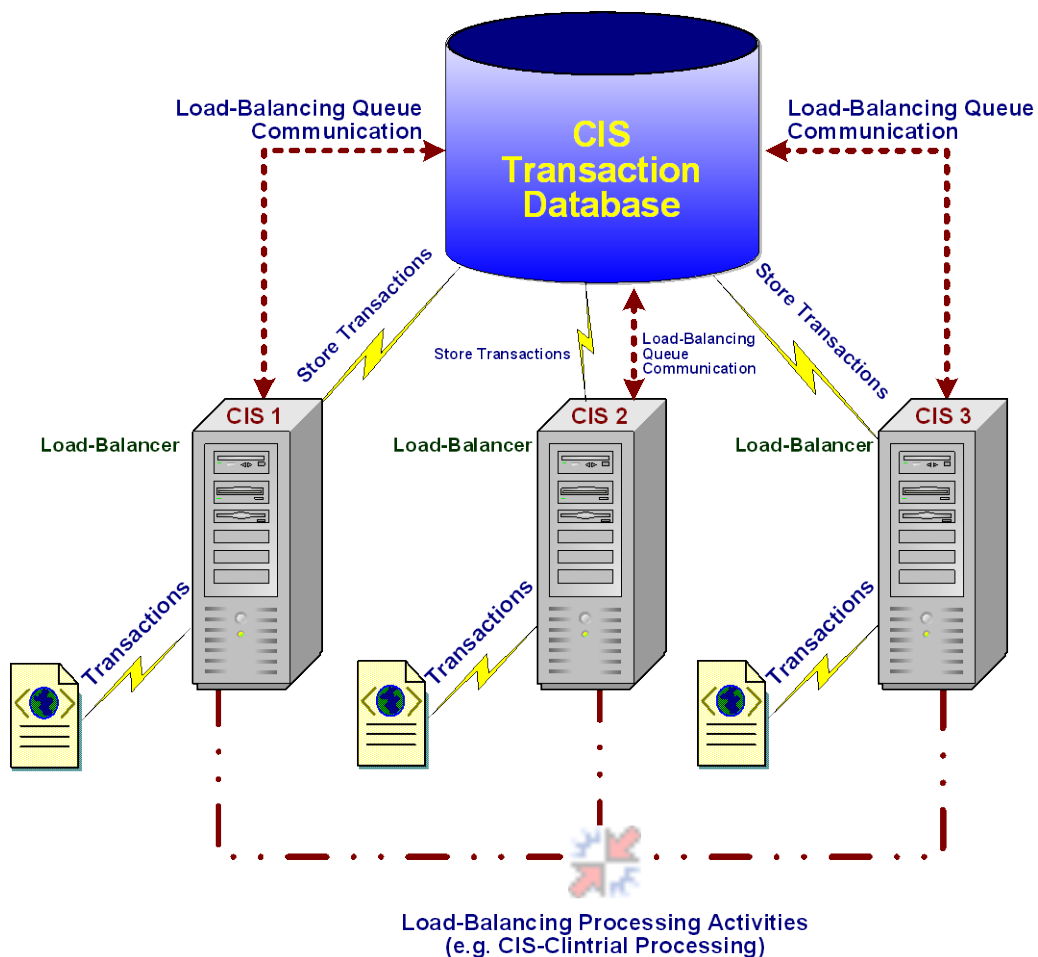
If the CIS components are installed on a single server, the CIS software performs all load-balancing actions but distributes data only to the single server.

## 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. In this illustration, the InForm Adapter, the software component with which the CIS software communicates directly, handles all requests from all computers.



## CHAPTER 2

# Planning and prerequisites

### In this chapter

Overview of planning.....	12
Checklist—Prerequisites.....	13
Installing and configuring the Oracle database software.....	15
Securing the CIS environment.....	22
Setting the MTS timeout.....	26

## 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
<b>Set up Windows 2003 server.</b>	
☐ 1 Set up a new Windows 2003 server on which to install the CIS 4.6 SP1a software. Release 4.6 does not support the Windows 2000 operating system	Microsoft Windows documentation.
<b>Install and configure Oracle software.</b>	
☐ 2 Install and configure the Oracle software on the Clintrial, InForm, and CIS computers.	<ul style="list-style-type: none"> <li>• Oracle documentation.</li> <li>• CIS <i>Release Notes</i> for:               <ul style="list-style-type: none"> <li>▪ Minimum Oracle database patches required for the CIS database.</li> <li>▪ Minimum Oracle software components required for the CIS Oracle client.</li> </ul> </li> <li>• <i>Installing and configuring Oracle database software</i> (on page 15).</li> </ul>
<b>Set up security.</b>	
☐ 3 Purchase and install an X.509 certificate.  <b>Note:</b> Allow ample time to complete this step.	<ul style="list-style-type: none"> <li>• <i>Digital certificates</i> (on page 23).</li> <li>• <i>Configuring X.509 digital certificates</i> (on page 36).</li> </ul>
☐ 4 Decide whether or not to enable SSL: <ul style="list-style-type: none"> <li>▪ For communications between the CIS software and the InForm Adapter software.</li> <li>▪ For internal communications among the components of the CIS software.</li> </ul>	<i>Securing messages</i> (on page 22).
☐ 5 Decide on a type of web service security.	<i>Securing messages</i> (on page 22).
☐ 6 Choose a company URL. The company URL must be the same for the CIS software and the InForm Adapter software and cannot be changed after installation.	<i>Specifying a company URL</i> (on page 45).

☑	Workflow step	Where to get more information
<b>Install the Clintrial, InForm, and InForm Adapter software.</b>		
☐	7 Install the Clintrial software.	<i>Clintrial Getting Started.</i>
☐	8 Install the InForm software.	For the InForm 4.6 software: <i>InForm Installation and Configuration.</i>  For the InForm 5.0 software: <i>InForm Installation Guide</i>
☐	9 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.	<i>InForm Adapter Installation Guide.</i>
☐	10 Make sure that the InForm Adapter generates transaction XML. Perform this step well before installing the CIS software.	<i>InForm Adapter Installation Guide.</i>
<b>Set the MTS timeout.</b>		
☐	11 Set the MTS timeout to control the timeout period for the Microsoft Transaction server.	<b><i>Setting the MTS timeout</i></b> (on page 26).



# Installing and configuring the Oracle database software

Before installing the Clintrial, InForm, or CIS software, install and configure the Oracle software on each computer 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 the InForm 4.6 software, see the *InForm Installation and Configuration Guide*.
- For the InForm 5.0 software, see the *InForm Installation Guide*.

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

If you are upgrading the CIS software from CIS 4.5 SP1, 4.5 SP1a, or 4.5 SP1b to CIS 4.6 SP1a, see the *CIS Release Notes*.

**Note:** The CIS 4.6 SP1a 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 different alias on each CIS computer.

## Setting initialization parameters

Because the CIS application generates short-term heavy loads on the Clintrial Oracle instance to which it attaches, the following initialization parameters in the Init.ora file are recommended when creating the Clintrial Oracle instance.

The following table lists recommended Oracle parameter settings. For descriptions, see the Oracle documentation.

By default, Oracle 10g turns on Automatic Memory Tuning during installation.

**Note:** Phase Forward recommends that you use Automatic Memory Tuning.

## Required parameters: Automatic Memory Tuning 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 dedicated server.

## Required parameters: Automatic Memory Tuning 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, follow the instructions in *Updating LOB storage to set the option to LOGGING* (on page 18).

## 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. Use the Windows Add/Remove Programs utility.
- 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 27).

## Updating LOB storage to set the option to LOGGING

If you have installed the CIS software and created tablespaces with the Oracle LOB storage option set to NOLOGGING and you want to keep the data that you have already synchronized 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.

The following table shows CIS database tables and columns that were created for the user **CISALL**.

Table	Column	Data type
CIS_DEFAULT_PROPERTIES	CONFIGXML	CLOB
CIS_LAST_TRANSACTIONS	TRANSACTIONXML	CLOB
CIS_LIB_MACHINES	OFFLINEREASONEXCEPTION MSG	CLOB
CIS_MAILQUEUE	BODY	CLOB
CIS_SYNCHCONNECTIONS	SYNCHCONFIG	CLOB
CIS_SYNCH_ERRORS	SOAPEXCEPTION	CLOB
CIS_SYNCH_ERRORS	STACKTRACE	CLOB
PM_AUDIT_EVENT	DATA	CLOB
PM_AUDIT_REPORT_CHANGE	OLD_CLOB_VALUE	CLOB
PM_AUDIT_REPORT_CHANGE	NEW_CLOB_VALUE	CLOB
PM_EVENTNOTIFICATIONS	NOTIFICATION_DATA	CLOB
PM_EVENTSUBSCRIPTIONS	SUBSCRIPTION_DATA	CLOB
PM_IDENTITY_PROFILE_CUST	BINARY_VALUE	BLOB
PM_IDENTITY_PROFILE_CUST_ AUDIT	BINARY_VALUE	BLOB
PM_IDENTITY_PROFILE__STD	IMAGE	BLOB
PM_IDENTITY_PROFILE_STD_AUDIT	IMAGE	BLOB

Table	Column	Data type
PM_JOB	JOBDATA	CLOB
PM_JOB_LOB	JOBERROR	CLOB
PM_SESSION	SESSION_DATA	BLOB
PM_SYSTEMSETTINGS	PROPERTY_CLOB_VALUE	CLOB
PM_SYSTEMSETTINGS_AUDIT	PROPERTY_CLOB_VALUE	CLOB
PM_USERSETTINGS	PROPERTY_CLOB_VALUE	CLOB

The following table shows CIS database tables and columns that were created for the user **CAUSER**.

Table	Column	Data type
CA_LANGUAGERESOURCETEXT	TEXT	BLOB
CA_MENUDATA	XML	BLOB
CA_PAGEREFERENCEDATA	XML	BLOB
CA_PLUGIN	PAGESTRUCTUREXML	BLOB
CA_PLUGINFILE	FILEBINARY	BLOB
CA_SERVERPLUGIN	ERRORDETAILS	BLOB
PM_AUDIT_EVENT	DATA	CLOB
PM_AUDIT_REPORT_CHANGE	OLD_CLOB_VALUE	CLOB
PM_AUDIT_REPORT_CHANGE	NEW_CLOB_VALUE	CLOB
PM_IDENTITY_PROFILE_CUST	BINARY_VALUE	BLOB
PM_IDENTITY_PROFILE_CUST_AUDIT	BINARY_VALUE	BLOB
PM_IDENTITY_PROFILE__STD	IMAGE	BLOB
PM_IDENTITY_PROFILE_STD_AUDIT	IMAGE	BLOB
PM_JOB	JOBDATA	CLOB
PM_JOB_LOB	JOBERROR	CLOB
PM_SESSION	SESSION_DATA	BLOB
PM_SYSTEMSETTINGS	PROPERTY_CLOB_VALUE	CLOB
PM_SYSTEMSETTINGS_AUDIT	PROPERTY_CLOB_VALUE	CLOB
PM_USERSETTINGS	PROPERTY_CLOB_VALUE	CLOB

## 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/Microsoft/MSDTC

Key	Name	Data value
MtxOCI (for Oracle 10g)	OracleOciLib	oci.dll
	OracleSqlLib	orasql10.dll
	OracleXaLib	oraclient10.dll
XADLL (For Windows 2003)	mtxoci.dll	Path to the mtxoci.dll file (the [SystemFolder])
SECURITY (For Windows 2003)	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, and 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

## Securing messages

If you are using X.509 digital certificates, during the installation of the CIS software you choose either **Authentication Only** or **Authentication, Signing and Encryption** to secure messages to web services .

- **Authentication Only**—Authenticates users but does not encrypt web service messages.

You can select **Authentication Only** at the following times:

- **When installing the CIS software**—This selection governs communication among the internal components of the CIS software. If you select **Authentication Only** for CIS communications, you must select it for all CIS computers in a group of load-balanced computers.
- **When configuring InForm Adapter interfaces**—This selection governs communication between the CIS software and the InForm Adapter software. The SSL setting for each InForm Adapter that you register with the CIS software is independent. If Phase Forward hosts the InForm Adapter software, SSL is mandatory.

**Notes:** Registering the individual InForm Adapters with the CIS software is covered in the *CIS Administrator Guide*.

Configuring the SSL setting for each InForm Adapter interface is covered in the *InForm Adapter Installation Guide*.

- **Authentication, Signing and Encryption**—Encrypts and signs messages, providing additional security by verifying that the requester has the CIS private key. The certificate must be installed on the computer running the CIS software and each computer running an instance of InForm Adapter that will be registered with the CIS software.

