Informatica

Informatica® Cloud Data Integration for PowerCenter

July 2024

Installation Guide

Informatica Cloud Data Integration for PowerCenter Installation Guide
July 2024

Publication Date: 2024-07-20

Table of Contents

Preface 8

Chapter 1: Getting started 9

Installation process 10

Chapter 2: Before you begin 11

Download the installers from Informatica Intelligent Cloud Services 11

Log in to Informatica Intelligent Cloud Services 11

Download the installers 12

Verify system requirements 12

Verify disk space 12

Verify sizing requirements 13

Review patch requirements 14

Verify port requirements 14

Review the environment variables on Linux 15

Verify the file descriptor limit on Linux 16

Prepare the repository databases 16

Prepare the domain configuration repository database 16

Prepare the CDI-PC repository database 20

Set up a database user account 23

Create a system user account 23

Set the database client environment variables 24

Prepare for Kerberos authentication 25

Set up the Kerberos configuration file 26

Generate the service principal and keytab file name format 27

Review the SPN and keytab format text file 29

Create the service principal names and keytab files 31

Set up keystore and truststore files 32

Validate the certificates with the TLS utility 33

Configuring the TLS utility in silent mode 34

Import the CDI-PC domain truststore certificates to the Secure Agent truststore 35

Run the pre-installation system check tool 35

Run the pre-installation system check tool in console mode 35

Run the pre-installation system check tool in graphical mode 37

Run the pre-installation system check tool in silent mode 40

Chapter 3: Installing Secure Agents 41

Install the Secure Agent on Linux 41

Secure Agent requirements on Linux 41

Configure the firewall 42

Downloading and installing the Secure Agent on Linux. . . . 42
Install the Secure Agent on Windows. . . . 43
Secure Agent requirements on Windows. . . . 44
Configure the firewall. . . . 44
Downloading and installing the Secure Agent on Windows. . . . 44
Verify the license edition. . . . 46
Generate keystore and truststore certificates. . . . 46
Import the Secure Agent truststore certificate to the domain truststore. . . . 47
Configure TLS for the Secure Agent. . . . 47

Chapter 4: Create a CDI-PC domain. . . . 48

Run the installer in console mode. . . . 48
Provide the license key and installation directory path. . . . 49
Configure domain settings and secure communication. . . . 50
Configure secure communication in the domain. . . . 52
Configure the domain configuration repository. . . . 52
Enter encryption key details. . . . 55
Configure the domain and node. . . . 55
Create the CDI-PC Repository Service and the CDI-PC Integration Service. . . . 57
Run the installer in graphical mode. . . . 58
Provide the license key and installation directory path. . . . 59
Configure domain settings and secure communication. . . . 61
Configure secure communication. . . . 62
Configure the domain configuration repository. . . . 62
Enter encryption key details. . . . 65
Configure the domain and node. . . . 66
Configure the ports. . . . 68
Configure Windows service. . . . 69
Create the CDI-PC Integration Service and the CDI-PC Repository Service. . . . 69
After you create the domain. . . . 70
Register the domain in CDI-PC 70
Create the CDI-PC Repository Service in Informatica Administrator. . . . 71
Create the CDI-PC Integration Service in Informatica Administrator. . . . 73
Configure JVM parameters. . . . 75
Post-installation step for Data Quality. . . . 75

Chapter 5: Join a CDI-PC domain. . . . 76

Run the installer in console mode. . . . 76
Provide the license key and installation directory path. . . . 77
Join an existing domain. . . . 78
Configure secure communication. . . . 78
Configure the domain configuration repository. . . . 79
Enter encryption key details. . . . 79

Configure the node. . . . 80
Create the CDI-PC Repository Service and the CDI-PC Integration Service. . . . 81
Run the installer in graphical mode. . . . 82
Provide the license key and installation directory path. . . . 82
Join an existing domain. . . . 84
Configure secure communication. . . . 85
Configure the domain configuration repository. . . . 85
Enter encryption key details. . . . 86
Configure the node. . . . 86
Configure the ports. . . . 87
Configure Windows service. . . . 88
CDI-PC Repository Service and the CDI-PC Integration Service. . . . 88
Post-installation step for PowerExchange. . . . 89
Configure JVM parameters. . . . 90

Chapter 6: Run the silent installer. . . . 91

Create the properties file. . . . 91
Run the installer in silent mode on Linux. . . . 91
Run the installer in silent mode on Windows. . . . 92

Chapter 7: Resuming an installation. . . . 93

Before you resume the installer. . . . 93
Resuming the installer in console mode. . . . 94
Resuming the installer in graphical mode. . . . 94
Resuming the installer in silent mode. . . . 94

Chapter 8: Before you migrate the Informatica domain. . . . 96

Copy folders to a common location. . . . 97
Set up keystore and truststore files for the CDI-PC domain. . . . 98
Update the node to add or replace the certificates. . . . 100
Run the TLS Utility to validate the certificates. . . . 100
Back up the PowerCenter repository. . . . 101
Back up essential Data Transformation files. . . . 102
Shut down the Informatica domain. . . . 102
Back up the Informatica domain. . . . 102
Import the CDI-PC domain truststore certificates to the Secure Agent truststore. . . . 104

Chapter 9: Migrate the domain 105

Run the installer in console mode. . . . 105
Enter the Informatica service directory details. . . . 106
Confirm the domain and node details. . . . 106
Enter the migration directory and backup preferences. . . . 107
Configure encryption key details. . . . 107

Run the installer in graphical mode. . . . 108
Enter the Informatica service directory details. . . . 108
Confirm the domain and node details. . . . 108
Enter the migration directory and backup preferences. . . . 109
Configure secure communication. . . . 109

Chapter 10: Migrate the domain with changes to node configuration. 111

Migrate the domain configuration repository to a different database. . . . 111
Migrate the installation to a different machine. . . . 112
Copy the installation directory. . . . 112
Verify port requirements. . . . 112
Configure native connectivity on service machines. . . . 113
Install database client software. . . . 114
Run the installer in console mode. . . . 115
Enter the Informatica service directory details. . . . 115
Confirm the domain and node details. . . . 115
Enter the migration directory. . . . 116
Configure secure communication. . . . 116
Configure the domain configuration repository. . . . 117
Configure the node details. . . . 119
Configure port numbers. . . . 119
Run the installer in graphical mode. . . . 120
Enter the Informatica service directory details. . . . 121
Confirm the domain and node details. . . . 121
Enter the migration directory. . . . 122
Configure secure communication. . . . 122
Configure the domain configuration repository. . . . 122
Configure the node details. . . . 125
Configure port numbers. . . . 126
Complete the node configuration changes. . . . 126

Chapter 11: Migrate the domain in silent mode. 129

Create the properties file. . . . 129
Run the installer in silent mode. . . . 130

Chapter 12: After you migrate the domain. 131

Register the domain. . . . 131
Update the backup directory location. . . . 132
Update the environment variables. . . . 132
Configure JVM parameters. . . . 133
Enable the CDI-PC domain application services. . . . 133
Upgrade the CDI-PC Repository Service content. . . . 134
Update the configuration files. . . . 134

Update $PMRootDir for the CDI-PC Integration Service. 134

Chapter 13: Install the CDI-PC Client. 136

Before you install the client. 136

Verify system requirements. 136

Set the environment variables. 136

Install the CDI-PC Client in graphical mode. 137

Install the CDI-PC Client in silent mode. 137

Post-installation step for PowerExchange. 138

Chapter 14: Uninstall Cloud Data Integration for PowerCenter (CDI-PC). 139

Uninstalling the CDI-PC domain in console mode. 140

Uninstalling the CDI-PC domain in graphical mode. 140

Uninstalling the CDI-PC domain in silent mode. 140

Chapter 15: Uninstalling the CDI-PC Client. 142

Uninstalling the CDI-PC Client in graphical mode. 142

Uninstalling the CDI-PC Client in silent mode. 142

Uninstalling the CDI-PC Client from the Control Panel. 143

Uninstalling the CDI-PC Client from the shortcut. 143

Chapter 16: Uninstalling the Secure Agent. 144

Uninstalling the Secure Agent on Linux. 144

Uninstalling the Secure Agent on Windows. 144

Appendix A: CDI-PC components. 146

Components. 146

Index. 151

Preface

Follow the instructions in the *Installation Guide* to learn how to install the different components of Cloud Data Integration for PowerCenter (CDI-PC). The guide includes pre- and post-requisite tasks and steps to install the Secure Agent, the CDI-PC domain, and the client for the CDI-PC domain.

CHAPTER 1

Getting started

To perform tasks in Cloud Data Integration for PowerCenter (CDI-PC), install all components and register the domain in Informatica Intelligent Cloud Services.

CDI-PC includes the following components:

- CDI-PC domain. An on-premises domain with services and repositories. You can extract data from sources, transform the data according to business logic that you build in the client application, and load the transformed data into targets. Import sources and targets and run workflows to move or transform data.
- CDI-PC Client. Use the CDI-PC Client to create, run, and monitor jobs that you run in the domain.
- Administrator tool. Log in to the Administrator tool to create application services and manage the domain and services.
- Secure Agent. A lightweight program that you install on a Linux or Windows machine. The Secure Agent enables communication between the on-premises domain and Informatica Intelligent Cloud Services.
- CDI-PC service. The Informatica Intelligent Cloud Services service to monitor domain status and initiate domain updates.

You can monitor the status of the on-premises domain and the services from the cloud. After you install and register the domain, you can use the CDI-PC Client to create and run workflows in the domain. Registering the domain in Informatica Intelligent Cloud Services creates a connection between the on-premises domain and the cloud. You require connectivity to monitor the status of your domains and services. You can then take required action if a domain or service becomes unavailable.

CDI-PC components are interdependent. You create the domain services after you register the domain in Informatica Intelligent Cloud Services.

Before you install CDI-PC, ensure that you have an organization and that you have the required CDI-PC license edition.

If you are an existing CDI-PC user that uses PowerExchange and you do not have the Cloud Allowed = Y option set for your PowerExchange Listener license keys, you must update your PowerExchange Listener license keys and ensure that they have the Cloud Allowed = Y option set before you upgrade or migrate to CDI-PC 2024.04.M or later.

Installation process

A CDI-PC installation includes multiple components that are interdependent. To ensure that you can perform tasks in CDI-PC, install the components and perform all configuration tasks in the correct order.

Consider the following high-level installation tasks:

1. Install the Secure Agent.
   Verify the requirements and perform all configuration tasks to install the Secure Agent.
2. Run the installer to create a CDI-PC domain, join a domain, or migrate an Informatica domain.
   The CDI-PC domain and the Secure Agent must be on the same operating system. For example, you can't establish communication between a domain installed on Linux and a Secure Agent installed on Windows.

   Note: You can't perform any of these tasks manually. You must run the installer.

   Perform the required prerequisite and post-requisite tasks. The tasks vary depending on whether you install or migrate the domain. When you migrate, you migrate the Informatica domain and the following services:

   - PowerCenter Integration Service
   - PowerCenter Repository Service
   - Web Services Hub Service
   - PowerExchange Listener Service
   - PowerExchange Logger Service
   - PowerCenter SAP BW Service

   If the domain includes other services, you can't proceed with migration.

   Note: You can't use the backup of an Informatica domain to create a CDI-PC domain. The restore of a 10.4.x domain generates an error. No error appears if you restore the backup of a 10.5.0, 10.5.1, 10.5.2, 10.5.3, 10.5.4, or 10.5.5 domain, but the domain doesn't work as expected. To migrate an Informatica domain, run the installer and choose the option to migrate.
3. Install the CDI-PC Client.
   Verify the requirements and perform the prerequisite tasks before you install the client.

   Install the client even if you migrate an Informatica domain. You can't use the PowerCenter Client with CDI-PC.