For more information, see *Managing certificates and applying security* (on page 69).

## Web policy for CIS and InForm Adapter software

Define the web service policy for the CIS software and the InForm Adapter software as follows:

If the CIS software uses	The InForm Adapter software must use
<b>Authentication Only.</b>	<b>TokenOnlyPolicy</b> for the service interfaces used by the CIS software.
<b>Authentication, Signing and Encryption.</b>	<b>FullPolicy</b> for the service interfaces used by the CIS software.



For more information, see:

- *Applying one X.509 digital certificate* (on page 72).
- *Applying a different X.509 digital certificate to different services* (on page 72).

**Note:** When you apply full security using one certificate, the certificate you use must have both a private and public key. When you apply full security using two certificates, the certificate you install on the InForm Adapter server must have a private key.

**Note:** Phase Forward only accepts X.509 digital certificates from a recognized Certificate Authority for communications between the InForm Adapter and CIS software. Phase Forward does not accept customer-created certificates.

## Digital certificates

The CIS software and the InForm Adapter software use X.509 digital certificates to secure messages between the web services in your product environment. During the installation or during the post-installation configuration for the CIS software and the InForm Adapter software, you use the Certificate Configuration utility to select the:

- X.509 certificate to apply.
- Servers on which to apply the certificate.
- Template with which to configure the digital certificate.

For more information, see:

- *Configuring X.509 digital certificates for Authentication Only* (on page 36).
- *Configuring X.509 digital certificates for Authentication, Signing and Encryption* (on page 40).
- *Managing certificates and applying full security* (on page 69).

**Note:** Before you install the CIS software, obtain the X.509 digital certificates you want to use from a third-party vendor, and install the certificates in a directory that you can access during the installation. After you install the CIS software, you can add or change X.509 digital certificate.

Phase Forward 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 SSL

To enable SSL, set up a key certificate on each server where the CIS software is installed.

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

### Creating a key certificate

- 1 On the server where the CIS software is installed, open the **Internet Information Services (IIS) Manager**.
- 2 Expand the Machine Name node, and then expand the Websites node.
- 3 Right-click **Default Web Site**, and select **Properties**.
- 4 Select the **Directory Security** tab.
- 5 Click **Server Certificate**.  
The IIS X.509 Certificate Wizard starts.
- 6 Click **Create new certificate**.
- 7 Type the certificate information. In the **Common name** field, specify the name of the study server.
- 8 Save the certificate request in a file that you will send to the certificate authority.
- 9 Process the certificate request by using a Certificate Authority.
- 10 Save the certificate in a file.

### Installing the certificate

- 1 On the server where the CIS software is installed, open the **Internet Information Services (IIS) Manager**.
- 2 Right-click **Default Web Site** and select **Properties**.
- 3 Click the **Directory Services** tab.
- 4 Click **Server Certificate**.  
The IIS X.509 Certificate Wizard starts.
- 5 Click **Process the pending request**.
- 6 Browse to the saved certificate.
- 7 Stop **IIS** and start it again.  
The SSL is now installed.

### 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.

## 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 Install the WSE 2.0 X.509 certificate tool with the administrator option.
- 2 To open the tool, select **Start > All Programs > WSE 2.0 > X509 Certificate Tool**.
- 3 Set the Certificate Location to **Local Computer**.
- 4 Set the Store Name to **Personal**.
- 5 Click **Open Certificate**.
- 6 Select your certificate, then click **OK**.
- 7 Click **View Private Key File Properties**.
- 8 Select the **Security** tab.
- 9 Click **Locations**.
- 10 In the Locations dialog box, change to the local computer and then click **OK**.
- 11 In the Select Users or Groups box, type **network service** and then click **Check Names**.  
The tool displays NETWORK SERVICE.
- 12 Make sure that the **Read and Execute** check box and the **Read** check box are selected.
- 13 Click **OK** to close the dialog box.
- 14 Continue to click **OK** on subsequent dialog boxes until the tool is closed.

## Setting the MTS timeout

Phase Forward 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, type **300**.
- 7 Click **OK**.

## CHAPTER 3

# Installing the CIS software

### In this chapter

Overview of the installation process.....	28
Running the CIS 4.6 SP1a installation program.....	29

## Overview of the installation process

This section describes how to install the CIS software on one or more CIS servers. During the installation, you must:

- Provide required information for each database user.
- Select network settings.
- Configure at least one X.509 digital certificate for the CIS software. Configure the private keys of the certificates to be accessible by the ASP.NET account.

In addition to installing the CIS software and configuring digital certificates for 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 a minimum of 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 SP1a installation program

## Selecting the installation process

Select the appropriate process.

Purpose of this installation	For more information, see
<p>You are upgrading from any of the following releases:</p> <ul style="list-style-type: none"> <li>The CIS 4.5 SP1, 4.5 SP 1a, 4.5 SP1b, or subsequent releases of CIS 4.5 SP1.</li> <li>The CIS 4.6 SP0 or 4.6 SP1 software release.</li> </ul> <p><b>Note:</b> Before you install the CIS 4.6 SP1a software, you must have already completed the upgrade instructions in the CIS <i>Release Notes</i>.</p>	<p>The CIS 4.6 SP1 <i>Release Notes</i>.</p> <p><b><i>Running the CIS installation when upgrading from a previous version</i></b> (on page 46).</p>
<p>You are creating a new CIS 4.6 SP1a installation.</p>	<p><b><i>Running the CIS installation for the first time</i></b> (on page 29).</p>
<p>You are adding a CIS 4.6 load-balanced server. CIS 4.6 is already installed on another server, and you want the server you are currently installing to share a database with the existing server.</p>	<p><b><i>Running the CIS installation for a load-balanced configuration</i></b> (on page 47).</p>

## Running the CIS installation for the first time

### Starting the installation

- 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, Phase Forward can use these log files to diagnose the problem.

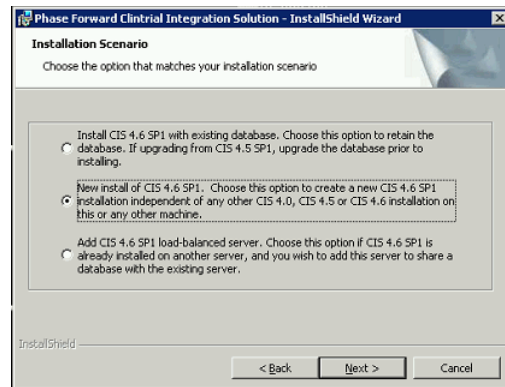
**Note:** After you complete the installation and use the log files to diagnose problems if necessary, delete the log files, because they can contain unencrypted information such as passwords.

- 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.

- Click **Next**.

The Installation Scenario page appears.



- 3 Select **New install of CIS 4.6 SP1** and then click **Next**.

The License Agreement page appears.

## Accepting the CIS licensing agreement

- To continue with the installation, select **I accept the terms in the license agreement** and then click **Next**.

**Note:** To print a copy of the license agreement, click the **Print** button.

The Customer Information page appears.

## Providing customer information

- 1 Type the following information in the specified fields:
  - **User Name**—User that is installing the CIS software.
  - **Organization**—Organization that is installing the CIS software.
  - Choose whether to require that users sign in to CIS in order to run the installation.
- 2 Click **Next**.

The Setup Type page appears.

## Choosing the setup type

The setup type determines whether the CIS software is installed in the default location.

- **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.



- 1 Select either Typical or Custom setup type.

Select an option	Then do this
Typical	<ul style="list-style-type: none"> <li>• Click <b>Next</b>.</li> </ul>
Custom	<ol style="list-style-type: none"> <li>1 Click <b>Next</b>. The Custom Setup page appears.</li> <li>2 To see how much space you need to install the CIS software, click <b>Space</b>.</li> <li>3 To change the directory in which to install the software, click <b>Change</b>. The Change Current Destination Folder appears.</li> <li>4 Navigate to the destination folder, then click <b>OK</b>.</li> </ol>

The CIS Administration Database Setup page appears.

## Setting up the CIS administration database for the first time

The screenshot shows a window titled "Phase Forward Clintrial Integration Solution - InstallShield Wizard". The main heading is "CIS Administration Database Setup". Below the heading is a note: "Please fill in the database information for the CIS Administration feature. Read the Admin Guide before choosing these settings." The form contains the following fields and controls:

- CIS Administration Database Instance Name:** A text box containing "rdcis012\_dev1".
- CIS Administration Database User:** A section containing:
  - Username:** A text box containing "cisadminuser".
  - Password:** A text box containing "\*\*\*\*\*".
  - Create Oracle User and Schema**

At the bottom of the dialog box are three buttons: "< Back", "Next >" (which is highlighted), and "Cancel".

- 1 Type 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.

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

- 2 Click **Next**.

The CIS Administration Database Account Creation page appears.

- 3 Type the following information:

- **Oracle System Username**—Name of an Oracle System user for an existing account. The default user name is **system**.
- **Oracle System Password**—Password for the Oracle System user. The default Password is **oracle**.

**Note:** If the user name and password you typed on the previous screen (in Step 1) already exist, a message appears and indicates that the installation will drop (destroy all existing data for that user) and re-create the Administration database user.

- **Default tablespace**—The name of the default tablespace reserved for the Oracle system user.
- **Temporary tablespace**—The name of the temporary tablespace reserved for the Oracle system user during installation.

- 4 Click **Next**.

The CIS Database Setup page appears.

## Setting up the CIS database for the first time

- 1 Type 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**—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 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 Type the following information:
  - **Oracle System User**—Name of an Oracle system user for an existing account. The default user name is System.

- **Oracle System Password**—Password for the Oracle system user. The default password is oracle.

**Note:** If the user name and password you typed on the previous screen (in Step 1) already exist, a message appears and indicates that the installation will drop (destroy all existing data for that user) and re-create the CIS Database user.

- **Default tablespace**—The name of the default tablespace reserved for the CIS database.
- **Temporary tablespace**—The name of the temporary tablespace reserved for CIS database during installation.

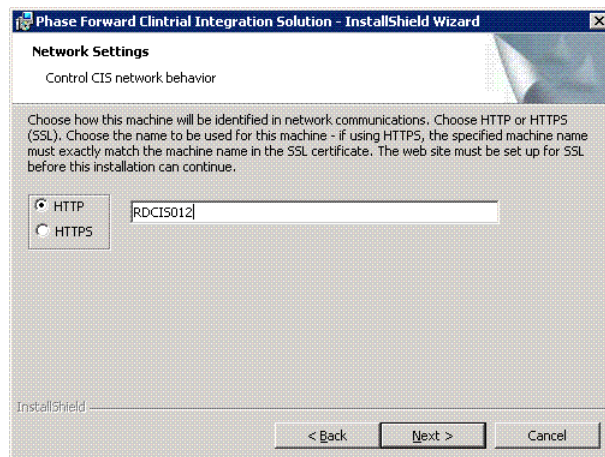
- 4 Click **Next**.

The Network Settings page appears.

## Choosing HTTP or HTTPS for network settings

After the CIS database has been created, you must choose whether to use HTTP or HTTPS to secure internal CIS communications.

**Note:** This setting does not affect communications between the CIS software and the InForm Adapter software.



The following fields for network communications within CIS are available:

- **HTTP**—The web service on the computer where the CIS software is installed is addressed using the HTTP protocol.
- **HTTPS**—The web service on the computer where the CIS software is installed is addressed using the HTTPS protocol. If you select this option:
  - HTTPS must be used when you use **https://machinename/CentralAdmin** to log on to the CIS Administration application.
  - HTTPS is used for all web service calls to the various components of the CIS software.
  - When you register the InForm Adapter software, you can select a different network communications option.
  - If you select HTTPS for one computer in a set of load-balanced CIS computers, you

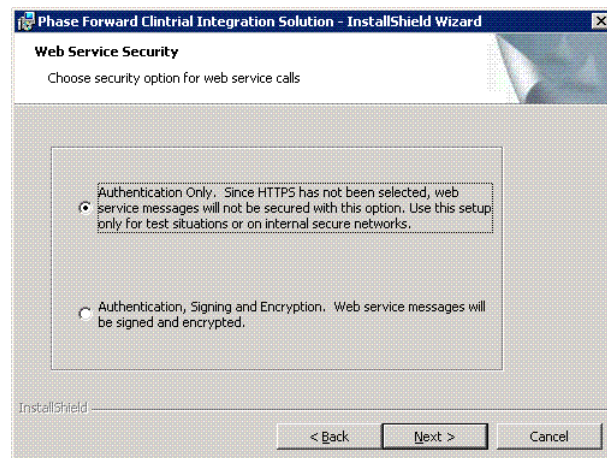
**must** select HTTPS for all computers that are used for CIS load-balancing.

**Note: The protocol must match the protocol that was chosen when installing on the first CIS server.**

- **Machine name text box**—Initially displays the simple computer name of the server. However, if you select HTTPS, you must type the computer name **exactly** as it is encoded in the SSL certificate for that computer.
- 1 Select either HTTP or HTTPS.
  - 2 Click **Next**.

The Web Service Security page appears.

## Choosing web service security



The following options for web service calls are available:

- **Authentication Only**—Web service calls are authenticated. Web service calls within CIS are encrypted using SSL if HTTPS was chosen on the previous screen.
  - **Authentication, Signing and Encryption**—All web service calls are authenticated, signed, and encrypted, and messages within CIS are encrypted again using SSL.
- 1 Select either Authentication only or Authentication, Signing and Encryption.
  - 2 Click **Next**.

The Choose Certificate page appears.

**Note: After you install the CIS software, you can change the method that you chose during the installation.**

## Configuring X.509 digital certificates

Select the procedure that matches your choice of web service security:

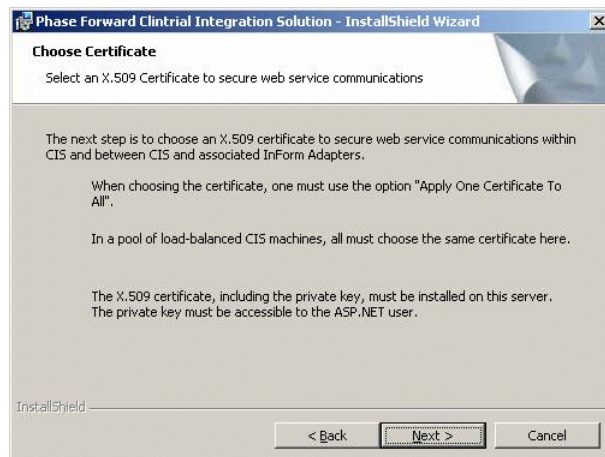
- *Configuring X.509 digital certificates for Authentication Only* (on page 36).
- *Configuring X.509 digital certificates for Authentication, Signing and Encryption* (on page 40).

### Configuring X.509 digital certificates for Authentication Only

Digital certificates are used to secure communications within your CIS environment, and between the CIS software and the InForm Adapter software. You must configure these certificates for your product and the InForm Adapter software.

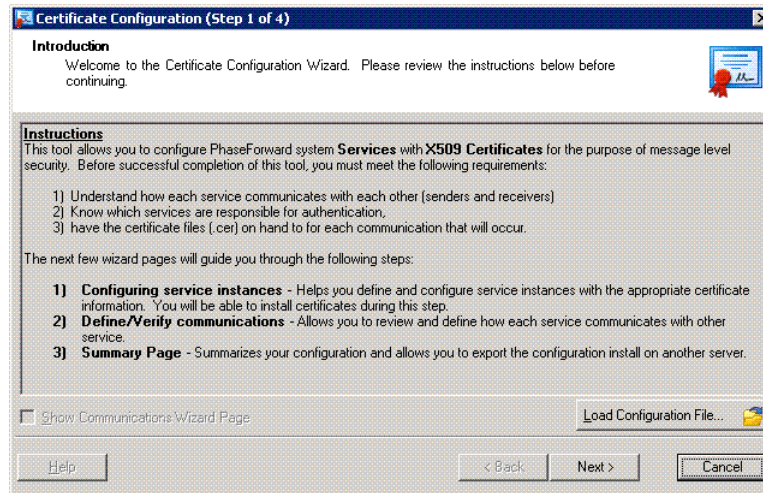
**Note:** If you have a pool of load-balanced CIS computers, you must apply the same X.509 certificate to all computers. The X.509 certificate, including the private key, must be installed on all load-balanced computers.

To configure digital certificates:



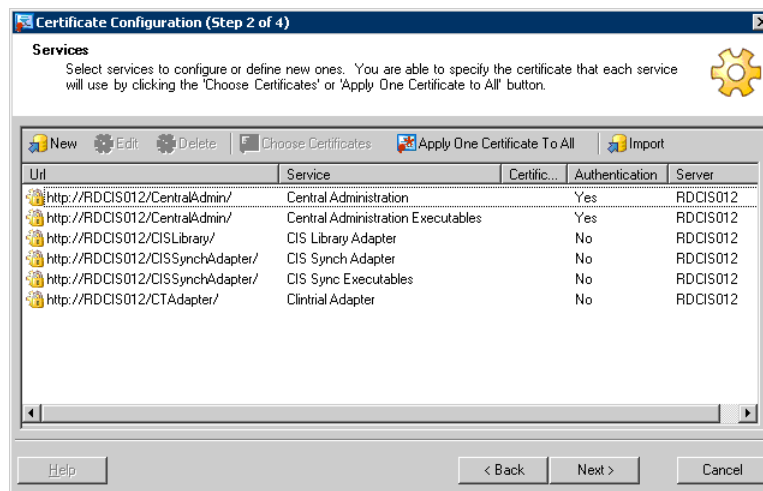
- 1 On the Choose Certificate page, click **Next**.

The Certificate Configuration Introduction page appears.



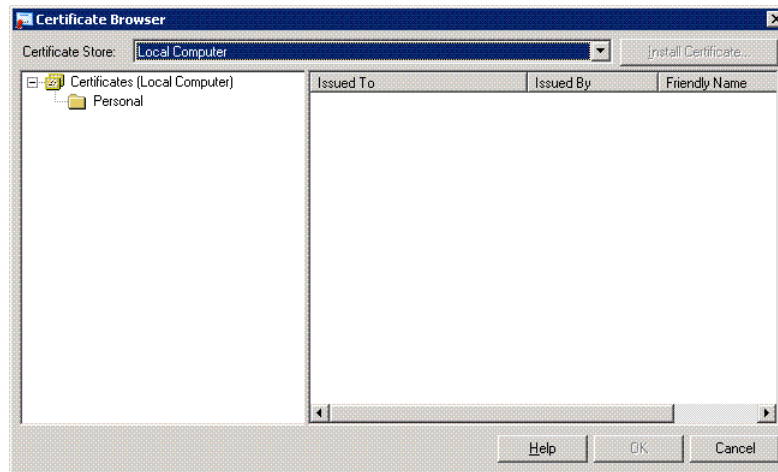
- 2 Click **Next**.

The Services page appears. Note that the Certificate column is empty.

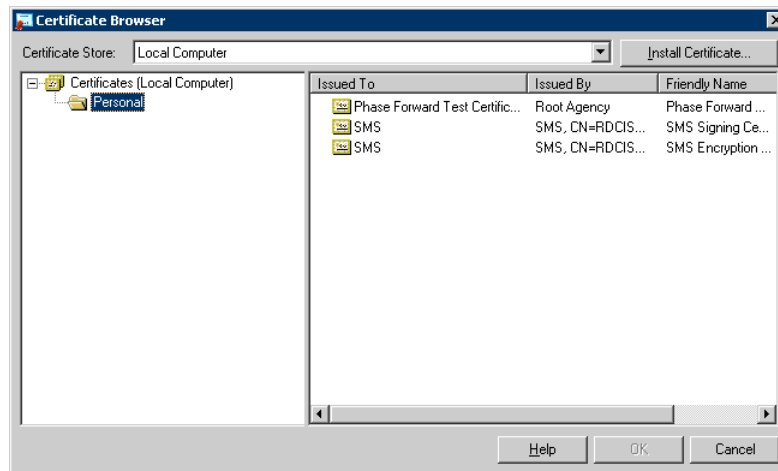


- 3 Click **Apply One Certificate To All**.

The Certificate Browser page appears.



- 4 In the **Personal** folder, select the X.509 certificate that will be used to secure communications in this CIS installation.

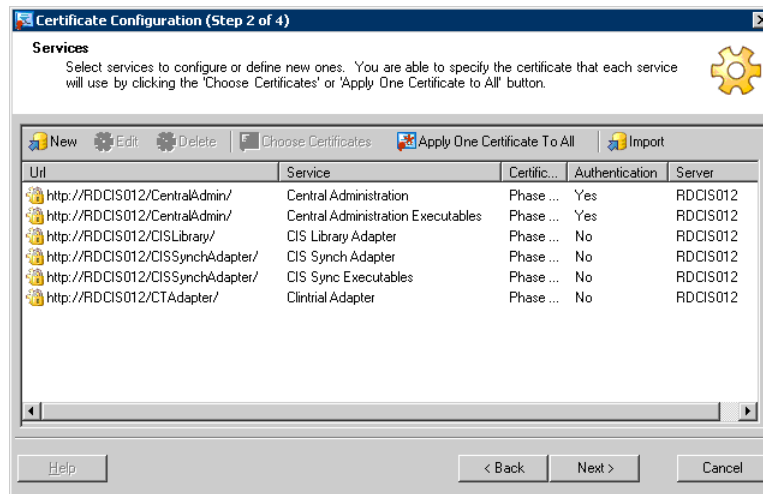


**Note:** From this page, you can also install an X.509 certificate. For more information, see *Installing and applying a new certificate* (on page 70).

- 5 Click **OK**.

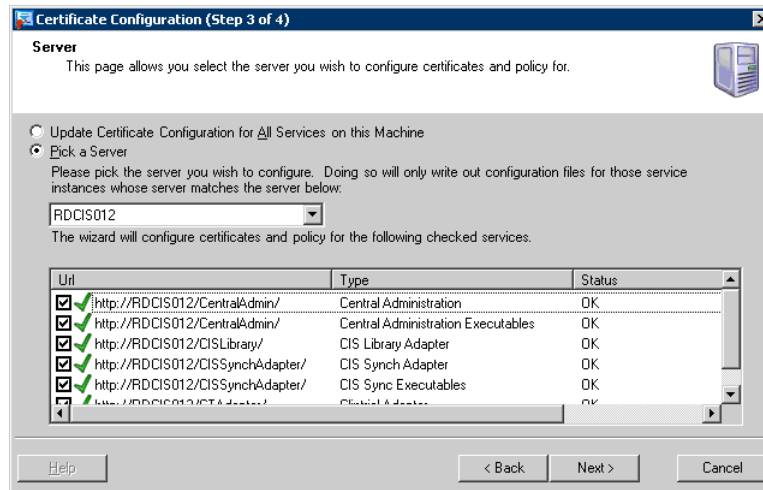


The Services page appears. Note that the selected X.509 certificate now appears, and that the Certificate column is populated.



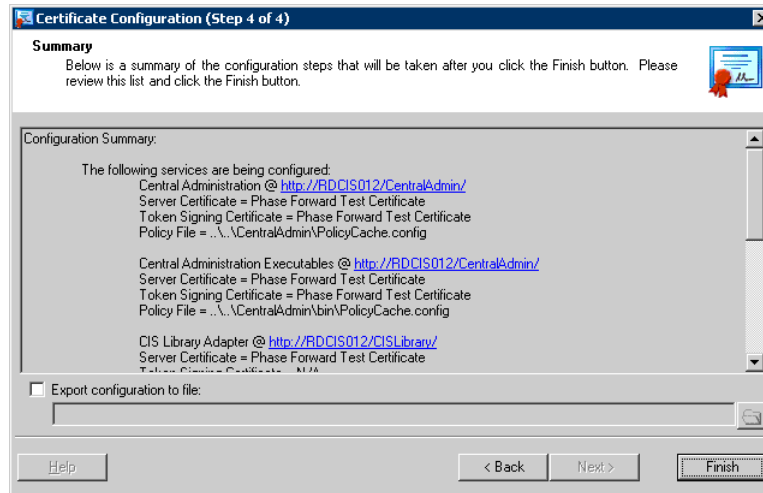
- 6 Click **Next**.

The Server page appears.



- 7 Click **Next**.

The Summary page appears. From this page, you can review your X.509 digital certificate information.



- 8 Click **Finish**.

The Company URL page appears.