CHAPTER 2

Before you begin

Before you run the installer to create a CDI-PC domain, review the requirements and perform all prerequisite tasks.

Download the installers from Informatica Intelligent Cloud Services

You can download the installers for CDI-PC components from Informatica Intelligent Cloud Services.

You can download the following installers:

- CDI-PC server. Run this installer to create or join a CDI-PC domain, or to migrate an Informatica domain to CDI-PC.
- CDI-PC Client. Run this installer to install the CDI-PC Client.
- Command line utilities. Download and extract this file to use command line programs such as infacmd, pmcmd, or pmrep on machines that don't have the domain or clients installed.
- CDI-PC TLS Utility. Download this utility to validate whether your custom TLS certificates are valid for use with CDI-PC.
- Digital signature for binaries. Download this digital signature to verify the integrity of the downloaded installers.

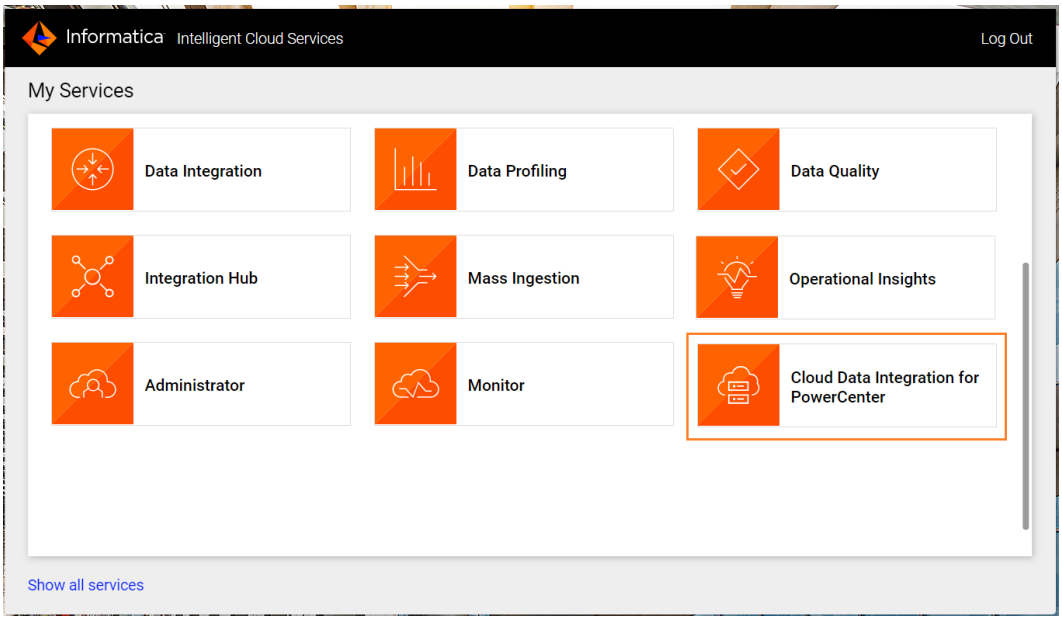
To download the files that you need, log in to Informatica Intelligent Cloud Services and download the files from the CDI-PC **Home** page.

Log in to Informatica Intelligent Cloud Services

Log in to Informatica Intelligent Cloud Services and select Cloud Data Integration for PowerCenter (CDI-PC) from the **My Services** page.

When you log in to Informatica Intelligent Cloud Services, the **My Services** page displays the services that your organization is licensed to use and common services that are available under the same license, such as Administrator.

The following image shows Cloud Data Integration for PowerCenter (CDI-PC) on the **My Services** page:



Download the installers

After you log in to Informatica Intelligent Cloud Services, you can download the installers from the CDI-PC **Home** page.

Before you download the installers, allow pop-ups in your browser.

1. On the **Home** page, click **Download Installers** in the **Download Installers** section.
2. On the **Download CDI-PC Installers** window that appears, select the installers that you want to download.
3. Click **Download**.

You can copy the downloaded files to the machines where you want to install the component.

Verify system requirements

You can find information about system requirements in the Product Availability Matrix (PAM) for Informatica Intelligent Cloud Services.

The PAM indicates the versions of browsers, operating systems, databases, and other types of data sources and targets that a product release supports. You can access the PAM on Informatica Network at https://network.informatica.com/community/informatica-network/product-availability-matrices/.

Verify disk space

Before you run the domain installer, verify the system requirements.

Verify the following the minimum system requirements for a node in the CDI-PC domain:

- Linux or Windows machine to run the CDI-PC Integration Service, CDI-PC Repository Service, and other services.

- 1 CPU with multiple cores
- 6 GB memory
- 50 GB disk space
- 1 GB temporary disk space to run the installer.
- Additional disk space required for updates.
  After you install the domain, it receives automated updates from Informatica Intelligent Cloud Services. These updates require an additional disk space of 10 GB. Plan for additional disk space for updates when you create the domain.
- Verify that you have read, write, and execute permissions on the `/tmp` directory.

Verify sizing requirements

Allocate resources for installation and deployment of services based on the expected deployment type of your environment.

Before you allocate resources, you need to identify the deployment type based on your requirements for the volume of processing and the level of concurrency. Based on the deployment type, you can allocate resources for disk space, cores, and RAM. You can also choose to tune services when you run the installer.

You can create a domain with one node and run the services on the same node or you can create multiple nodes in the domain. When you plan the application services for the domain, consider system requirements based on the services that you run on a node.

Note: Based on workload and concurrency requirements, you might need to optimize performance by adding cores and memory on a node.

The following table lists the minimum system requirements for a node based on some common configuration scenarios:

Services	Processor	Memory	Disk Space
One node runs the following services: - CDI-PC Integration Service - CDI-PC Repository Service - Web Services Hub	2 CPUs with multiple cores	8 GB	15 GB
One node runs the following services: - CDI-PC Integration Service - CDI-PC Repository Service	1 CPU with multiple cores	4 GB	10 GB

The sizing requirements account for the following factors:

- Disk space required to extract the installer
- Temporary disk space to run the installer
- Disk space required to install the services and components
- Disk space required for log directories
- Requirements to run the application services

The sizing numbers don't account for operational data processing and object caching requirements for native mode of execution.

Review patch requirements

Before you run the installer, verify that the Linux machine has the required operating system patches and libraries.

The following table lists the patches required for the different Linux operating systems:

Operating System	Operating System Patch
Red Hat Enterprise Linux 7.3 and later 7.x versions	All of the following packages, where <version> is any version of the package: - e2fsprogs-libs-<version>.el7 - keyutils-libs-<version>.el7 - libselinux-<version>.el7 - libsepol-<version>.el7
Red Hat Enterprise Linux 8.x	All of the following packages, where <version> is any version of the package: - e2fsprogs-libs-<version>.el8 - keyutils-libs-<version>.el8 - libselinux-<version>.el8 - libsepol-<version>.el8

Verify port requirements

The installer sets up the ports for components in the CDI-PC domain, and it designates a range of dynamic ports to use for some services.

You can specify the port numbers to use for the components and a range of dynamic port numbers to use for the application services. You can also use the default port numbers provided by the installer. Verify that the port numbers are available on the machines where you run the installer.

Note: Services and nodes can fail to start if there is a port conflict.

The following table describes the port requirements for installation:

Port	Description
Node port	Port number for the node created during installation. Default is 6005.
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.

Port	Description
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.
Range of dynamic ports for application services	Range of port numbers that can be dynamically assigned to application service processes as they start up. When you start an application service that uses a dynamic port, the Service Manager dynamically assigns the first available port in this range to the service process. The number of ports in the range must be at least twice the number of application service processes that run on the node. Default is 6014 to 6114.
Static ports for application services	Static ports have dedicated port numbers assigned that do not change. When you create the application service, you can accept the default port number, or you can manually assign the port number.

Review the environment variables on Linux

Configure environment variables for the CDI-PC installation on Linux.

The following table describes the environment variables to review:

Variable	Description
IATEMPDIR	Location of the temporary files created during installation. Informatica requires 1 GB disk space for temporary files. Configure the environment variable if you do not want to create temporary files in the `/tmp` directory. If you want to change the default `/tmp` directory, you must set `IATEMPDIR` and `_JAVA_OPTIONS` environment variables to the new directory. For example, set the variable to `export IATEMPDIR=/home/user`. **Note:** Unset the `IATEMPDIR` variable after the installation.
_JAVA _OPTIONS	Configure the environment variable to change the temporary directory. If you want to change the default `/tmp` directory, you must set `IATEMPDIR` and `_JAVA_OPTIONS` the environment variables to the new directory. For example, set the variable to `export _JAVA_OPTIONS=-Djava.io.tmpdir=/home/user`. **Note:** Unset the `_JAVA _OPTIONS` variable after the installation.
LANG and LC_ALL	Change the locale to set the appropriate character encoding for the terminal session. For example, set the encoding to `Latin1` or `ISO-8859-1` for French, `EUC-JP` or `Shift JIS` for Japanese, or `UTF-8` for Chinese or Korean. The character encoding determines the types of characters that appear in the UNIX terminal.
DISPLAY	Unset the `DISPLAY` environment before you run the installer. Installation might fail if the `DISPLAY` environment variable has some value.

Note: Make sure that the `NOEXEC` flag is not set for the file system mounted on the `/tmp` directory.

Verify the file descriptor limit on Linux

Set the file descriptor limit and the maximum user processes. The domain service processes can use a large number of files. To prevent errors that result from the large number of files and processes, you can change system settings with the limit command if you use a C shell, or the ulimit command if you use a Bash shell.

List operating system settings

To get a list of the operating system settings, including the file descriptor limit, run the following command:

With C shell, run `limit`

With Bash shell, run `ulimit -a`

Set the file descriptor limit

Set the file descriptor limit per process to 16,000 or higher. The recommended limit is 32,000 file descriptors per process.

To change system settings, run the limit or ulimit command with the pertinent flag and value. For example, to set the file descriptor limit, run one of the following commands:

With C shell, run `limit -h filesize <value>`

With Bash shell, run `ulimit -n <value>`

Set max user processes

The domain uses a large number of user processes. Use the ulimit -u command to adjust the max user processes setting to a level that is high enough to account for all the processes.

To set the max user processes, run the following command:

With C shell, run `limit -u processes <value>`

With Bash shell, run `ulimit -u <value>`

Prepare the repository databases

The installer prompts you to optionally create some services during the installation. Some service properties require database information. If you want the installer to create a service that requires a database, you must prepare the database before you run the installer. To prepare the databases, verify the data base requirements, set up the database, and set up a user account. The database requirements depend on the services that you create.

If you do not create services during installation, you can create them manually after you install.

Prepare the domain configuration repository database

The domain stores configuration and user information in a relational database called the domain configuration repository.

Set up a database and user account for the domain configuration repository before you run the installation. Verify that the database is accessible to the node in the domain.

When you install the CDI-PC domain, you provide the database and user account information for the domain configuration repository. The installer uses JDBC to communicate with the domain configuration repository.

You can use one of the following databases for the domain configuration repository:

- IBM DB2
- Oracle
- Microsoft SQL Server
- PostgreSQL
- Sybase

Allow 200 MB of disk space for the database.

IBM DB2 database requirements

You can create a domain configuration repository on an IBM DB2 database. Configure the database settings based on requirements specific to the domain configuration repository.

Use the following guidelines when you set up the repository on IBM DB2:

- On the IBM DB2 instance where you create the database, set the following parameters to ON:
  - DB2_SKIPINSERTED
  - DB2_EVALUNCOMMITTED
  - DB2_SKIPDELETED
  - AUTO_RUNSTATS
- On the database, set the following configuration parameters:

Parameter	Value
applheapsz	8192
appl_ctl_heap_sz	8192
logfilsiz	8000
DynamicSections	3000
maxlocks	98
locklist	50000
auto_stmt_stats	ON

- Use a single-node DB2 database tablespace.
- Set the tablespace pageSize parameter to 32768 bytes.