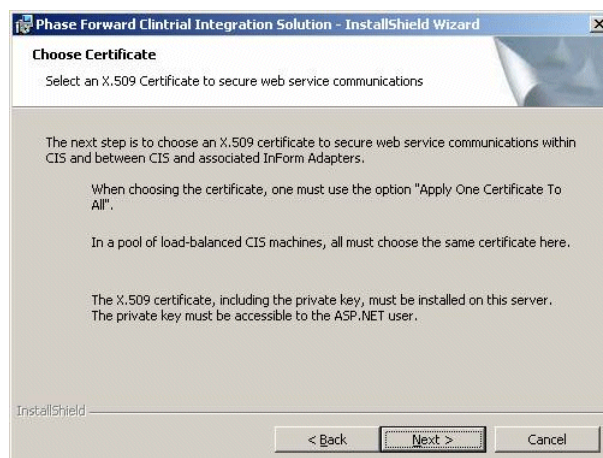
- 9 Continue with *Specifying a company URL* (on page 45).

### Configuring X.509 digital certificates for Authentication, Signing and Encryption

Digital certificates are used to secure communications within your CIS environment, and between the CIS software and the InForm Adapter software. You must configure these certificates for your product and the InForm Adapter software.

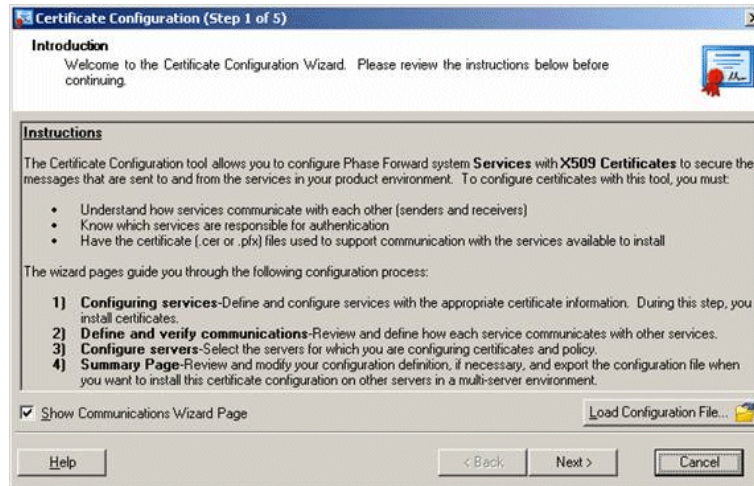
**Note:** If you have a pool of load-balanced CIS computers, you must apply the same X.509 certificate to all computers. The X.509 certificate, including the private key, must be installed on all load-balanced computers.

To configure digital certificates:



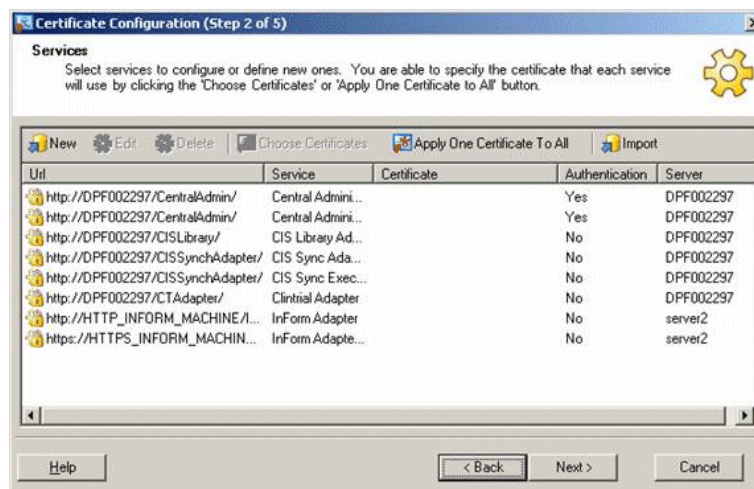
- 1 On the Choose Certificate page, click **Next**.

The Certificate Configuration Introduction page appears.



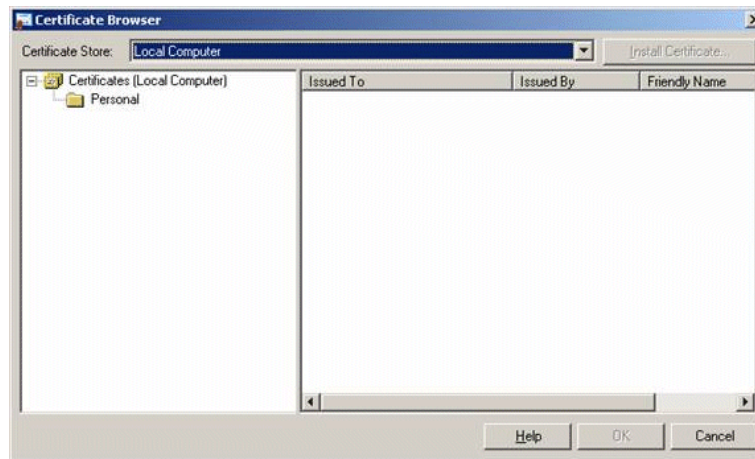
- 2 Click **Next**.

The Services page appears. Note that the Certificate column is empty.

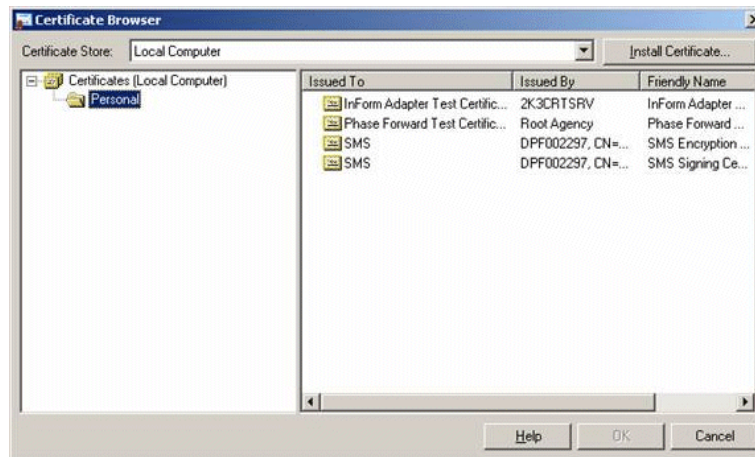


- 3 Click **Apply One Certificate To All**.

The Certificate Browser page appears.



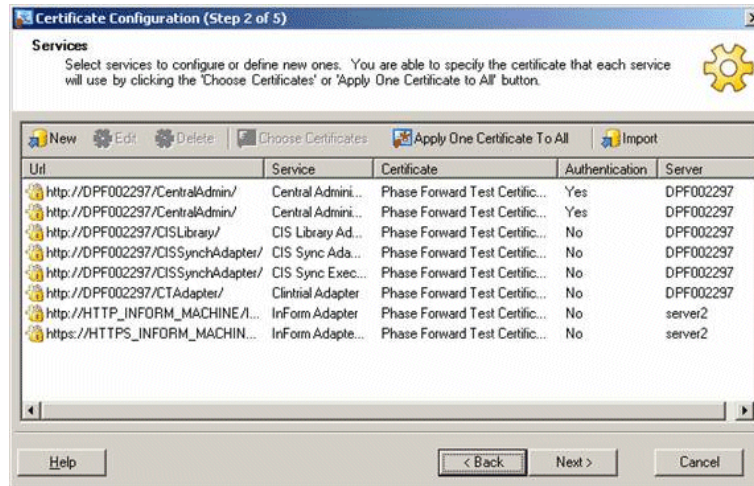
- 4 In the **Personal** folder, select the X.509 certificate that will be used to secure communications in this CIS installation.



**Note:** From this page, you can also install an X.509 certificate. For more information, see *Installing and applying a new certificate* (on page 70).

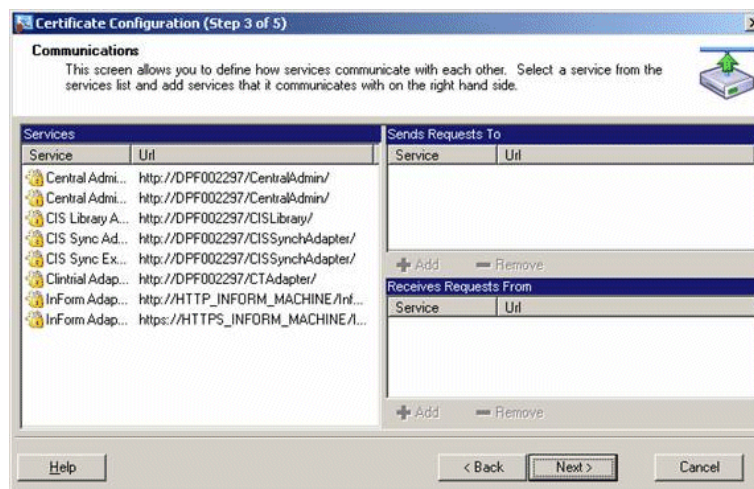
- 5 Click **OK**.

The Services page appears. Note that the selected X.509 certificate now appears.



- 6 Click **Next**.

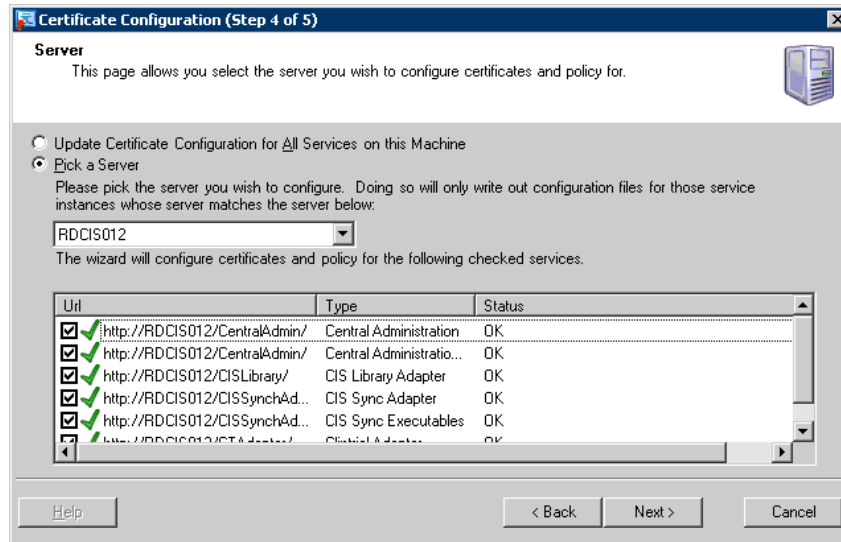
The Communications page appears.



- 7 Click **Next**.

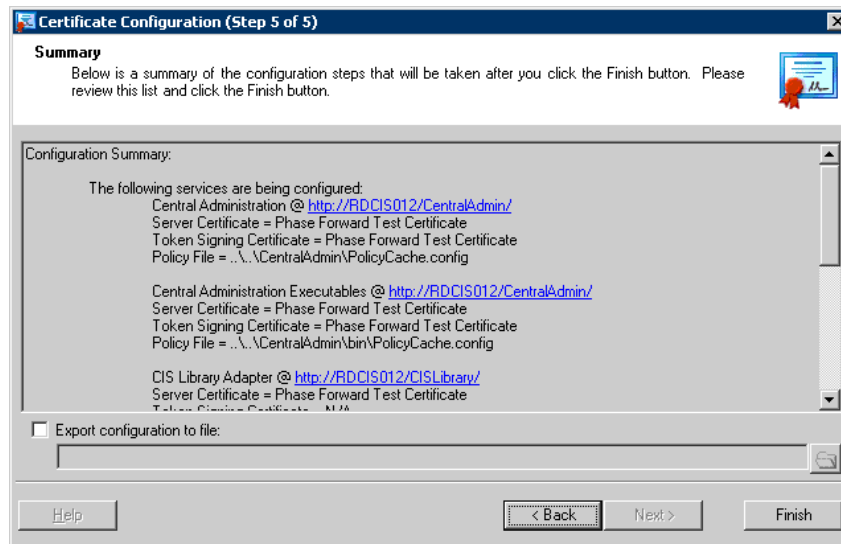


The Server page appears.



- 8 Click **Next**.

The Summary page appears. From this page, you can review your X.509 digital certificate information.



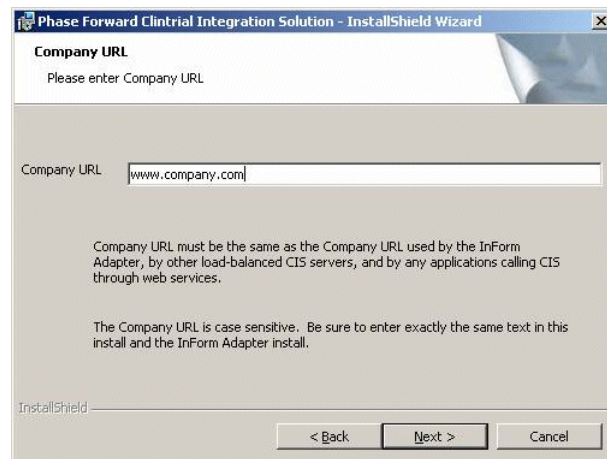
- 9 Click **Finish**.

The Company URL page appears.

- 10 Continue with *Specifying a company URL* (on page 45).

## Specifying a company URL

If you are installing CIS 4.6 SP1a for the first time, specify a company URL. If you have already installed a CIS 4.6 SP1a server, such as in a load balanced configuration, the Company URL already exists, and the Company URL field on the Company URL page is filled in and disabled.



- 1 In the **Company URL** field, provide your company URL:
  - This value does not need to correspond to a registered domain name, but it must be the same in the CIS software and the InForm Adapter software.
  - Use only letters, numbers, and periods. Do not use special characters.
  - CROs should choose a naming convention such as `www.TheNameOfTheCRO.com`, or `www.TheNameOfTheClientCompany.com`. For CROs that are using separate CIS and InForm Adapter servers for each customer, the latter option is preferred.

**Note:** The Company URL cannot be changed after the InForm Adapter software and the CIS software are installed. If the values for each respective company URL do not correspond exactly, the InForm Adapter software and the CIS software cannot communicate with each other.

- 2 Click **Next**.  
The Ready to Install the Program page appears.

## Running the installation

- To begin 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 when upgrading from a previous version.

The table lists the prerequisites, based on your previous version of the CIS software. For more information, see the *Release Notes*.

If you are upgrading from this release	Do this
CIS 4.5 SP1, 4.5 SP1a, 4.5 SP1c or subsequent releases of CIS 4.5 SP1 software	Follow the upgrade procedures in the CIS 4.6 SP1a <i>Release Notes</i> , including the instructions to upgrade the Oracle database software. The <i>Release Notes</i> indicate when to return to this <i>Installation Guide</i> .
CIS 4.6 SP1 or subsequent releases of the CIS 4.6 SP1 software	<ol style="list-style-type: none"> <li>1 Make sure that supported versions of the InForm software, Clintrial software, and InForm Adapter software are installed and their corresponding Oracle client and server requirements have been met. For more information, see the <i>Release Notes</i>.</li> <li>2 Uninstall the CIS 4.6 SP1 software.</li> </ol>

### To run the CIS software 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, Phase Forward 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 create a log file.
- The installation begins and the Welcome page appears.
- 2 Click **Next**.  
The Installation Scenario page appears.
  - 3 Select **Install CIS 4.6 SP1 with existing database**.
  - 4 Click **Next**.  
The License Agreement page appears.
  - 5 Continue with *Accepting the CIS licensing agreement* (on page 48).



## Running the CIS installation for a load-balanced configuration or with existing database

### About load-balancing

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.

In a load-balanced configuration, you do the following:

- First, install the first server using the standard installation process.  
For more information, see *Running the CIS installation for the first time* (on page 29).
- Next, you install additional servers using the installation procedures for load-balancing.

### 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, Phase Forward can use these log files to diagnose the problem.

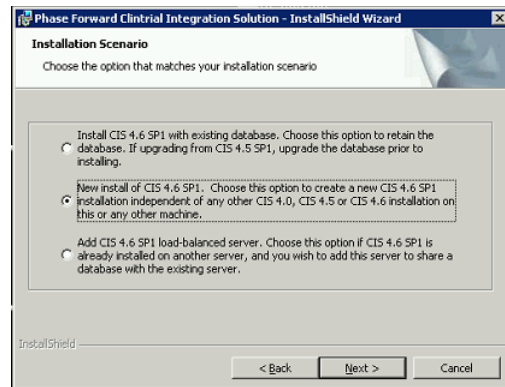
**Note:** After you complete the installation and use the log files to diagnose problems if necessary, delete the log files, because they can contain unencrypted information such as passwords.

- **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 **Add CIS 4.6 load-balanced server** and then click **Next**.

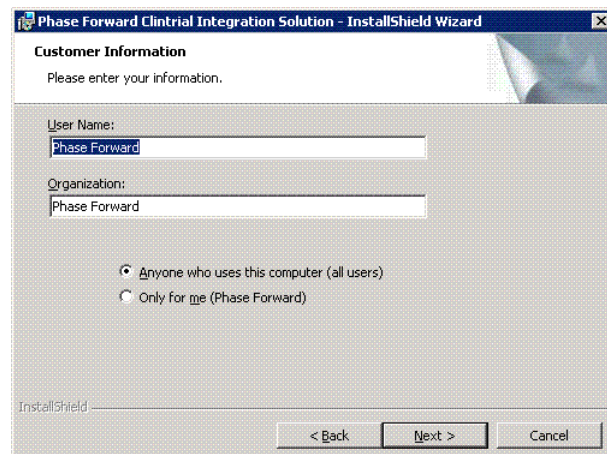
## Accepting the CIS licensing agreement

- To continue with the installation, select **I accept the terms in the license agreement**, and then click **Next**.

**Note:** To print a copy of the license agreement, click the **Print** button.

The Customer Information page appears.

## Providing customer information



- 1 Type 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.
- Choose whether to require that users sign in to the CIS application in order to run the installation.

- 2 Click **Next**.  
The Setup Type page appears.

## Choosing the setup type

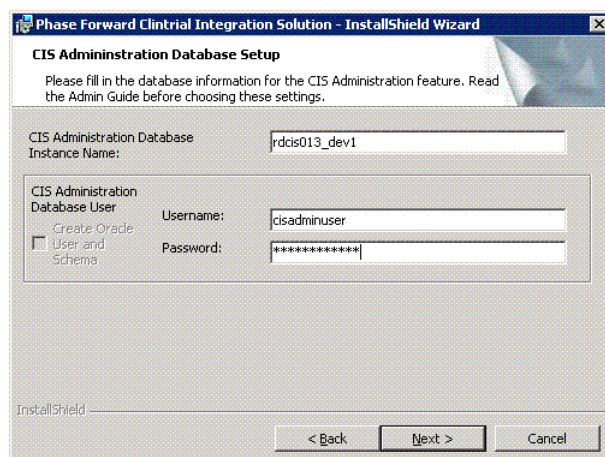
The setup type determines whether the CIS software is installed in the default location.

- **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.
- 1 Select either Typical or Custom setup type.

Select an option	Then do this
Typical	<ul style="list-style-type: none"> <li>• Click <b>Next</b>.</li> </ul>
Custom	<ol style="list-style-type: none"> <li>1 Click <b>Next</b>. The Custom Setup page appears.</li> <li>2 To see how much space you need to install the CIS software, click <b>Space</b>.</li> <li>3 To change the directory in which to install the software, click <b>Change</b>. The Change Current Destination Folder appears.</li> <li>4 Navigate to the destination folder, then click <b>OK</b>.</li> </ol>

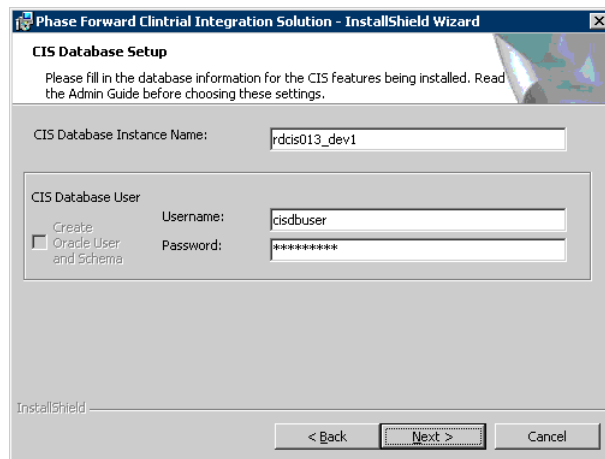
The CIS Administration Database Setup page appears.

## Setting up the CIS administration database for load-balancing or with an existing database



- 1 Type 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 load-balancing or with an existing database

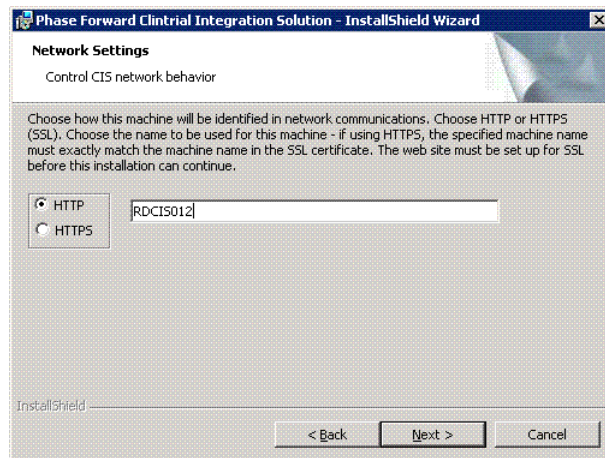


- 1 Type the database connection information for the CIS database user that is created by this installation:
    - **CIS Database Instance Name**—Oracle TNS name. The Oracle TNS name must not be greater than 16 characters.
    - **CIS Database User**—CIS Database username and password. Note that the Create Oracle User and Schema checkbox is dimmed. These fields are pre-populated, because you have already installed the initial CIS server.
  - 2 Click **Next**.
- The Network Settings page appears.

## Choosing HTTP or HTTPS for network settings

After the CIS database has been created, you must choose whether to use HTTP or HTTPS to secure internal CIS communications.

**Note:** This setting does not affect communications between the CIS software and the InForm Adapter software.



The following fields for network communications within CIS are available:

- **HTTP**—The web service on the computer where the CIS software is installed is addressed using the HTTP protocol.
- **HTTPS**—The web service on the computer where the CIS software is installed is addressed using the HTTPS protocol. If you select this option:
  - HTTPS must be used when you use **https://*machinename*/CentralAdmin** to log on to the CIS Administration application.
  - HTTPS is used for all web service calls to the various components of the CIS software.
  - When you register the InForm Adapter software, you can select a different network communications option.
  - If you select HTTPS for one computer in a set of load-balanced CIS computers, you **must** select HTTPS for all computers that are used for CIS load-balancing.

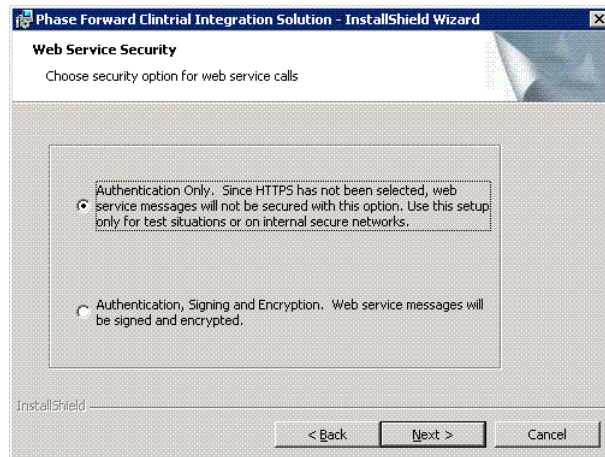
**Note:** The protocol must match the protocol that was chosen when installing on the first CIS server.

- **Machine name text box**—Initially displays the simple computer name of the server. However, if you select HTTPS, you must type the computer name **exactly** as it is encoded in the SSL certificate for that computer.

- 1 Select either HTTP or HTTPS.
- 2 Click **Next**.

The Web Service Security page appears.

## Choosing web service security



The following options for web service calls are available:

- **Authentication Only**—Web service calls are authenticated. Web service calls within CIS are encrypted using SSL if HTTPS was chosen on the previous screen.
- **Authentication, Signing and Encryption**—All web service calls are authenticated, signed, and encrypted, and messages within CIS are encrypted again using SSL.

1 Select either Authentication only or Authentication, Signing and Encryption.

**Note:** The web security option you choose must match the protocol chosen when the installation was run on the first CIS server.

2 Click **Next**.

The Choose Certificate page appears.

**Note:** After you install the CIS software, you can change the method that you chose during the installation.

## Configuring X.509 digital certificates

Select the procedure that matches your choice of web service security:

- *Configuring X.509 digital certificates for Authentication Only* (on page 53).
- *Configuring X.509 digital certificates for Authentication, Signing and Encryption* (on page 56).

## Configuring X.509 digital certificates for Authentication Only

Digital certificates are used to secure communications within your CIS environment, and between the CIS software and the InForm Adapter software. You must configure these certificates for your product and the InForm Adapter software.