  In a single-partition database, specify a tablespace that meets the pageSize requirements. If you do not specify a tablespace, the default tablespace must meet the pageSize requirements.

  In a multi-partition database, you must specify a tablespace that meets the pageSize requirements. Define the tablespace on a single node.
- Verify the database user has CREATETAB, CONNECT, and BINDADD privileges.

Note: The default value for DynamicSections in DB2 is too low for the Informatica repositories. Informatica requires a larger DB2 package than the default. When you set up the DB2 database for the domain configuration repository or a Model repository, you must set the DynamicSections parameter to at least 3000.

If the DynamicSections parameter is set to a lower number, you can encounter problems when you install or run Informatica. The following error message can appear:

```
[informatica][DB2 JDBC Driver]No more available statements. Please recreate your package
with a larger dynamicSections value.
```

Oracle database requirements

You can create a domain configuration repository on an Oracle database. Configure the database settings based on requirements specific to the domain configuration repository.

Use the following guidelines when you set up the repository on an Oracle database:

- Set the open_cursors parameter to 4000 or higher.
- Set the permissions on the view `$parameter` for the database user.
- Set the privileges for the database user to run *show parameter open_cursors* in the Oracle database. When you run the pre-installation (i10Pi) system check tool, i10Pi runs the command against the database to identify the OPEN_CURSORS parameter with the domain database user credentials.

  You can run the following query to determine the open cursors setting for the domain database user account:

  ```
  SELECT VALUE OPEN_CURSORS FROM V$PARAMETER WHERE UPPER(NAME)=UPPER('OPEN_CURSORS')
  ```
- Verify that the database user has the following privileges:

  CREATE SEQUENCE

  CREATE SESSION

  CREATE SYNONYM

  CREATE TABLE

  CREATE VIEW
- CDI-PC does not support Oracle public synonyms for repository tables. Verify that public synonyms have not been created for any tables in the database.

Microsoft SQL Server database requirements

You can create a domain configuration repository on a Microsoft SQL Server database. Configure the database settings based on requirements specific to the domain configuration repository.

Use the following guidelines when you set up the repository on a Microsoft SQL Server database:

- Set the allow snapshot isolation and read committed isolation level to ALLOW_SNAPSHOT_ISOLATION and READ_COMMITTED_SNAPSHOT to minimize locking contention.
  To set the isolation level for the database, run the following commands:

  ```
  ALTER DATABASE DatabaseName SET ALLOW_SNAPSHOT_ISOLATION ON
  ```

  ```
  ALTER DATABASE DatabaseName SET READ_COMMITTED_SNAPSHOT ON
  ```

  To verify that the isolation level for the database is correct, run the following commands:

  ```
  SELECT snapshot_isolation_state FROM sys.databases WHERE name=[DatabaseName]
  ```

  ```
  SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name = DatabaseName
  ```
- Grant the CONNECT, CREATE TABLE, and CREATE VIEW privileges to the database user account.
- Specify the schema name when you configure the database for the repository.

PostgreSQL database requirements

You can create a domain configuration repository on a PostgreSQL database. Configure the database settings based on requirements specific to the domain configuration repository.

Use the following guidelines when you set up the database on PostgreSQL:

- Verify that the database user account has CONNECT, CREATE TABLE, and CREATE VIEW privileges.
- Specify the database schema name when you use PostgreSQL as the database.
- Ensure that PostgreSQL has sufficient disk space for the data files. By default, the data files are present in the following location:

  `<PostgreSQL installation directory>/data`
- On the database, set the configuration parameters.

  The following table lists the minimum and recommended values for the configuration parameters:

Parameter	Minimum Value	Recommended Value
max_connections	200	4000
shared_buffers	2 GB	16 GB
max_locks_per_transaction	1024	1024
max_wal_size	1 GB	8 GB
checkpoint_timeout	5 minutes	30 minutes

Sybase database requirements

You can create a domain configuration repository on a Sybase database. Configure the database settings based on requirements specific to the domain configuration repository.

Use the following guidelines when you set up the repository on an Sybase database:

- Set the default database for the Sybase database user, else the DefineDomain command fails.
- Set the database server page size to 16K or higher. You must set the page size to 16K as this is a one-time configuration and cannot be changed afterwards.
- Set the database locking configuration to use row-level locking.
  The following table describes the database locking configuration that you must set:

Database Configuration	Sybase System Procedure	Value
Lock scheme	sp_configure "lock scheme"	0, datarows

- Set the Sybase database option "ddl in tran" to TRUE.
- Set "allow nulls by default" to TRUE.
- Turn ON the Sybase database option `select into/bulkcopy/pllsort`. By default, `select into/bulkcopy/pllsort` is turned off in newly created databases.
- Enable the "select" privilege for the sysobjects system table.

- Create the following login script to disable the default VARCHAR truncation:

```
create procedure dbo.sp_string_rtrunc_proc as set string_rtruncation on
sp_modifylogin "user_name", "login script", sp_string_rtrunc_proc
```

  The login script is run every time the user logs into the Sybase instance. The stored procedure sets the parameter at the session level. The sp_modifylogin system procedure updates "user_name" with the stored procedure as its "login script". The user must have permission to invoke the stored procedure.
- Verify that the database user has CREATE DEFAULT, CREATE PROCEDURE, CREATE RULE, CREATE TABLE, and CREATE VIEW privileges.
- Set the database configurations to the recommended baseline values.
  The following table lists the database memory configuration parameters that you must set:

Database Configuration	Sybase System Procedure	Value
Maximum amount of total physical memory	sp_configure "max memory"	2097151
Procedure cache size	sp_configure "procedure cache size"	500000
Number of open objects	sp_configure "number of open objects"	5000
Number of open indexes	sp_configure "number of open indexes"	5000
Number of open partitions	sp_configure "number of open partitions"	5000
Heap memory per user	sp_configure "heap memory per user"	49152
Number of locks	sp_configure "number of locks"	500000

  You can adjust the recommended values according to operations that are performed on the database.

Prepare the CDI-PC repository database

A CDI-PC repository is a collection of database tables containing metadata. A CDI-PC Repository Service manages the repository and performs all metadata transactions between the repository database and repository clients.

You can create a CDI-PC repository on the following database types:

- IBM DB2
- Oracle
- Microsoft SQL Server
- PostgreSQL
- Sybase

Allow 35 MB of disk space for the database.

Note: Install the database client on the machine where you want to run the CDI-PC Repository Service.

For more information about configuring the database, see the documentation for your database system.

IBM DB2 database requirements

You can create a CDI-PC repository on an IBM DB2 database. Configure the database settings based on requirements specific to the CDI-PC repository.

Use the following guidelines when you set up the repository on IBM DB2:

- Set up the database with the tablespace on a single node. When the tablespace is on one node, CDI-PC Client and CDI-PC Integration Service access the repository faster than if the repository tables exist on different database nodes.

  Specify the single-node tablespace name when you create, copy, or restore a repository. If you do not specify the tablespace name, DB2 uses the default tablespace.
- Informatica does not support IBM DB2 table aliases for repository tables. Verify that table aliases have not been created for any tables in the database.

Oracle database requirements

You can create a CDI-PC repository on an Oracle database. Configure the database settings based on requirements specific to the CDI-PC repository.

Use the following guidelines when you set up the repository database:

- Set the storage size for the tablespace to a small number to prevent the repository from using an excessive amount of space. Also verify that the default tablespace for the user that owns the repository tables is set to a small size.

  The following example shows how to set the recommended storage parameter for a tablespace named REPOSITORY:

  ```
  ALTER TABLESPACE "REPOSITORY" DEFAULT STORAGE ( INITIAL 10K NEXT 10K MAXEXTENTS
  UNLIMITED PCTINCREASE 50 );
  ```

  Verify or change the storage parameter for a tablespace before you create the repository.
- Verify that the database user has the following privileges:

  CREATE SEQUENCE

  CREATE SESSION

  CREATE SYNONYM

  CREATE TABLE

  CREATE VIEW
- Verify that the database tables don't use public synonyms.
- You can configure the connection between the domain or the CDI-PC repository and Oracle RAC. Oracle Real Application Clusters (RAC) enables high availability of database applications. The domain and CDI-PC Repository Service are resilient to failover of Oracle RAC databases for all CRUD operations. The following operations in the CDI-PC repository are resilient to the database failover in an Oracle RAC setup:

  - ExecuteQuery
  - ObjectExport
  - ObjectImport
  - PurgeVersion
  - RollbackDeployment

Microsoft SQL Server database requirements

You can create a CDI-PC repository on a Microsoft SQL Server database. Configure the database settings based on requirements specific to the CDI-PC repository.

Use the following guidelines when you set up the repository database:

- Set the database server page size to 8K or higher. This is a one-time configuration and cannot be changed afterwards.
- Verify that the database user account has the CONNECT, CREATE TABLE, and CREATE VIEW privileges.

PostgreSQL database requirements

You can create a CDI-PC repository on a PostgreSQL database. Configure the database settings based on requirements specific to the CDI-PC repository.

Use the following guidelines when you set up the repository database:

- Verify that the database user account has CREATE TABLE and CREATE VIEW privileges.
- Ensure that PostgreSQL has sufficient disk space for the data files. By default, the data files are present in the following location:

  ```
  <PostgreSQL installation directory>/data
  ```

- On the database, set the configuration parameters.

  The following table lists the minimum and recommended values for the configuration parameters:

Parameter	Minimum Value	Recommended Value
max_connections	200	4000
shared_buffers	2 GB	16 GB
max_locks_per_transaction	1024	4000
max_wal_size	1 GB	8 GB
checkpoint_timeout	5 minutes	30 minutes

- To configure the PostgreSQL database for the CDI-PC repository, set values for the PostgreSQL database host, port, and service name for the pg_service.conf file in the following format:

  ```
  [XRS_DB_SERVICE_NAME]
  host=Database host IP
  port=Database port
  dbname=CDI-PC Repository Service database service name
  ```

  Ensure that the entries for the [XRS_DB_SERVICE_NAME] entry matches the information for the CDI-PC Repository Service. To securely connect to PostgreSQL for the CDI-PC repository, set the security property along with the remaining required database properties in the pg_service.conf file in the following format:

  ```
  sslmode=require
  ```

- Set the PGSERVICEFILE environment variable to the location of the pg_service.conf file. The pg_service.conf file contains the connection parameters for PostgreSQL database connection in the prod x installation directory. For example, set the variable as follows:
  Using a Bourne shell:

  ```
  $ export PGSERVICEFILE; PGSERVICEFILE=<pg_service.conf file
  directory>/pg_service.conf
  ```

Using a C shell:

```
$ setenv PGSERVICEFILE <pg_service.conf file
directory>/pg_service.conf
```

Sybase database requirements

You can create a CDI-PC repository on an Sybase database. Configure the database settings based on requirements specific to the CDI-PC repository.

Use the following guidelines when you set up the repository on an Sybase database:

- Set the database server page size to 8K or higher. This is a one-time configuration and cannot be changed afterwards.
- Set the Sybase database option "ddl in tran" to TRUE.
- Set "allow nulls by default" to TRUE.
- Verify the database user has CREATE TABLE and CREATE VIEW privileges.
- Set the database memory configuration requirements.
  The following table lists the memory configuration requirements and the recommended baseline values:

Database Configuration	Sybase System Procedure	Value
Number of open objects	sp_configure "number of open objects"	5000
Number of open indexes	sp_configure "number of open indexes"	5000
Number of open partitions	sp_configure "number of open partitions"	8000
Number of locks	sp_configure "number of locks"	500000

You can adjust the recommended values according to operations that are performed on the database.

Set up a database user account

Set up a database and user account for the repository databases.

Use the following rules and guidelines when you set up the user accounts:

- The database user account must have permissions to create and drop tables, indexes, and views, and to select, insert, update, and delete data from tables.
- Use 7-bit ASCII to create the password for the account.
- To prevent database errors in one repository from affecting any other repository, create each repository in a separate database schema with a different database user account. Do not create a repository in the same database schema as the domain configuration repository or any other repository in the domain.

Create a system user account

Create a user account to run the CDI-PC domain. To migrate from an Informatica domain on the same machine, use the same user account that you used to install Informatica services.

Verify that the user account has write permission on the installation directory.

Verify that the user account does not have any privileges and permissions to access sensitive files on the machine where you install the domain.

Set the database client environment variables

Set environment variables depending on the type of database you use.

The following table lists the environment variables for an IBM DB2 database:

Environment variable	Value
DB2DIR	<database path>
DB2INSTANCE	<DB2InstanceName>
PATH	<database path>/bin
LD_LIBRARY_PATH	<database path>/lib64

The following table lists the environment variables for an Oracle database:

Environment variable	Value
ORACLE_HOME	<Client install database path>
TNS_ADMIN	Set to the location of the tnsnames.ora file:$ORACLE_HOME/network/admin
PATH	<user installation directory>/server/bin:$ORACLE_HOME/bin:$PATH
LD_LIBRARY_PATH	<user installation directory>/server/bin:$Oracle_HOME/lib:$LD_LIBRARY_PATH
INFA_TRUSTSTORE	Set INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD

The following table lists the environment variables for a Microsoft SQL Server database:

Environment variable	Value
ODBCHOME	<User installation directory>/ODBC7.1
ODBCINI	$ODBCHOME/odbc.ini
ODBCINST	$ODBCHOME/odbcinst.ini
PATH	$ODBCHOME/bin:$PATH
LD_LIBRARY_PATH	<user installation directory>/server/bin:$ODBCHOME/lib:$LD_LIBRARY_PATH
INFA_TRUSTSTORE	Set INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD

The following table lists the environment variables for a PostgreSQL database:

Environment Variable	Value
PGSERVICEFILE	Set to the location of the pg_service.conf file: <pg_service.conf file directory>/pg_service.conf
PGHOME	/usr/pgsql -10
PATH	$PGHOME/bin:${PATH}
LD_LIBRARY_PATH	$PGHOME/lib:${LD_LIBRARY_PATH}
INFA_TRUSTSTORE	Set INFA_TRUSTSTORE and INFA_TRUSTSTORE_PASSWORD
POSTGRES_ODBC	Set the value to 1 for the PostgreSQL ODBC connection. You can set it for all the repositories in the domain or for any PostgreSQL repository that uses an ODBC connection.
USE_LIBPQ	Set the value to YES.

The following table lists the environment variables for an Sybase database:

Environment Variable	Value
SYBASE15	<database path>/sybase<version> >
SYBASE_ASE	${SYBASE15}/ASE-<version>
SYBASE_OCS	${SYBASE15}/OCS-<version>
PATH	${SYBASE}/bin:${SYBASE}/${SYBASE_OCS}/bin:${SYBASE}/${SYBASE_ASE}/bin:${SYBASE}/${SYBASE_FTS}/bin:${PATH}
SYBASE_FTS	FTS-16_0
LD_LIBRARY_PATH	${LD_LIBRARY_PATH}:${SYBASE}/${SYBASE_OCS}/lib:${SYBASE}/${SYBASE_ASE}/lib:${SYBASE}/${SYBASE_FTS}/lib

Prepare for Kerberos authentication

You can configure the CDI-PC domain to use Kerberos network authentication to authenticate users, services, and nodes.

Kerberos is a network authentication protocol which uses tickets to authenticate access to services and nodes in a network. Kerberos uses a Key Distribution Center (KDC) to validate the identities of users and services and to grant tickets to authenticated user and service accounts. In the Kerberos protocol, users and services are known as principals. The KDC has a database of principals and their associated secret keys that are used as proof of identity. Kerberos can use an LDAP directory service as a principal database.

To use Kerberos authentication, you must install and run the CDI-PC domain on a network that uses Kerberos network authentication. CDI-PC can run on a network that uses Kerberos authentication with Microsoft Active Directory service as the principal database.

The CDI-PC domain requires keytab files to authenticate nodes and services in the domain without transmitting passwords over the network. The keytab files contain the service principal names (SPN) and associated encrypted keys. Create the keytab files before you create nodes and services in the CDI-PC domain.

Set up the Kerberos configuration file

Kerberos stores configuration information in a file named *krb5.conf*. CDI-PC requires specific properties set in the Kerberos configuration file so that the CDI-PC domain can use Kerberos authentication correctly. You must set the properties in the krb5.conf configuration file.

The configuration file contains the information about the Kerberos server, including the Kerberos realm and the address of the KDC. You can request the Kerberos administrator to set the properties in the configuration file and send you a copy of the file.

1. Back up the krb5.conf file before you make any changes.
2. Edit the krb5.conf file.
3. In the *libdefaults* section, set or add the properties required by CDI-PC.

   The following table lists the values to which you must set properties In the libdefaults section:

Parameter	Value
default_realm	Name of the service realm for the CDI-PC domain.
forwardable	Allows a service to delegate client user credentials to another service. Set this parameter to **True**. The CDI-PC domain requires application services to authenticate the client user credentials with other services.
default_tkt_enctypes	Encryption types for the session key in ticket-granting tickets (TGT). Set this parameter only if session keys must use specific encryption types. Set the following encryption types: - default_tkt_enctypes = aes256-cts-hmac-sha1-96 - default_tgs_enctypes = aes256-cts-hmac-sha1-96 - permitted_enctypes = aes256-cts-hmac-sha1-96
udp_preference_limit	Determines the protocol that Kerberos uses when it sends a message to the KDC. Set udp_preference_limit = 1 to always use TCP. The CDI-PC domain supports only the TCP protocol. If the udp_preference_limit is set to any other value, the CDI-PC domain might shut down unexpectedly.

4. In the *realms* section, include the port number in the address of the KDC separated by a colon.

   For example, if the KDC address is <kdc server ip address> and the port number is 88, set the *kdc* parameter to the following:

   ```
   kdc = <kdc server ip address>:88
   ```

5. Save the krb5.conf file.
6. Store the krb5.conf file in a directory that is accessible to the machine where you plan to install the CDI-PC services.

   When you configure a domain to use Kerberos cross-realm authentication, you add properties for each Kerberos realm to the Kerberos configuration file. You also include the name of each realm when you run infasetup commands to enable Kerberos authentication in the domain and on domain nodes.

The following example shows the content of a krb5.conf with the required properties:

```
[libdefaults]
default_realm = AFNIKRB.AFNIDEV.COM
forwardable = true
udp_preference_limit = 1

[realms]
AFNIKRB.AFNIDEV.COM = {
  admin_server = SMPLKERDC01.AFNIKRB.AFNIDEV.COM
  kdc = SMPLKERDC01.AFNIKRB.AFNIDEV.COM:88
 }

[domain_realm]
afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
.afnikrb.afnidev.com = AFNIKRB.AFNIDEV.COM
```

For more information about the Kerberos configuration file, see the Kerberos network authentication documentation.

Generate the service principal and keytab file name format

If you run the CDI-PC domain with Kerberos authentication, you must associate Kerberos service principal names (SPN) and keytab files with the nodes and processes in the CDI-PC domain. CDI-PC requires keytab files to authenticate services without requests for passwords.

Based on the security requirements for the domain, you can set the service principal level to one of the following levels:

Node level

If the domain is used for testing or development and does not require a high level of security, you can set the service principal at the node level. You can use one SPN and keytab file for the node and all the service processes on the node. You must also set up a separate SPN and keytab file for the HTTP processes on node.

Process level

If the domain is used for production and requires a high level of security, you can set the service principal at the process level. Create a unique SPN and keytab file for each node and each process on the node. You must also set up a separate SPN and keytab file for the HTTP processes on node.

The CDI-PC domain requires the service principal and keytab file names to follow a specific format. To ensure that you follow the correct format for the service principal and keytab file names, use the CDI-PC Kerberos SPN Format Generator to generate a list of the service principal and keytab file names in the format required by the CDI-PC domain.

The CDI-PC Kerberos SPN Format Generator is shipped with the CDI-PC services installer.

Service principal requirements at node level

If the CDI-PC domain does not require a high level of security, the node and service processes can share the same SPNs and keytab files. The domain does not require a separate SPN for each service process in a node.

The CDI-PC domain requires SPNs and keytab files for the following components at node level:

Principal distinguished name (DN) for the LDAP directory service

Principal name for the bind user DN that is used to search the LDAP directory service. The name of the keytab file must be `infa_ldapuser.keytab`.

Node process

Principal name for the CDI-PC node that initiates or accepts authentication calls. The same principal name is used to authenticate the services in the node. Each gateway node in the domain requires a separate principal name.

HTTP processes in the domain

Principal name for all web application services in theCDI-PC domain, including CDI-PC Administrator. The browser uses this principal name to authenticate with all HTTP processes in the domain. The name of the keytab file must be `webapp_http.keytab`.

Service principal requirements at process level

If the CDI-PC domain requires a high level of security, create a separate SPN and keytab file for each node and each service in the node.

The CDI-PC domain requires SPNs and keytab files for the following components at process level:

Principal distinguished name (DN) for the LDAP directory service

Principal name for the bind user DN that is used to search the LDAP directory service. The name of the keytab file must be `infa_ldapuser.keytab`.

Node process

Principal name for the CDI-PC node that initiates or accepts authentication calls.

CDI-PC Administrator service

Principal name for the CDI-PC Administrator service that authenticates the service with other services in the CDI-PC domain. The name of the keytab file must be*_AdminConsole.keytab*.

HTTP processes in the domain

Principal name for all web application services in the CDI-PC domain, including CDI-PC Administrator. The browser uses this principal name to authenticate with all HTTP processes in the domain. The name of the keytab file must be `webapp_http.keytab`.

Service process

Principal name for the service that runs on a node in the CDI-PC domain. Each service requires a unique service principal and keytab file name.

You do not need to create the SPNs and keytab files for the services before you run the installer. You can create the SPN and keytab file for a service when you create the service in the domain. The SPN and keytab file for a service must be available when you enable the service.

Running the SPN Format Generator

You can run the CDI-PC Kerberos SPN Format Generator to generate a file that shows the correct format for the SPNs and keytab file names required in the CDI-PC domain.

You can run the SPN Format Generator from the command line or from the CDI-PC installer. The SPN Format Generator generates a file with the names of the service principal and keytab files based on the parameters you provide.

Note: Verify that the information you provide is correct. The SPN Format Generator does not validate the values you enter.

1. On the machine where you extracted the installation files, go to the following directory: `<CDI-PC installation files directory>/Server/Kerberos`
2. On a shell command line, run the `SPNFormatGenerator` file.
3. Press **Enter** to continue.

4. In the **Service Principal Level** section, select the level at which to set the Kerberos service principals for the domain. Select either process level or node level.
5. Enter the domain and node parameters required to generate the SPN format.
   a. Domain name. Name of the domain. The name must not exceed 128 characters and must be 7-bit ASCII only. It cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
   b. Node name. Name of the CDI-PC node.
   c. Node host name. Fully qualified host name or the IP address of the machine on which to create the node. The node host name cannot contain the underscore (_) character. Do not use localhost. The host name must explicitly identify the machine.
   d. Service realm name. Name of the Kerberos realm for the CDI-PC domain services. The realm name must be in uppercase.