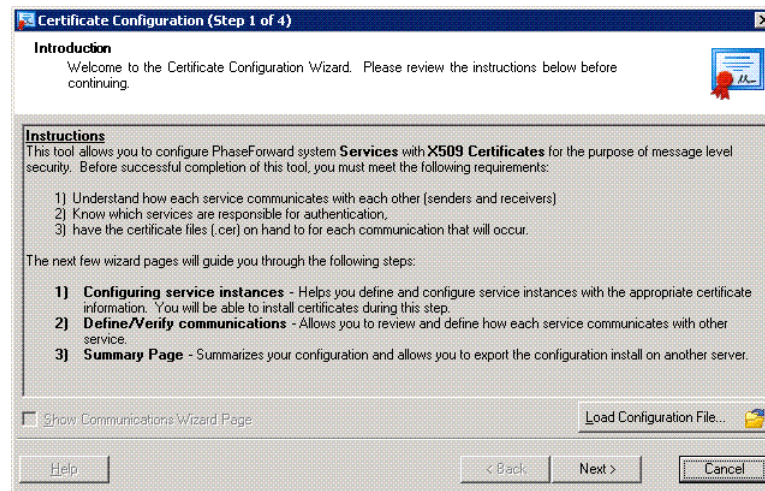
**Note:** If you have a pool of load-balanced CIS computers, you must apply the same X.509 certificate to all computers. The X.509 certificate, including the private key, must be installed on all load-balanced computers.

To configure digital certificates:



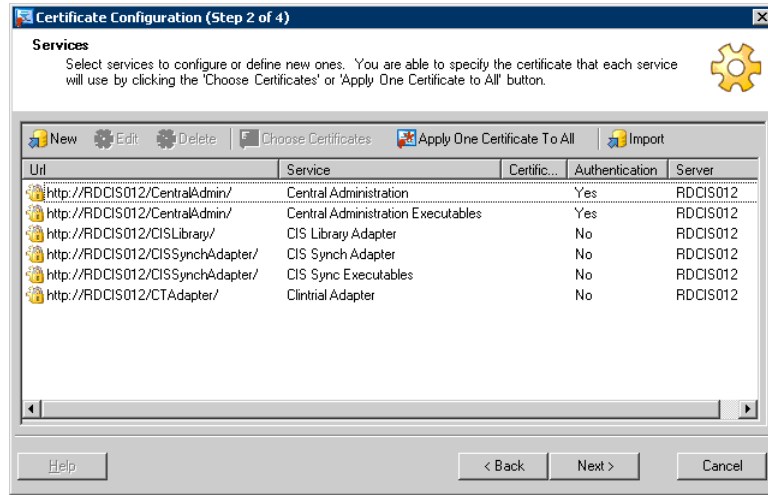
- 1 On the Choose Certificate page, click **Next**.

The Certificate Configuration Introduction page appears.



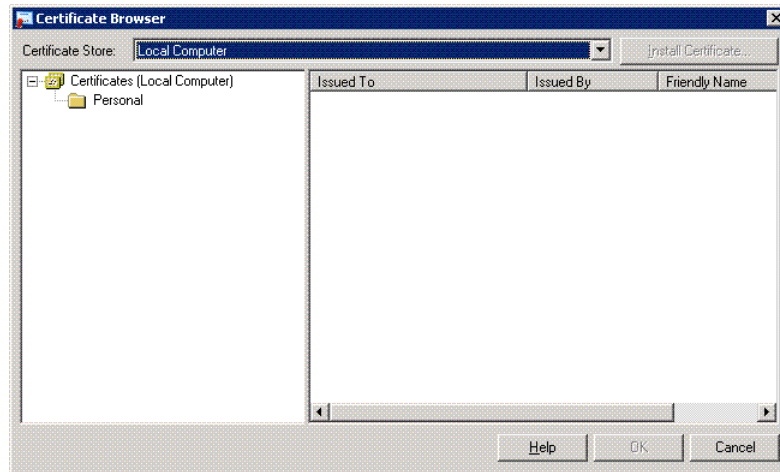
- 2 Click **Next**.

The Services page appears. Note that the Certificate column is empty.



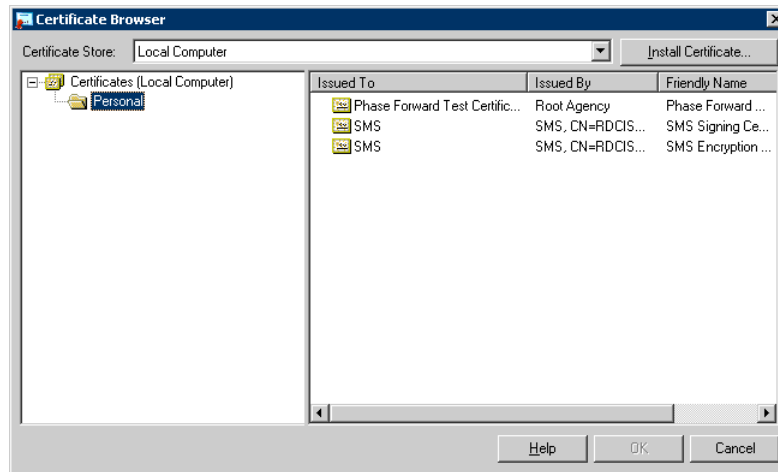
- 3 Click **Apply One Certificate To All**.

The Certificate Browser page appears.



- 4 In the **Personal** folder, select the X.509 certificate that will be used to secure communications in this CIS installation.

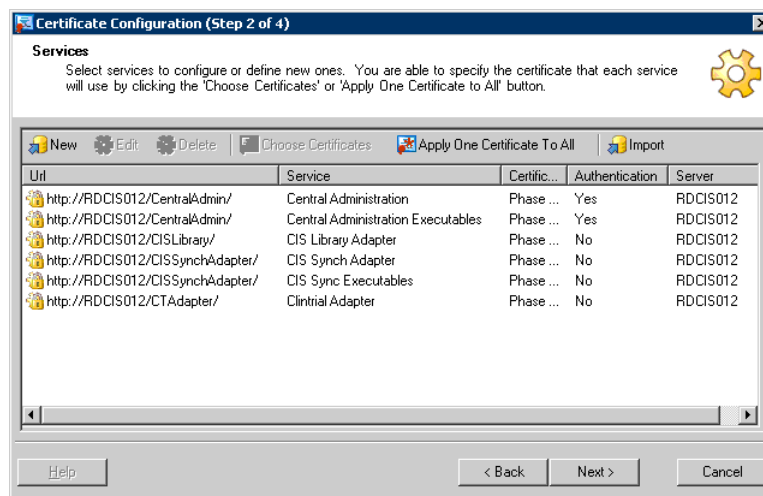




**Note:** From this page, you can also install an X.509 certificate. For more information, see *Installing and applying a new certificate* (on page 70).

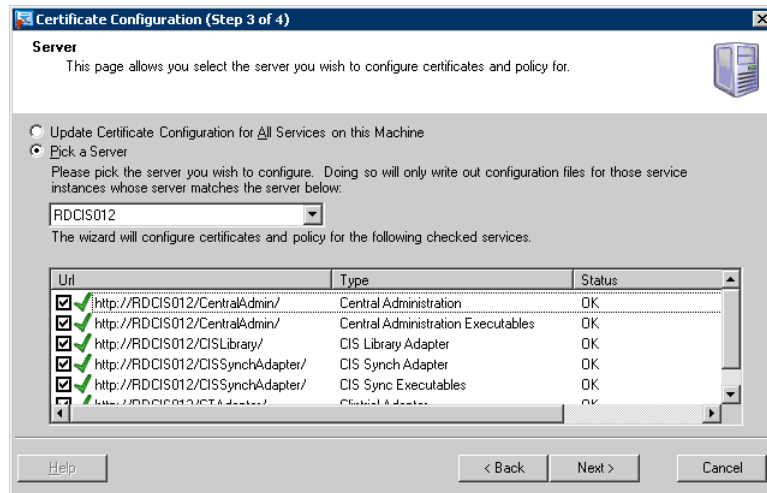
- 5 Click **OK**.

The Services page appears. Note that the selected X.509 certificate now appears, and that the Certificate column is populated.



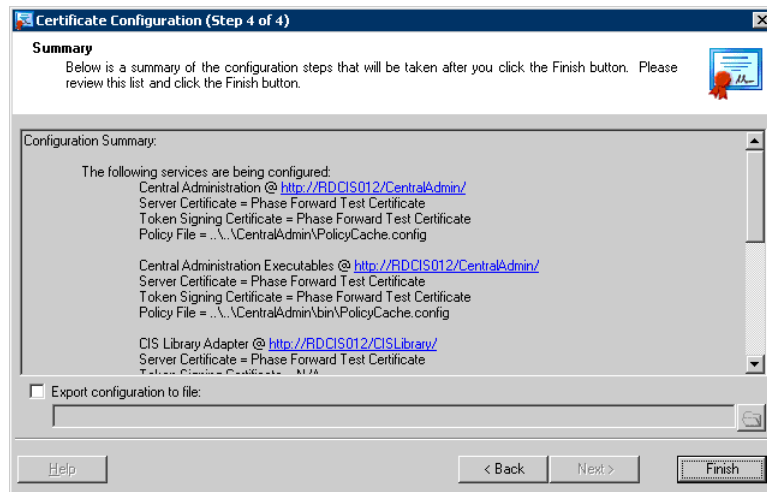
- 6 Click **Next**.

The Server page appears.



- 7 Click **Next**.

The Summary page appears. From this page, you can review your X.509 digital certificate information.



- 8 Click **Finish**.

The Company URL page appears.

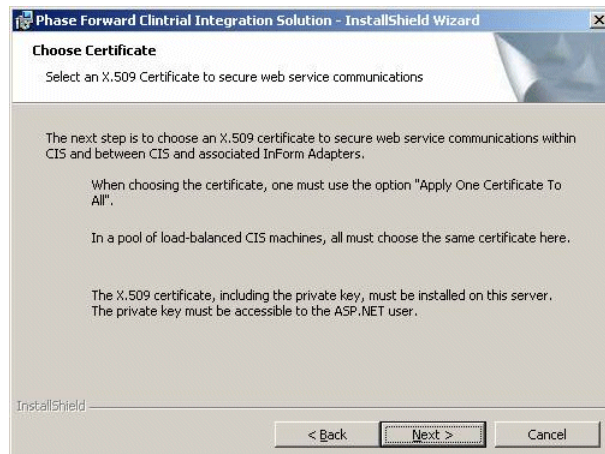
- 9 Continue with *Specifying a company URL* (on page 61).

### Configuring X.509 digital certificates for Authentication, Signing and Encryption

Digital certificates are used to secure communications within your CIS environment, and between the CIS software and the InForm Adapter software. You must configure these certificates for your product and the InForm Adapter software.

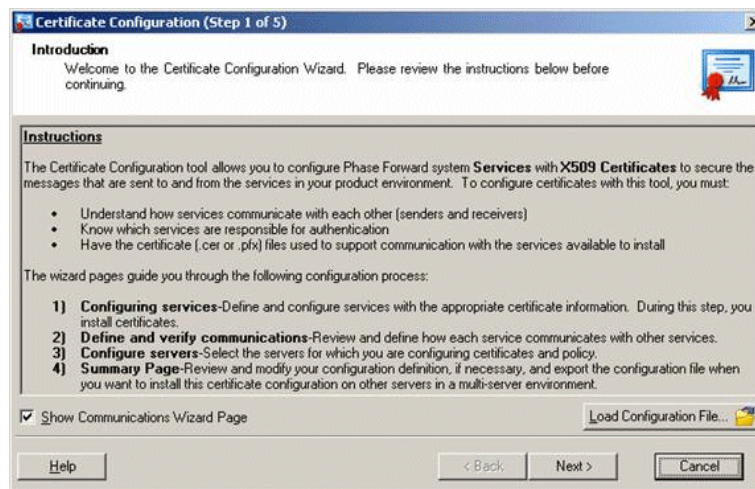
**Note:** If you have a pool of load-balanced CIS computers, you must apply the same X.509 certificate to all computers. The X.509 certificate, including the private key, must be installed on all load-balanced computers.

To configure digital certificates:



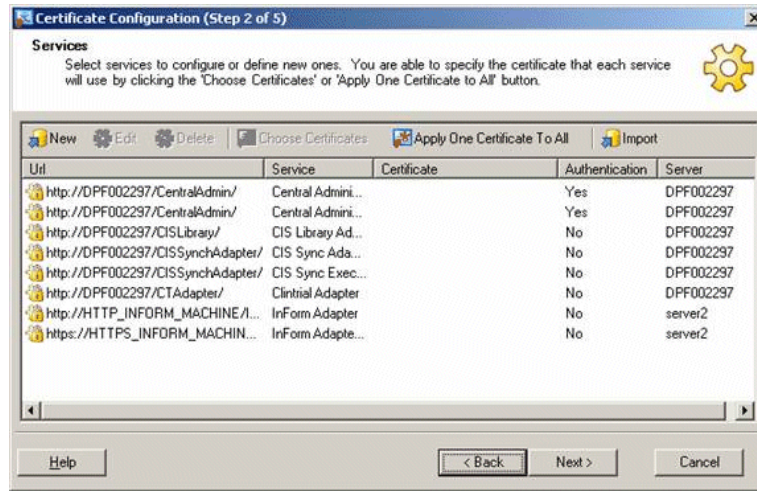
- 1 On the Choose Certificate page, click **Next**.

The Certificate Configuration Introduction page appears.



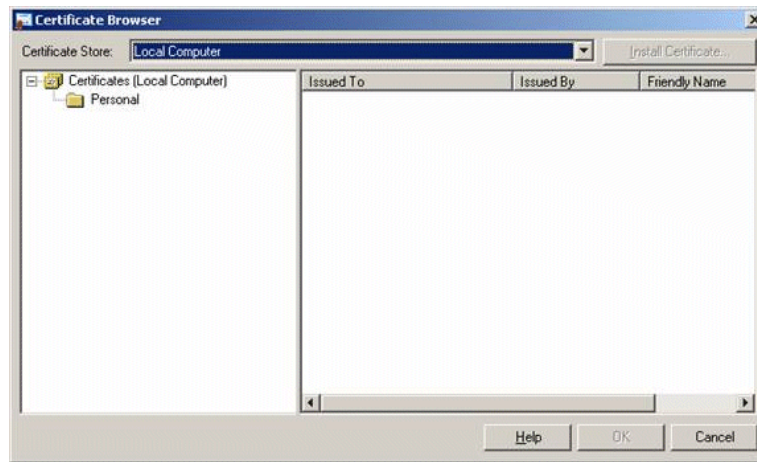
- 2 Click **Next**.

The Services page appears. Note that the Certificate column is empty.

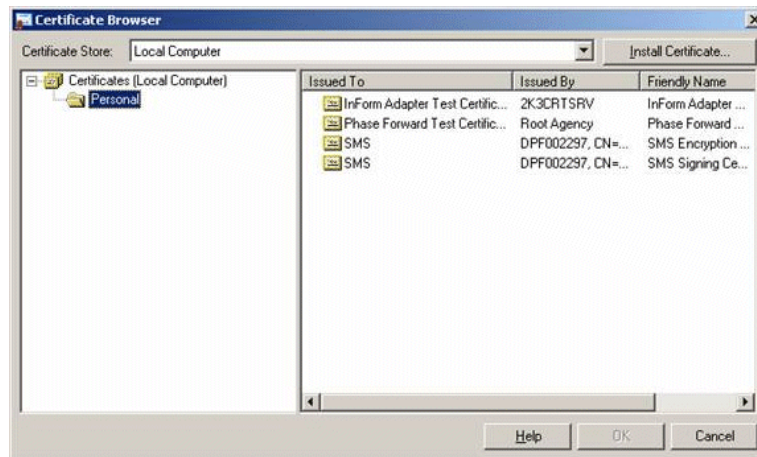


- 3 Click **Apply One Certificate To All**.

The Certificate Browser page appears.



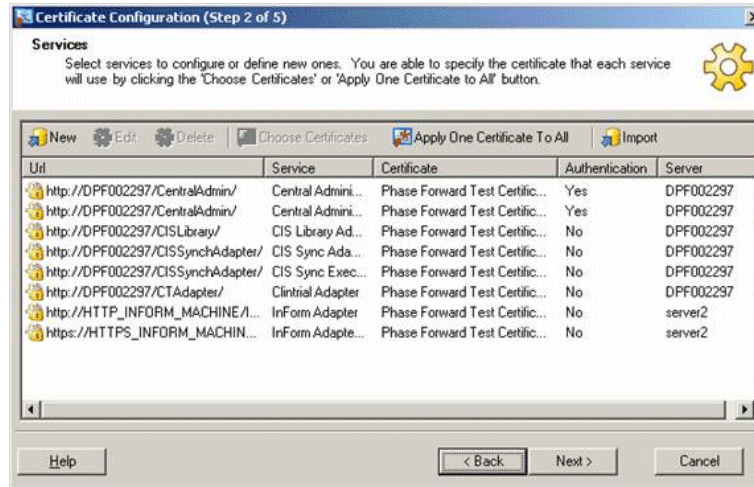
- 4 In the **Personal** folder, select the X.509 certificate that will be used to secure communications in this CIS installation.



**Note:** From this page, you can also install an X.509 certificate. For more information, see *Installing and applying a new certificate* (on page 70).

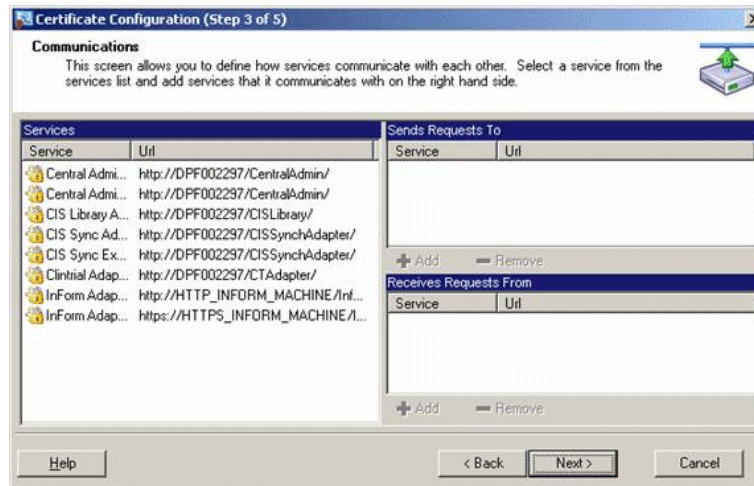
- 5 Click **OK**.

The Services page appears. Note that the selected X.509 certificate now appears.



- 6 Click **Next**.

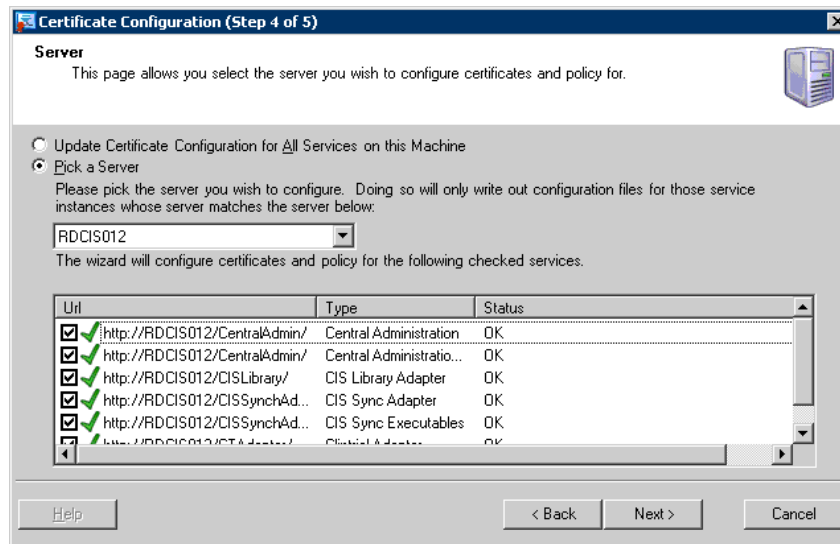
The Communications page appears.



- 7 Click **Next**.

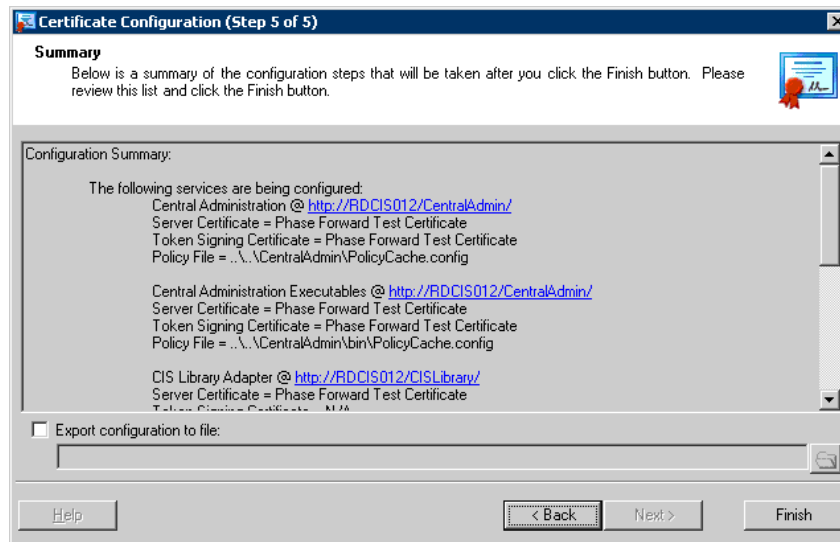


The Server page appears.



- 8 Click **Next**.

The Summary page appears. From this page, you can review your X.509 digital certificate information.



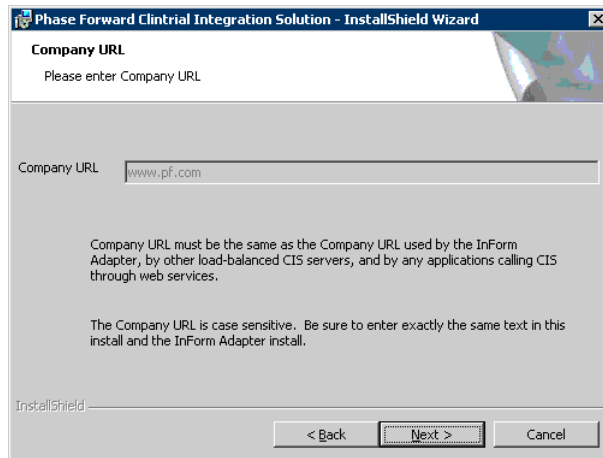
- 9 Click **Finish**.

The Company URL page appears.

- 10 Continue with *Specifying a company URL* (on page 61).

## Specifying a company URL

Because you have already installed a CIS 4.6 SP1a server, such as in a load-balanced configuration, the Company URL already exists. On the Company URL page, the Company URL field is filled in and entry to the field is disabled.



- Click **Next**.

The Ready to Install the Program page appears.

## Running the installation

- To begin 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.

## Shutting down the Phase Forward CIS 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.

You must manually stop and disable the service on the second and subsequent servers in a load-balanced configuration.

- 1 Open the services applet:
  - a Select **Start > Settings > Control Panel**.
  - b Double-click **Administrative Tools**.
  - c Double-click **Services**.
- 2 Right-click the PhaseForward CIS Sync Job Scheduler service and select **Stop**.

- 3 Right click the service name and select **Properties**.
- 4 Change the startup type to **disabled**.
- 5 Close the windows.



## CHAPTER 4

# After completing the CIS installation

### In this chapter

Securing the Service user name and password.....	64
Securing the predefined CIS user accounts .....	65
Updating the registry if CIS and the InForm software are installed on the same computer....	66
Increasing the timeout period for ASP.NET .....	67
Changing database connection information .....	68
Managing certificates and applying full security.....	69
Configuring CIS behind a Proxy server .....	74
Adding a service when there is more than one InForm Adapter service .....	75
Monitoring MS DTC logs.....	76

## 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, Phase Forward 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

To secure your CIS environment, Phase Forward 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.

## Updating the registry if CIS and the InForm software are installed on the same computer

If the CIS software and the InForm software are installed on the same computer, you must update the ByPassKeyPhrase key in your registry.

To update the registry:

- 1 Run regedit.
- 2 Navigate to **HKLM/Software/Phase Forward/AuthenticationFilter**.
- 3 Type the following value for ByPassKeyPhrase:  
`/CIS/|/CentralAdmin/|/CTAdapter/|/CISyncAdapter/|/CISLibrary/|/aspnet_client`
- 4 Clear the Internet Explorer cache.
  - a Open the Internet Explorer.
  - b Click **Tools > Internet Options > Delete Files**.
- 5 Restart IIS.

## 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 the servers. 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 (<http://www.asp.net/>).

**Note:** Phase Forward 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 (usually you would change this information if the Oracle password is changed), 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.