   If you set the service principal at node level, the prompt **Add Node?** appears. If you set the service principal at process level, the prompt **Add Service?** appears.
6. At the **Add Node?** prompt, enter 1 to generate the SPN format for an additional node. Then enter the node name and node host name.
   To generate the SPN formats for multiple nodes, enter 1 at each **Add Node?** prompt and enter a node name and node host name.
7. At the **Add Service?** prompt, enter 1 to generate the SPN format for a service that will run on the preceding node. Then enter the service name.
   To generate the SPN formats for multiple services, enter 1 at each **Add Service?** prompt and enter a service name.
8. Enter 2 to end the **Add Service?** or **Add Node?** prompts.
   The SPN Format Generator displays the path and file name of the file that contains the list of service principal and keytab file names.
9. Press **Enter** to exit the SPN Format Generator.
   The SPN Format Generator generates a text file that contains the SPN and keytab file names in the format required for the CDI-PC domain.

Review the SPN and keytab format text file

The Kerberos SPN Format Generator generates a text file named `SPNKeytabFormat.txt` that lists the format for the service principal and keytab file names required by the CDI-PC domain. The list includes the SPN and keytab file names based on the service principal level you select.

Review the text file and verify that there are no error messages.

The text file contains the following information:

Entity Name

Identifies the node or service associated with the process.

SPN

Format for the SPN in the Kerberos principal database. The SPN is case sensitive. Each type of SPN has a different format.

An SPN can have one of the following formats:

Keytab Type	SPN Format
NODE_SPN	isp/<*NodeName*>/<*DomainName*>@<*REALMNAME*>
NODE_AC_SPN	_AdminConsole/<*NodeName*>/<*DomainName*>@<*REALMNAME*>
NODE_HTTP_SPN	HTTP/<*NodeHostName*>@<*REALMNAME*> **Note:** The Kerberos SPN Format Generator validates the node host name. If the node host name is not valid, the utility does not generate an SPN. Instead, it displays the following message: Unable to resolve host name.
SERVICE_PROCESS_SPN	<*ServiceName*>/<*NodeName*>/<*DomainName*>@<*REALMNAME*>

Keytab File Name

Format for the name of the keytab file to be created for the associated SPN in the Kerberos principal database. The keytab file name is case sensitive.

The keytab file names use the following formats:

Keytab Type	Keytab File Name
NODE_SPN	<*NodeName*>.keytab
NODE_AC_SPN	_AdminConsole.keytab
NODE_HTTP_SPN	webapp_http.keytab
SERVICE_PROCESS_SPN	<*ServiceName*>.keytab

Keytab Type

Type of the keytab. The keytab type can be one of the following types:

- NODE_SPN. Keytab file for a node process.
- NODE_AC_SPN. Keytab file for the CDI-PC Administrator service process.
- NODE_HTTP_SPN. Keytab file for HTTP processes in a node.
- SERVICE_PROCESS_SPN. Keytab file for a service process.

Service Principals at Node Level

The following example shows the contents of the SPNKeytabFormat.txt file generated for service principals at the node level:

```
ENTITY_NAME   SPN                                              KEY_TAB_NAME
KEY_TAB_TYPE
Node01        isp/Node01/InfaDomain@MY.SVCREALM.COM            Node01.keytab
NODE_SPN
Node01        HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM   webapp_http.keytab
NODE_HTTP_SPN
Node02        isp/Node02/InfaDomain@MY.SVCREALM.COM            Node02.keytab
NODE_SPN
Node02        HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM   webapp_http.keytab
NODE_HTTP_SPN
Node03        isp/Node03/InfaDomain@MY.SVCREALM.COM            Node03.keytab
NODE_SPN
```

```
Node03        HTTP/NodeHost03.enterprise.com@MY.SVCREALM.COM     webapp_http.keytab
NODE_HTTP_SPN
```

Service Principals at Process Level

The following example shows the contents of the SPNKeytabFormat.txt file generated for service principals at the process level:

```
ENTITY_NAME         SPN
KEY_TAB_NAME            KEY_TAB_TYPE
Node01              isp/Node01/InfaDomain@MY.SVCREALM.COM
Node01.keytab           NODE_SPN
Node01              _AdminConsole/Node01/InfaDomain@MY.SVCREALM.COM
_AdminConsole.keytab    NODE_AC_SPN
Node01              HTTP/NodeHost01.enterprise.com@MY.SVCREALM.COM
webapp_http.keytab      NODE_HTTP_SPN
Node02              isp/Node02/InfaDomain@MY.SVCREALM.COM
Node02.keytab           NODE_SPN
Node02              _AdminConsole/Node02/InfaDomain@MY.SVCREALM.COM
_AdminConsole.keytab    NODE_AC_SPN
Node02              HTTP/NodeHost02.enterprise.com@MY.SVCREALM.COM
webapp_http.keytab      NODE_HTTP_SPN
Service10:Node01    Service10/Node01/InfaDomain@MY.SVCREALM.COM
Service10.keytab        SERVICE_PROCESS_SPN
Service100:Node02   Service100/Node02/InfaDomain@MY.SVCREALM.COM
Service100.keytab       SERVICE_PROCESS_SPN
Service200:Node02   Service200/Node02/InfaDomain@MY.SVCREALM.COM
Service200.keytab       SERVICE_PROCESS_SPN
```

Create the service principal names and keytab files

After you generate the list of SPN and keytab file names in CDI-PC format, send a request to the Kerberos administrator to add the SPNs to the Kerberos principal database and create the keytab files. Enable 256-bit encryption for each user account that you use to generate the keytab files.

Use the following guidelines when you create the SPN and keytab files:

The user principal name (UPN) must be the same as the SPN.

When you create a user account for the service principal, you must set the UPN with the same name as the SPN. The application services in the CDI-PC domain can act as a service or a client depending on the operation. You must configure the service principal to be identifiable by the same UPN and SPN.

A user account must be associated with only one SPN. Do not set multiple SPNs for one user account.

Enable delegation in Microsoft Active Directory.

You must enable delegation for all user accounts with service principals used in the CDI-PC domain. In the Microsoft Active Directory Service, set the **Trust this user for delegation to any service (Kerberos only)** option for each user account that you set an SPN.

Delegated authentication happens when a user is authenticated with one service and that service uses the credentials of the authenticated user to connect to another service. Because services in the CDI-PC domain need to connect to other services to complete an operation, the CDI-PC domain requires the delegation option to be enabled in Microsoft Active Directory.

Use the ktpass utility to create the service principal keytab files.

Microsoft Active Directory supplies the ktpass utility to create keytab files. CDI-PC supports Kerberos authentication only on Microsoft Active Directory and has certified only keytab files that are created with ktpass.

The keytab files for a node must be available on the machine that hosts the node. By default, the keytab files are stored in the following directory: `<CDI-PC installation directory>/isp/config/keys`. During installation, you can specify a directory on the node to store the keytab files.

When you receive the keytab files from the Kerberos administrator, copy the keytab files to a directory that is accessible to the machine where you plan to install the CDI-PC services. When you run the CDI-PC installer, specify the location of the keytab files. The CDI-PC installer copies the keytab files to the directory for keytab files on the CDI-PC node.

Set up keystore and truststore files

When you create the domain, you configure secure communication for the domain and set up a secure connection to Informatica Administrator (the Administrator tool) and the Secure Agent. You use custom TLS certificates to configure secure configuration. To use custom certificates, set up keystore and truststore files.

Set up files for secure communication within the CDI-PC domain and for a secure connection to the Administrator tool and Secure Agent. CDI-PC requires certificates configured for host name validation. Ensure that the host name mentioned in the certificate matches the host that you apply it on. To create the required files, you can use the following programs:

keytool

You can use keytool to create a TLS certificate or a Certificate Signing Request (CSR) as well as keystores and truststores in JKS format.

OpenSSL

You can use OpenSSL to create a TLS certificate or CSR as well as convert a keystore in JKS format to PEM format.

For more information about OpenSSL, see the documentation on the following website: https://www.openssl.org/docs/

For a higher level of security, send your CSR to a Certificate Authority (CA) to get signed certificates. If you use CA-signed certificates, you get a certificate chain with an ordered list of certificates that include the root certificate, one or more intermediate certificates, and the user certificate. Enter all certificates in the chain when you generate the PEM format.

For information about how to generate and configure custom keystore and truststore certificates, see the following KB article: Configure keystore and truststore for Cloud Data Integration for PowerCenter

The software available for download at the referenced links belongs to a third party or third parties, not Informatica. The download links are subject to the possibility of errors, omissions or change. Informatica assumes no responsibility for such links and/or such software, disclaims all warranties, either express or implied, including but not limited to, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and disclaims all liability relating thereto.

Secure communication within the domain

Before you enable secure communication within the domain, verify that the following requirements are met:

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

Note that RSA encryption requires more than 512 bits.

You have a signed TLS certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into keystores.

Ensure that you have keystores in the following formats:

- PEM format, named infa_keystore.pem
- JKS format, named infa_keystore.jks

If you use CA-signed certificates, ensure that the keystore files contain the root and intermediate TLS certificates.

Note: Use the same password for the keystore in JKS format and the private key pass phrase used to generate the TLS certificate.

You imported the certificate into truststores.

Ensure that you have truststores in the following formats:

- PEM format, named infa_truststore.pem
- JKS format, named infa_truststore.jks

Ensure that the truststore files contain the root, intermediate, and end user TLS certificates.

The keystores and truststores are in the correct directory.

Ensure that the keystore and truststore are in a directory that is accessible to the installer.

Secure connection to the Administrator tool

Before you secure the connection to the Administrator tool, verify that the following requirements are met:

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

Note that RSA encryption requires more than 512 bits.

You have a signed TLS certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into a keystore in JKS format.

A keystore can't contain more than one certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate. Alternatively, you can use a shared certificate and keystore.

Validate the certificates with the TLS utility

CDI-PC requires valid custom keystore and truststore certificates to secure communication between Informatica Intelligent Cloud Services and the domain, and between the domain and clients. The TLS utility verifies that the certificates are valid for communication between two hosts. You can choose to run the utility to validate your certificates.

1. Download the TLS utility from Informatica Intelligent Cloud Services.

   For information about how to download the utility, see "Download the installers from Informatica Intelligent Cloud Services" on page 11

2. Copy the certificates that you want to validate to the same machine.

   After you validate the certificates, you can copy them to the host machine.

3. Extract the ZIP file to any location on the machine.

4. Open a command prompt from the directory where you extracted the utility, and run the following command to start the utility:

   ```
   java -jar CDI-PC_TLS_Utility.jar
   ```

   The utility prompts you for the details of the first host.

5. Enter certificate details of the domain, Secure Agent, or CDI-PC Client machine.

   If you have multiple domain nodes or multiple Secure Agents, enter the certificate details of all the domain, Secure Agent, or CDI-PC Client machines.

6. Enter the following details for the first host and press **Enter** after each entry:

   - First host keystore path. The absolute path to the keystore file on the first host.
   - First host keystore password. The keystore password.
   - First host truststore path. The absolute path to the truststore file on the first host.
   - First host truststore password. The keystore password.
   - First host DNS or IP address. The DNS or IP address of the host on which you use the certificate. If you enter the DNS, enter the fully qualified host name and the short name of the host. Enter comma-separated values. If the certificate includes wildcards in the host details, enter the DNS information for each host on which you use the certificate.

7. Enter the details for the second host.

   With details of both hosts, the utility tries to connect from the first host to the second host and verifies the host entries in the certificates against details entered. If the second host certificates are present on the first host and host entries are validated, the utility returns a message to indicate that the validation is successful.

8. If the certificates of the second host are not present in the truststore of the first host, you can choose whether you want the utility to import the certificates. The import modifies the truststore of the first host. Enter `Y` to import the certificates and continue or `N` to exit.

   If you choose to import the certificates, the utility imports the certificates and continues the validation.

9. The utility then tries to connect from the second host to the first host. If connection and host entry verification succeed, the utility returns a successful validation message. You might be prompted to import the certificates of the first host into the second host if they aren't present in the truststore of the second host.

   If connection and host entry verification succeed, the utility returns a successful validation message.

You can view detailed information in the tlscertificateutils.log file generated in the following location:
`<utility installation directory>/logs`

Configuring the TLS utility in silent mode

Complete the following configurations in the installation properties file to add more than one node or Secure Agents while defining the domain security properties:

- To configure a domain with multiple Secure Agents, add the following parameter and set it's value to the number of Secure Agents:

  ```
  NUMBER_OF_SECURE_AGENT= <number of Secure Agents>
  ```

- Add extra keystore and truststore file details based on the number of Secure Agents.

  ```
  DMA_KEYSTORE_FILE_1=
  DMA_KEYSTORE_PASSWORD_1=
  DMA_TRUSTSTORE_FILE_1=
  DMA_TRUSTSTORE_PASSWORD_1=
  DMA_HOST_DETAILS_1=
  ```

Import the CDI-PC domain truststore certificates to the Secure Agent truststore

Put the domain certificates on the Secure Agent machine to ensure that the Secure Agent can communicate with the domain.

If you ran the TLS utility to validate your certificates, you don't need to perform this task. The TLS utility validates the certificates and verifies that the domain and the Secure Agent can communicate. The verification process exchanges the certificates if they aren't already present.

To import the CDI-PC domain certificates to the Secure Agent truststore, run the following command:

```
keytool -importcert -file <absolute path to the domain certificate file>.crt -keystore
<JKS Truststore name>.jks -alias <Any other alias name> -deststoretype JKS -v -
trustcacerts
```

Run the pre-installation system check tool

Run the **Pre-Installation (i10Pi) System Check Tool** before you install CDI-PC.

The **Pre-Installation (i10Pi) System Check Tool** verifies whether a machine meets the system requirements for the CDI-PC installation. Informatica recommends that you verify the minimum system requirements before you start the installation. When you run the system check tool before you perform the installation, the installer sets fields for certain fields, such as the database connection and domain port numbers, based on the information that you enter during the system check.

Run the pre-installation system check tool in console mode

Run the Pre-installation (i10Pi) System Check Tool to verify whether the machine meets the system requirements for installation.

Ensure that you verified the minimum system requirements and prepared the domain configuration repository database.

1. Log in to the machine with a system user account.
2. Close all the other applications.
3. On a shell command line, run the install file.

   The installer displays the message to verify that the locale environment variables are set.
4. If the environment variables are not set, press **n** to exit the installer and set them as required.

   If the environment variables are set, press **y** to continue.
5. Press **1** to install CDI-PC.
6. Press **1** to run the Pre-Installation (i10Pi) System Check Tool that verifies whether the machine meets the system requirements for the installation.
7. On the Informatica Pre-Installation (i10Pi) System Check Tool **Welcome** section, press **Enter**.

   The **System Information** section appears.
8. Enter the absolute path for the installation directory.

The directory names in the path can't contain spaces or the following special characters: ` % * + ; \ / " ? , < > @ # ! %) (} {] [' | &

Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

9. Press **Enter**.
10. Enter the starting port number for the node that you will create on the machine. The default port number for the node is 6005.
11. Press **Enter**.

    The **Database and JDBC Connection Information** section appears.
12. Configure the database for the domain configuration repository.

    Choose the database type and enter the database user ID and password. Select 1 for Oracle, 2 for Microsoft SQL Server, 3 for IBM DB2, 4 for Sybase, and 5 for PostgreSQL.
13. To connect to a secure database, select **1**. Select **2** if you do not want to provide secure parameters in a custom connection string.

    If you select **1**, include the security parameters in addition to the connection parameters.
14. To enter the JDBC connection information using the JDBC URL information, press **1**. To enter the JDBC connection information using a custom JDBC connection string, press **2**.

    To connect to a secure database, enter the JDBC connection using a custom JDBC connection string.
15. Enter the JDBC connection information.

    - To enter the connection information using a custom JDBC connection string, type the connection string and specify the connection parameters.
      Use the following syntax in the JDBC connection string:
      IBM DB2

      ```
      jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
      ```

      Oracle

      ```
      jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
      ```

      Microsoft SQL Server

      ```
      jdbc:Informatica:sqlserver://<host name>:<port
      number>;SelectMethod=cursor;DatabaseName=
      ```

      PostgreSQL

      ```
      jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
      ```

      Sybase

      ```
      jdbc:Informatica:sybase://<host name>:<port number>;DatabaseName=
      ```

      Verify that the connection string contains all the connection parameters required by your database system.
    - To enter the connection information using the JDBC URL information, specify the JDBC URL properties.

The following table describes the connection information:

Prompt	Description
Database host name	Host name for the database server.
Database port number	Port number for the database.
Database service name	Service name for Oracle databases, or database name for Microsoft SQL Server and PostgreSQL databases.

The tool checks the settings of the hard drive, the availability of the ports, and the configuration of the database. After the system check is complete, the **System Check Summary** section displays the results of the system check.

16. Analyze the results of the system check.

    Each requirement is listed, along with one of the following check statuses:

    - [Pass] - The requirement meets the criteria for the installation.
    - [Fail] - The requirement doesn't meet the criteria for the installation. Resolve the issue before you proceed with the installation.
    - [Information] - Verify the information and perform any additional tasks as outlined in the details.

    The results of the system check are saved to the following file: `<installer directory>/Server/I10PI/I10PI/en/I10PI_summary.txt`

17. Press **Enter** to close the Pre-Installation (i10Pi) System Check Tool.

If the Pre-Installation (i10Pi) System Check Tool finishes with failed requirements, resolve the failed requirements and run the Pre-Installation (i10Pi) System Check Tool again. You can still perform the installation. However, Informatica recommends that you resolve the failed requirements before you proceed.

Run the pre-installation system check tool in graphical mode

Run the Pre-installation (i10Pi) System Check Tool to verify whether the machine meets the system requirements for installation.

Ensure that you verified the minimum system requirements and prepared the domain configuration repository database.

1. Log in to the machine with a system user account.
2. Close all the other applications.
3. Go to the root of the directory that contains the installation files and run `install.bat` as administrator.
4. Select **Install CDI-PC**.
5. Select **Run the Pre-Installation (i10Pi) System Check Tool** to verify whether the machine meets the system requirements for the installation.
6. Click **Start**.

   The Informatica Pre-Installation (i10Pi) System Check Tool **Welcome** page appears.
7. Click **Next**.

   The **System Information** page appears.
8. Enter the absolute path for the installation directory.

The directory names in the path can't contain spaces or the following special characters: ` % * + ; \ / " ? , < > @ # ! %) (} {] [' | &

Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

9. Enter the starting port number for the node that you will create or upgrade on the machine. The default port number for the node is 6005.
10. Click **Next**.

    The **Database and JDBC Connection Information** page appears.
11. Enter the information for the domain configuration repository database.

    The following table describes the properties that you specify for the database and user account:

Property	Description
Database Type	Database for the repository. Select one of the following databases: - IBM DB2 - Microsoft SQL Server - Oracle - PostgreSQL - Sybase
Database User ID	User account for the repository database.
User Password	Password for the database user account.

    Note: The domain configuration repository must be accessible to all gateway nodes in the domain. Specify tablespace properties for IBM DB2 and schema properties for Microsoft SQL Server.
12. If you plan to use a secure database for the domain configuration repository, select **secure database parameters**.
13. Enter the database connection information.
    - To enter the connection information using the JDBC URL information, select **JDBC URL** and specify the JDBC URL properties.

The following table describes the JDBC URL properties that you need to specify:

Property	Description
Database Address	Host name and port number for the database in the format `host_name:port_no`.
Database Service Name	Service or database name: - IBM DB2. Enter the service name. - Oracle. Enter the service name. - Microsoft SQL Server. Enter the database name. - PostgreSQL. Enter the database name. - Sybase. Enter the database name.
JDBC Parameters	Optional parameters for the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

- To connect to a secure database, enter the JDBC connection using a custom JDBC connection string. To enter the connection information using a custom JDBC connection string, type the connection string and specify the connection parameters.
  Use the following syntax in the JDBC connection string:
  IBM DB2

  ```
  jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=
  ```

  Oracle

  ```
  jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=
  ```

  Microsoft SQL Server

  ```
  jdbc:Informatica:sqlserver://<host name>:<port
  number>;SelectMethod=cursor;DatabaseName=
  ```

  PostgreSQL

  ```
  jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=
  ```

  Sybase

  ```
  jdbc:Informatica:sybase://<host name>:<port number>;DatabaseName=
  ```

  Verify that the connection string contains all the connection parameters required by your database system.

14. Click **Test Connection** to verify that you can connect to the database, and then click **OK** to continue.
15. Click **Next** to start the system check.

    The tool checks the settings of the hard drive, availability of the ports, and configuration of the database. After the system check is complete, the **System Check Summary** page appears that displays the results of the system check.
16. Analyze the results of the system check.

    Each requirement is listed along with one of the following check statuses:

    - [Pass] - The requirement meets the criteria for the installation.

- [Fail] - The requirement doesn't meet the criteria for the installation. Resolve the issue before you proceed with the installation.
- [Information] - Verify the information and perform any additional tasks as outlined in the details.

The results of the system check are saved to the following file: `<installation directory>/Server/I10PI/I10PI/en/I10PI_summary.txt`

17. Click **Done** to close the Pre-Installation (i10Pi) System Check Tool.

If the Pre-Installation (i10Pi) System Check Tool finishes with failed requirements, resolve the failed requirements and run the Pre-Installation (i10Pi) System Check Tool again. While you can perform the installation without fixing the failed requirements, Informatica recommends that you resolve the failed requirements before you proceed.

Run the pre-installation system check tool in silent mode

Run the Pre-installation (i10Pi) System Check Tool in silent mode to verify system requirements for installation without user intervention.

1. Extract the CDI-PC installer file.
2. Navigate to the following location:

   `<CDI-PC installation directory>/Server/I10PI`
3. To specify the properties for I10Pi in silent mode, update the SilentInput.properties file in the `I10PI` folder.
4. To run i10Pi in silent mode, run the `silentInstall` file in the `I10PI` folder.

   The results of the system check are saved to the I10PI_summary.txt file in the following location: `<installer directory>/Server/I10PI/I10PI/en`

If the Pre-Installation (i10Pi) System Check Tool finishes based on failed requirements, resolve the failed requirements and run the Pre-Installation (i10Pi) System Check Tool again. You can still perform the installation. However, Informatica recommends that you resolve the failed requirements before you proceed.

CHAPTER 3

Installing Secure Agents

You can install Secure Agents on Windows or Linux.

Install the Secure Agent on Linux

The Secure Agent on Linux runs as a process. You can use a shell command line to install, register, start, stop, and uninstall the Secure Agent.

You can also use the shell command line to check the Secure Agent status.

When you install a Secure Agent, you perform the following tasks:

1. Verify that the machine meets the minimum requirements.
2. Download the Secure Agent installer files.
3. Install and register the Secure Agent.

Consider the following guidelines:

- Create a user profile to install the Secure Agent with full access to all folders from the Secure Agent installation directory.
- If the machine already has a Secure Agent installed, verify that you install the Secure Agent with a different Linux user account.
- Verify that you install the Secure Agent on a machine that isn't running the CDI-PC domain.

For more information about Secure Agent requirements, see Best Practices for Installing the Secure Agent.

Secure Agent requirements on Linux

You can install the Secure Agent on any machine that has internet connectivity and can access Informatica Intelligent Cloud Services. Before you install the Secure Agent on Linux, verify the system requirements.