**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 information

- 1 Log on to a CIS server.
- 2 Open a Windows command prompt from the root of the installation directory.
- 3 Type the following command:

```
UpdateCISPassword Instance User Password
```

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

```
UpdateCISPassword DEV5.WORLD CISALL NEWPASSWORD
```

**Note:** If the servers are part of a pool of load-balanced servers, you must run this command on each CIS server.

## Changing the CIS administration database information

- 1 Log on to a CIS server.
- 2 Open a Windows command prompt from the **CentralAdmin\bin** directory under the installation directory.
- 3 Type the following command:

```
CAConfig CADB Instance User Password
```

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

```
CAConfig CADB DEV5.WORLD CISALL NEWPASSWORD
```

**Note:** If the servers are part of a pool of load-balanced servers, you must run this command on each CIS server.

# Managing certificates and applying full security

After installing the CIS software, you can manage certificates and implement full security to sign and encrypt messages. To complete these tasks, you run the Certificate Configuration utility using one of the following options:

- **Authentication Only** (on page 69)—Used to apply a new certificate to a service. Usually, you apply a new certificate when an X.509 certificate has expired or after you have applied full security but decide to revert to **Authentication Only**.
- **Authentication, Signing and Encryption** (on page 72)—Used to sign and encrypt messages for web services.

**Note:** If you have a pool of load-balanced CIS computers, you must apply the same X509 certificate to all computers. The X509 certificate, including the private key, must be installed on all load-balanced computers.

**Note:** In addition to performing these procedures for the CIS software, you must also perform the corresponding procedures for the InForm Adapter software. For more information, see the *InForm Adapter Installation Guide*.

## Using the Authentication Only option

### Overview of Authentication Only security

You can change a certificate for web services using the Certificate Configuration utility and the Authentication Only option.

When changing an X.509 digital certificate that is already installed or when installing a new X.509 digital certificate for web services, consider the following:

- The certificate that you want to apply must be in a certificate store that you can access using the Certificate Configuration utility.
- If the certificate has already been installed, you provided the Private Key password and granted the ASP.NET account permission to access the certificate when you installed the certificate.
- If you are installing a new certificate, you must provide the Private Key password and grant the ASP.NET account permission to access the certificate now. You can perform this task using the Certificate Configuration utility. For more information, see *Configuring X.509 digital certificates for Authentication Only* (on page 36).

**Note:** You can also use a third-party application to install an X.509 digital certificate, provide a Private Key password, and grant the ASP.NET account permission to access the certificate. For specific instructions, refer to the product documentation for the third-party application.


## Applying a certificate that is already installed

The following summarizes the steps you perform to apply an X.509 digital certificate that is already installed. For more information, see *Configuring X.509 digital certificates for Authentication Only* (on page 36).

- 1 Select **Start > Programs > Phase Forward > CIS > Web Service Security > Authentication Only**.  
The Certificate Configuration utility starts and the Introduction page appears.
- 2 Click **Next**.  
The Services page appears.
- 3 Select **Apply One Certificate To All**.  
The Certificate Browser window appears.
- 4 Select the store where the certificate is installed, and select the certificate that you want to apply.
- 5 Click **OK**.  
The Certificate Selection window opens.
- 6 Click **OK**.  
The Services page appears, and the new certificate appears next to the services that you selected.
- 7 Click **Next**, and accept the default selections until the Summary page appears.
- 8 Click **Finish**.

## Installing and applying a new certificate

The following summarizes the steps to install and apply a new X.509 digital certificate. For more information, see *Configuring X.509 digital certificates for Authentication Only* (on page 36).

- 1 Select **Start > Programs > Phase Forward > CIS > Web Service Security > Authentication Only**.  
The Certificate Configuration utility starts and the Introduction page appears.
- 2 Click **Next**.  
The Services page appears.
- 3 Select **Apply One Certificate To All**.  
The Certificate Browser page appears.
- 4 Select the store where the certificate is stored.
- 5 Click **Install Certificate**.  
The Certificate Installer window appears.
- 6 Click the browse icon () to select the certificate you want to install and apply.
- 7 Verify that **File Contains Private Key** is selected.
- 8 Verify that **Add ASP.NET** is selected.
- 9 Select the **ASP.NET Account**.
- 10 Click **OK**.



The Certificate Browser window appears.

- 11 Select the certificate that you just installed.
- 12 Click **OK**.

The Services page appears.

- 13 Click **Next**, and accept the default selections until the Summary page appears.
- 14 Click **Finish**.
- 15 Grant rights to the private key to the NETWORK SERVICE user.

For more information, see *Granting rights to the NETWORK SERVICE user for the private key* (on page 25).

## 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 Install the WSE 2.0 X.509 certificate tool with the administrator option.
- 2 To open the tool, select **Start > All Programs > WSE 2.0 > X509 Certificate Tool**.
- 3 Set the Certificate Location to **Local Computer**.
- 4 Set the Store Name to **Personal**.
- 5 Click **Open Certificate**.
- 6 Select your certificate, then click **OK**.
- 7 Click **View Private Key File Properties**.
- 8 Select the **Security** tab.
- 9 Click **Locations**.
- 10 In the Locations dialog box, change to the local computer and then click **OK**.
- 11 In the Select Users or Groups box, type **network service** and then click **Check Names**.

The tool displays NETWORK SERVICE.

- 12 Make sure that the **Read and Execute** check box and the **Read** check box are selected.
- 13 Click **OK** to close the dialog box.
- 14 Continue to click **OK** on subsequent dialog boxes until the tool is closed.

## Using the Authentication, Signing and Encryption option

### Overview of Authentication, Signing and Encryption

You can use the Authentication, Signing and Encryption option to implement full security. Full security includes:

- User authentication.
- Signing and encryption of web messages.

When implementing full security for services, consider the following:

- The certificate that you want to apply must be installed and accessible using the Certificate Configuration utility. If the certificate is not already installed, you must install it using either the Certificate Configuration utility or a third-party application. For more information, see *Installing and applying a new certificate* (on page 70).
- You must provide a password for the private key.
- You must grant the ASP.NET account permission to access the certificate.
- You must edit the base URL for the InForm Adapter web service and apply a new certificate.
- You must add an InForm Adapter service if you have multiple InForm Adapters that use different certificates.

When you implement full security using the Overview of Authentication, Signing and Encryption option, you can apply:

- One X.509 digital certificate to the CIS and InForm Adapter services.
- Different certificates to the CIS and InForm Adapter services.

**Note:** For CIS installations hosted by Phase Forward, one X.509 certificate per CIS and InForm Adapter, obtained from an external (root) Certificate Authority (such as Verisign), will be used.

### Applying one X.509 digital certificate

To apply one X.509 digital certificate for all services and implement full security, run the Certificate Configuration utility using the Authentication, Signing and Encryption option. For more information, see *Configuring X.509 digital certificates for Authentication, Signing and Encryption* (on page 40).

### Applying a different X.509 digital certificate to different services

The following steps provide instructions for applying a different X.509 digital certificate for the InForm Adapter service. Before you perform these steps, you must apply a single certificate to all the services in your CIS environment. For more information, see *Configuring X.509 digital certificates for Authentication, Signing and Encryption* (on page 40).

To apply a different X.509 digital certificate to an InForm Adapter service:

- 1 Select **Start > Programs > Phase Forward > CIS > Web Service Security > Authentication, Signing and Encryption**.

The Certificate Configuration utility starts and the Introduction page appears.

- 2 Click **Next**.

The Services page appears and displays a list of URLs for the services in your environment. The list can include two URLs for the InForm Adapter service:

`//HTTP_/INFORM_MACHINE_NAME/` for a non-secured connection, and


`//HTTPS_/INFORM_MACHINE_NAME/` for a secured connection.

- 3 From the services list, select either `//HTTP` or `//HTTPS` for the InForm Adapter service.

**Note:** You cannot add a base URL for both HTTP and HTTPS. You can choose only one.

- 4 Click **Edit**.

The Service Definition page appears.

- 5 Click the add icon ()

The Base URL Definition page appears.

- 6 Type the existing URL (either `//HTTP_/INFORM_MACHINE_NAME/` or `//HTTPS_/INFORM_MACHINE_NAME/`) where the `INFORM_MACHINE_NAME` portion of the URL is the actual computer name.

- 7 Click **OK** until you return to the Services page.

- 8 Select **Choose Certificate**.

The Certificate Selection page appears and displays the certificate that you previously applied to all services.

- 9 Click the browse icon ()

The Certificate Browser page appears.

- 10 Select the store where the certificate is installed, and select the certificate that you want to use for the InForm Adapter service.

**Note:** From this page, you can also install an X.509 certificate. For more information, see *Installing and applying a new certificate* (on page 70).

- 11 Click **OK** until you return to the Services page.

- 12 Click **Next**, and accept the default values until the Summary page appears.

- 13 Click **Finish**.

## 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\CentralAdmin\web.config
- *installation\_path*\Program Files\Phase Forward\Clintrial Integration Solution\CISLibrary\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 as a direct child of the <configuration> tag; for example, as a sibling of the <startup> tag:

```
<startup>
  <supportedRuntime version="v1.1.4322" />
</startup>
```

- 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.

## Adding a service when there is more than one InForm Adapter service

If you have more than one InForm Adapter service in your CIS environment, you must configure each additional service. When you configure the additional services, you provide the same information as the original service except for the URL that identifies the location of the other InForm Adapter services.

To add a service when there is more than one InForm Adapter service:

- 1 Select **Start > Programs > Phase Forward > CIS > Web Service Security > Authentication, Signing and Encryption Security**.

The Certificate Configuration utility starts, and the Introduction page appears.

- 2 Click **Next**.


The Services page appears.

- 3 Select an existing InForm Adapter service.

- 4 Click **New**.

The Service Definition window appears.

- 5 Type information for the new InForm Adapter service. The information you type for the new InForm Adapter service must be the same as the original InForm Adapter service except for the URL that identifies the location of the InForm Adapter software. Therefore, enter the following values:


- In the **Type** field, type InForm Adapter.
- Select **This service receive request from other services**.
- Using the Add icon () , type a URL that provides the location of the InForm Adapter software for which you are adding the service.
- In the **Server** field, select the same server that was used by the original InForm Adapter service.

- 6 Click **OK**.

The Services page appears.

- 7 Click **Next**.

The Communications page appears.

- 8 For the new service, use the **Add** icon () to add the same Receives Requests From services as those defined for the original InForm Adapter service.

- 9 Click **Next** and accept the default values until the Summary page appears.

- 10 Click **Finish**.

## 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 problems within your system, the logs can quickly reach their maximum size.

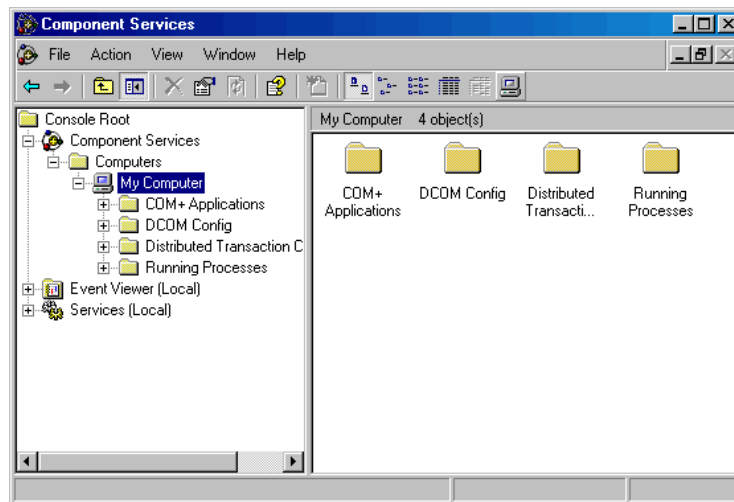
Phase Forward recommends the following:

- Move the logs from their default location (%SystemRoot%\SYSTEM32\DTClog) to some other 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 > Programs > Administrative Tools > Component Services**.



- 3 Expand **Component Services**.
- 4 Expand **Computers**.
- 5 Right-click **My Computer** and select **Properties**.
- 6 Select the **MS DTC** tab.
- 7 Perform the maintenance that is described in the following table.

To do this:

Move MS DTC logs

Follow these steps:

In the Location field, specify the directory in which to store the MS DTC logs.

To do this:	Follow these steps:
Expand the log capacity	<p>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.</p> <p>You might receive the following message:</p> <p>The MS DTC log file is full and cannot accept new log records.</p>
Clear a log	Click Reset log.

- 8 Click **OK**.
- 9 Restart the MS DTC service by issuing the following command in a Windows command window:  

```
net start MSDTC
```