Verify the following requirements before you install the Secure Agent on Linux:

- Verify that the machine uses a supported operating system.
- Verify that the machine has at least 15 GB of free disk space. CDI-PC requires 5 GB for installation and 10 GB for automated updates.
- Verify that the `libidn.x86_64` package is installed.
  If it isn't installed, install it using the following command: `sudo yum install libidn.x86_64`

  Note: The command to install the package might vary based on your Linux distribution.
- Ensure that ports in the default port range 14000 - 14999 are open on the machine.

For more information about Secure Agent requirements, see this article:
https://knowledge.informatica.com/s/article/526096

Configure the firewall

If your organization uses a protective firewall, include the Informatica Intelligent Cloud Services domain name or IP address ranges in the list of approved domain names or IP addresses. To ensure that the Secure Agent can perform all necessary tasks through the firewall, enable the port that the Secure Agent uses.

The Secure Agent uses port 443 (HTTPS) to connect to the internet. Configure your firewall to allow traffic to pass over port 443.

The allowlists of domains and IP addresses can vary according to your data center, which is also called a POD (Point of Deployment). You can identify your POD through the URL that appears when you open any service in Informatica Intelligent Cloud Services. The first few characters of the URL string identify the POD. For example, if the URL starts with `usw3.dm-us.informaticacloud.com`, your POD is USW3.

For the allowlists of Informatica Intelligent Cloud Services domains and IP addresses for different PODs, see Pod Availability and Networking in the documentation portal or click the link at the top of the **Runtime Environments** page in Administrator.

Downloading and installing the Secure Agent on Linux

To install the Secure Agent on a Linux machine, you must download and run the Secure Agent installation program and then register the agent.

Secure Agent registration requires an install token. To get the install token, copy the token when you download the agent or use the **Generate Install Token** option in Administrator. The token expires after 24 hours.

When you register the agent, it is added to its own Secure Agent group by default. You can add the agent to a different Secure Agent group.

Before you download and install the Secure Agent, verify that no other Secure Agent is installed on the machine using the same Linux user account. If there is, you must uninstall it.

Tip: To verify the checksum of the Secure Agent installation program, use the agent REST API version 2 resource. For more information about the agent resource, see *REST API Reference*.

1. Open Administrator and select **Runtime Environments**.
2. On the **Runtime Environments** page, click **Download Secure Agent**.
3. Select the Linux 64-bit operating system platform, copy the install token, and then click **Download**.

   The installation program is downloaded to your machine. The name of the installation program is `agent64_install_ng_ext.<agent core version>.bin`.
4. Save the installation program to a directory on the machine where you want to run the Secure Agent.

   Note: If the file path contains spaces, the installation might fail.
5. From a shell command line, navigate to the directory where you downloaded the installation program and enter the following command:

   ```
   ./agent64_install_ng_ext.bin -i console
   ```
6. When the installer completes, navigate to the following directory:

   ```
   <Secure Agent installation directory>/apps/agentcore
   ```
7. To start the Secure Agent, enter the following command:

   ```
   ./infaagent startup
   ```

The Secure Agent Manager starts. You must register the agent using the user name that you use to access Informatica Intelligent Cloud Services. You must also supply the install token.

8. If you did not copy the install token when you downloaded the agent, click **Generate Install Token** on the **Runtime Environments** page in Administrator, and copy the token.
9. To register the agent, in the `<Secure Agent installation directory>/apps/agentcore` directory, enter one of the following commands using your Informatica Intelligent Cloud Services user name and the token that you copied:
   - To add the agent to its own Secure Agent group, use the following command:

     ```
     ./consoleAgentManager.sh configureToken <user name> <install token>
     ```

   - To add the agent to an existing Secure Agent group, use the following command:

     ```
     ./consoleAgentManager.sh configureTokenWithRuntime <user name> <install token>
     <Secure Agent group name>
     ```

     Note: If the command includes a Secure Agent group name that doesn't exist, the Secure Agent is not assigned to a group. Be sure to use a valid Secure Agent group name.

   The following table lists the command options:

Option	Description
User Name	Required. Informatica Intelligent Cloud Services user name of the user installing the Secure Agent.
Install Token	Required. The install token that you copied.
Secure Agent group name	Optional. Include when you want to add the agent to an existing Secure Agent group instead. If this option isn't included in the command, the agent will be in its own Secure Agent group.

   You can check the registration status of a Secure Agent using the following command:

   ```
   ./consoleAgentManager.sh isConfigured
   ```

Install the Secure Agent on Windows

On Windows, the Secure Agent runs as a Windows service. When you install the Secure Agent, you also install the Informatica Cloud Secure Agent Manager.

By default, the Secure Agent starts when you start Windows. You can stop and restart the Secure Agent using the Secure Agent Manager or Windows Services. If you install the Secure Agent on a different volume than the one that you use to run the installation program, you must start and stop the Secure Agent from Windows Services.

You can also use the Secure Agent Manager to check the Secure Agent status and configure proxy information. The Secure Agent works with BASIC, DIGEST, and NTLMv2 proxy authentication.

You can launch the Secure Agent Manager from the Start menu or desktop icon. When you close the Secure Agent Manager, it minimizes to the Windows taskbar notification area for quick access.

When you install a Secure Agent, you perform the following tasks:

1. Verify that the machine meets the minimum requirements.

2. Download the Secure Agent installer files.
3. Install and register the Secure Agent.

Secure Agent requirements on Windows

You can install the Secure Agent on any machine that has internet connectivity and can access Informatica Intelligent Cloud Services. Before you install the Secure Agent on Windows, verify the system requirements.

Verify the following minimum requirements before you install the Secure Agent on Windows:

- The Secure Agent machine uses a supported operating system. For the list of supported operating systems for the Secure Agent, see the Product Availability Matrix (PAM) for Informatica Intelligent Cloud Services on the Knowledge Base.
- The Secure Agent machine has Microsoft Visual C++ 2015 Redistributable.
- The Secure Agent machine has at least 4 CPU cores, 16 GB RAM, and at least 15 GB of free disk space. CDI-PC requires 5 GB for installation and 10 GB for automated updates.
- The Secure Agent machine is on a volume with at least 250 GB disk space, with at least 5 GB free space or three times the size of the Secure Agent installation, whichever is greater.
- No other Secure Agent is installed on the machine. If another Secure Agent is installed on the machine, uninstall it first.

For more information about Secure Agent requirements, see this article:
https://knowledge.informatica.com/s/article/526096

Configure the firewall

If your organization uses a protective firewall, include the Informatica Intelligent Cloud Services domain name or IP address ranges in the list of approved domain names or IP addresses. To ensure that the Secure Agent can perform all necessary tasks through the firewall, enable the port that the Secure Agent uses.

The Secure Agent uses port 443 (HTTPS) to connect to the internet. Configure your firewall to allow traffic to pass over port 443.

The allowlists of domains and IP addresses can vary according to your data center, which is also called a POD (Point of Deployment). You can identify your POD through the URL that appears when you open any service in Informatica Intelligent Cloud Services. The first few characters of the URL string identify the POD. For example, if the URL starts with `usw3.dm-us.informaticacloud.com`, your POD is USW3.

For the allowlists of Informatica Intelligent Cloud Services domains and IP addresses for different PODs, see Pod Availability and Networking in the documentation portal or click the link at the top of the **Runtime Environments** page in Administrator.

Downloading and installing the Secure Agent on Windows

To install the Secure Agent on a Windows machine, you must download and run the Secure Agent installation program and then register the agent.

Secure Agent registration requires an install token. To get the install token, copy the token when you download the agent or use the **Generate Install Token** option in Administrator. The token expires after 24 hours.

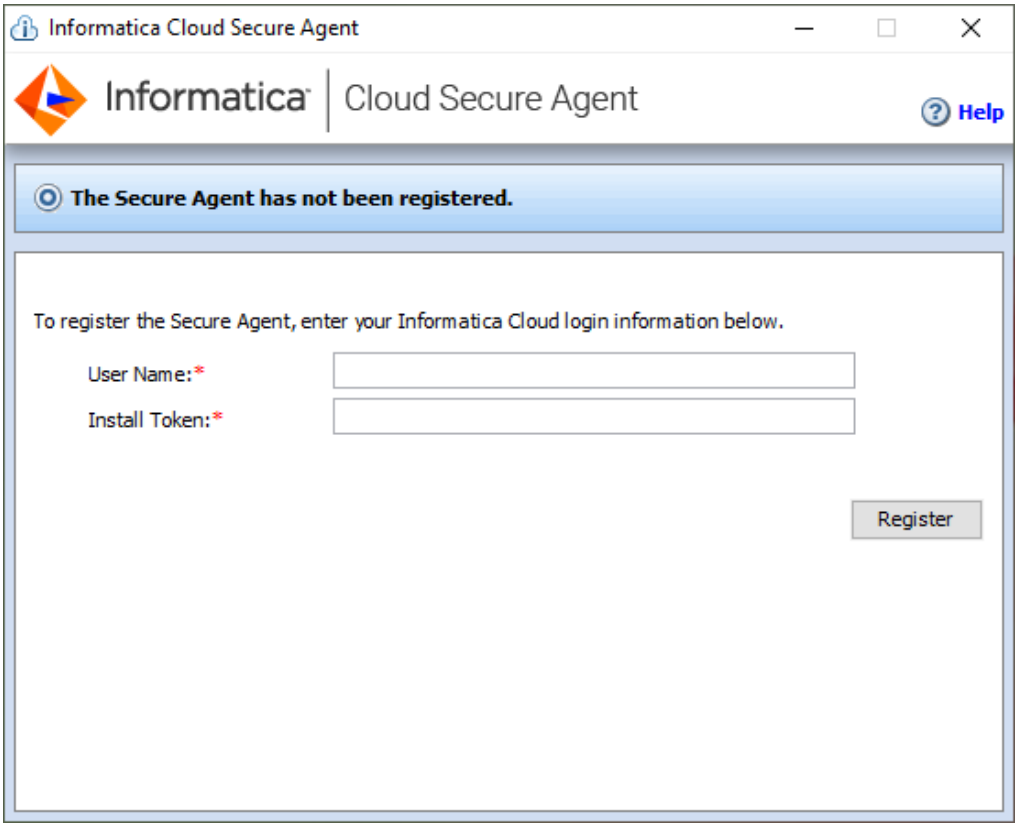
Before you download and install the Secure Agent, verify that no other Secure Agent is installed on the machine. If any other Secure Agent exists, you must uninstall it.

Tip: To verify the checksum of the Secure Agent installation program, use the agent REST API version 2 resource. For more information about the agent resource, see *REST API Reference*.

1. Open Administrator and select **Runtime Environments**.
2. On the **Runtime Environments** page, click **Download Secure Agent**.
3. Select the Windows 64-bit operating system platform, copy the install token, and then click **Download**.

   The installation program is downloaded to your machine. The name of the installation program is `agent64_install_ng_ext.<agent core version>.exe`.
4. Run the installation program as an Administrator:
   a. Specify the Secure Agent installation directory, and click **Next**.
   b. Click **Install** to install the agent.

   The **Cloud Secure Agent** dialog box opens and prompts you to register the agent as shown in the following image:



5. If you did not copy the install token when you downloaded the agent, click **Generate Install Token** on the **Runtime Environments** page in Administrator, and copy the token.
6. In the Secure Agent Manager, enter the following information, and then click **Register**:

Option	Description
User Name	User name that you use to access Informatica Intelligent Cloud Services.
Install Token	Token that you copied.

The Secure Agent Manager displays the status of the Secure Agent. It takes a minute for all of the services to start.

7. If your organization uses an outgoing proxy server to connect to the internet, enter the proxy server information.
8. Close the Secure Agent Manager.

   The Secure Agent Manager minimizes to the taskbar and continues to run as a service until stopped.

Verify the license edition

To access the CDI-PC Home page and perform CDI-PC tasks in Informatica Intelligent Cloud Services, you require a specific license edition.

To enable license editions, contact Informatica Global Customer Support.

Generate keystore and truststore certificates

Use a key and certificate management utility to generate keystore and truststore certificates for the Secure Agent.

To create the required files, you can use the following programs:

keytool

You can use keytool to create a TLS certificate or a Certificate Signing Request (CSR) as well as keystores and truststores in JKS format.

OpenSSL

You can use OpenSSL to create a TLS certificate or CSR as well as convert a keystore in JKS format to PEM format.

For more information about OpenSSL, see the documentation on the following website: https://www.openssl.org/docs/

The software available for download at the referenced links belongs to a third party or third parties, not Informatica. The download links are subject to the possibility of errors, omissions or change. Informatica assumes no responsibility for such links and/or such software, disclaims all warranties, either express or implied, including but not limited to, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and disclaims all liability relating thereto.

For a higher level of security, send your CSR to a Certificate Authority (CA) to get signed certificates. If you use CA-signed certificates, you get a certificate chain with an ordered list of certificates that include the root certificate, one or more intermediate certificates, and the user certificate. Enter all certificates in the chain when you generate the PEM format.

For information about how to generate and configure custom keystore and truststore certificates, see the following KB article: Configure keystore and truststore for Cloud Data Integration for PowerCenter

You can use the TLS utility to validate your certificates. The utility verifies that the certificates are valid for communication between two hosts. For information about how to run the utility, see “Validate the certificates with the TLS utility” on page 33.

Import the Secure Agent truststore certificate to the domain truststore

To ensure that the Secure Agent can communicate with the domain, the Secure Agent certificates must be present in the domain truststore. After you generate the truststore certificate, import the certificate into the domain truststore.

If you ran the TLS utility to validate your certificates, you don't need to perform this task. The TLS utility validates the certificates and verifies that the domain and the Secure Agent can communicate. The verification process exchanges the certificates if they aren't already present.

To import the Secure Agent truststore certificate to the CDI-PC domain truststore, run the following command with appropriate values:

```
keytool -importcert -file <Secure Agent Cert file>.crt -keystore infa_truststore.jks -
alias <Any other alias name> -deststoretype JKS -v -trustcacerts
```

Configure TLS for the Secure Agent

Configure Transport Layer Security (TLS) for the Secure Agent where you enabled the Domain Management App to enable secure communication between the Secure Agent and the domain.

Import the CDI-PC domain truststore certificate into the truststore folder on the Secure Agent machine. If you don't import the domain certificate before you configure the Secure Agent, you must restart the Domain Management App after you import the domain certificate.

1. Log in to Informatica Intelligent Cloud Services and open Administrator.
2. Select **Runtime Environments** and click the Secure Agent.
3. Expand the **System Configuration Details** section and click **Edit**.
4. Select Domain Management App from the list of services.
5. Select *SECURITY_CFG* from the list of configuration property types.
6. Enter the following property values:

Property	Description
DMA_DOMAINS_COMM_KEYSTORE	Path and file name of the keystore file generated for the Secure Agent.
DMA_DOMAINS_COMM_KEYSTORE_PASS	Password for the keystore file.
DMA_DOMAINS_COMM_TRUSTSTORE	Path and file name of the truststore file generated for the Secure Agent.
DMA_DOMAINS_COMM_TRUSTSTORE_PASS	Password for the truststore file.

7. Mark the passwords as sensitive fields.
8. Click **Save**.

CHAPTER 4

Create a CDI-PC domain

You can run the installer in console, graphical, or silent mode to create a CDI-PC domain.

When you run the installer, you can choose to create a domain. The domain consists of core CDI-PC services to support the domain. The domain is a collection of nodes that represent the machines on which the application services run. You create a domain the first time you run the installer. If you install on a single machine, you create the domain and gateway node on the machine. If you install on multiple machines, you create an Informatica domain and a gateway node during the first installation. During the installation on the additional machines, you create gateway or worker nodes that you join to the domain.

When the installer creates a domain, it installs files for services. If you run the installer in console mode, you can create the services during the installation process, or you can manually create them after installation. To create the services during installation, log in to Informatica Intelligent Cloud Services and register the domain on the CDI-PC Home page. You can then continue to create the services.

If you run the installer in silent mode, you can't create the services during installation. After the installation succeeds, register the domain and then log in to Informatica Administrator to create the services.

Run the installer in console mode

To create a CDI-PC domain, you run the installer and configure the communication and security settings for the domain and between the domain and clients.

Run the Pre-Installation (i10Pi) System Check Tool before you install. For information about running the Pre-Installation (i10Pi) System Check Tool, see "Run the pre-installation system check tool in console mode" on page 35.

1. Log in to the machine with a system user account.
2. Clear the DISPLAY variable on the machine.
3. Use the unset command to clear the following variables:

   `INFA_HOME`, `INFA_NODE_NAME`, and `INFA_DOMAINS_FILE`
4. Close all the other applications.
5. On a shell command line, run the install.sh file.

   The installer displays the message to verify that the locale environment variables are set.
6. Press **1** to install CDI-PC.

   Default is 1.
7. Press **2** to migrate an existing Informatica PowerCenter domain to a CDI-PC domain.
8. Press **1** to run the installer.

The installer displays the following options based on the platform you are installing on:

1. Press **1** to run the Pre-Installation System Check Tool.
2. Press **2** to run the Cloud Data Integration for PowerCenter (CDI-PC) installer.

Default is 2.

9. Press **2** to run the Cloud Data Integration for PowerCenter (CDI-PC) installer.

   The **Welcome** section appears.

10. Read the copyright information and press **Enter** to continue.

    The Installation Prerequisites section displays the installation requirements.

11. Verify that all requirements are met before you continue the installation and press **Enter** to continue.

    The **License and Installation Directory** section appears.

Provide the license key and installation directory path

Specify the installation directory and the path to the license key file.

1. Enter the absolute path to the installation directory.

   The directory names in the path can't contain spaces or the following special characters:

   ` % * + ; \ / " ? , < > @ # ! %) (} {] [' | &

   Default is the user home directory for the user that runs the installation.

   Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

2. Enter the absolute path to the license key and press **Enter**.

   You can enter the license key of any version.

3. Choose **1** to enable Kerberos network authentication, otherwise choose **2** and press **Enter**.

   Default is 1.

   Note: You can enable either Kerberos authentication or Security Assertion Markup Language (SAML) authentication in the domain. You cannot enable both authentication modes.

   If you enabled Kerberos network authentication, the **Network Security - Service Principal Level** section appears.

   If you did not enable Kerberos network authentication, the **Pre-Installation Summary** section appears. Review the installation information and press Enter to continue. Skip to "Configure domain settings and secure communication" on page 50.

4. Select the level at which to set the Kerberos service principals for the domain.

   All nodes in a CDI-PC domain must use the same service principal level. When you join a node to a domain, select the same service principal level used by the gateway node in the domain.
   Choose one of the following levels:

   1. **Process Level**. Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node. The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.

2. **Node Level**. Configures the domain to share SPNs and keytab files on a node. This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Use the node level option for domains that do not require a high level of security, such as test and development domains.

The **Network Security - Kerberos Authentication** section appears.

5. Enter the parameters required for Kerberos authentication.
   - **Domain Name**. Name of the domain. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
   - **Node Name**. Name of the CDI-PC node.
   - **Node Host Name**. Fully qualified host name or the IP address of the machine on which to create the node. The node host name cannot contain the underscore (_) character.

     Note: Do not use localhost. The host name must explicitly identify the machine.
   - **Service Realm Name**. Name of the Kerberos realm to which the CDI-PC domain services belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
   - **User Realm Name**. Name of the Kerberos realm to which the CDI-PC domain users belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
   - **Keytab Directory**. Directory where all keytab files for the CDI-PC domain are stored. The name of a keytab file in the CDI-PC domain must follow a format set by Cloud Data Integration for PowerCenter (CDI-PC).
   - **Fully Qualified Path to the Kerberos Configuration File**. Path and file name of the Kerberos configuration file. Cloud Data Integration for PowerCenter (CDI-PC) requires the following name for the Kerberos configuration file: `krb5.conf`

   Important: If you configure the domain to run with Kerberos authentication, the domain and node name and the node host name must match the names you specified when you ran the Cloud Data Integration for PowerCenter (CDI-PC) Kerberos SPN Format Generator to generate SPN and keytab file names. If you use a different domain, node, or host name, generate the SPN and keytab file names again and ask the Kerberos administrator to add the new SPN to the Kerberos principal database and create the keytab files.

   The **Pre-Installation Summary** section appears.
6. Review the installation information and press **Enter** to continue.

   The installer copies the CDI-PC files to the installation directory. After the installer copies the files, the **Domain Selection** page appears.

Configure domain settings and secure communication

Choose to create a domain and enter port and keystore file information to configure secure configuration between the CDI-PC domain and the Administrator tool.

1. Press **1** to create a domain.
2. Enter the HTTPS port number for the Administrator tool. Default is 8443.
3. Enter the absolute path to the custom keystore file to configure secure communication between the Administrator tool and the domain.

   Use the keystore that's in .jks format.
4. Enter the keystore password.

5. Choose whether to enable SAML authentication to configure Security Assertion Markup Language (SAML)-based single sign-on (SSO) support for web-based Informatica applications in a CDI-PC domain.

   Press **1** to enable and configure SAML authentication. Press **2** to disable SAML authentication and skip to "Configure secure communication in the domain" on page 52. Default is Yes.
6. Enter the Identity Provider URL for the domain.
7. Specify the relying party trust name or the service provider identifier for the domain as defined in the identity provider. If you choose No, the service provider identifier is set to "Informatica".
8. Specify whether or not the IdP will sign the SAML assertion.
9. Enter the identity provider assertion signing certificate alias name.
10. Enter the directory where you store your custom TLS certificates to enable SAML authentication in the domain.

    Specify the directory only, not the full path to the file.
11. Specify the location and passwords of the keystore and truststore files.

    The following table describes the location and password of the truststore and keystore files:

Property	Description
Truststore Directory	The directory containing the custom truststore file. Specify the directory only, not the full path to the file.
Truststore Password	The password for the custom truststore file.
Keystore Directory	The directory containing the custom keystore file.
Keystore Password	The password for the custom keystore file.

12. To specify the Authentication Context Comparison, specify the strength comparison of the authentication mechanism used by the user with the IdP server.

    Supported values are MINIMUM, MAXIMUM, BETTER, or EXACT option. Default is MINIMUM.
13. To set the Authentication Context Class, specify the expected mechanism of first time authentication of the user with the IdP server.

    Supported values are PASSWORD or PASSWORDPROTECTEDTRANSPORT. Default is PASSWORD.
14. Specify whether or not you want to enable the webapp to sign the SAML authentication request.

    Default is disabled.
15. Specify the alias name of the private key that was imported to the node SAML keystore using which the SAML request should be signed.
16. Specify the password to access the private key used for signing the SAML request.
17. Specify the algorithm that the web application uses to sign the SAML request.

    Use one of the following values:

    `RSA_SHA256, DSA_SHA1, DSA_SHA256, RSA_SHA1, RSA_SHA224, RSA_SHA384, RSA_SHA512, ECDSA_SHA1, ECDSA_SHA224, ECDSA_SHA256, ECDSA_SHA384, ECDSA_SHA512, RIPEMD160, or RSA_MD5.`
18. Specify whether or not you want IdP to sign the SAML response.

    Choose this to enable the webapp to receive the signed SAML response. Default is disabled.
19. Specify whether or not IdP will encrypt the SAML assertion.

Choose this to enable the webapp to receive an encrypted SAML assertion. Default is enabled.

20. Specify the alias name of the private key present in the gateway node SAML truststore that Informatica uses to decrypt the SAML assertion.
21. Provide the password to access the private key to use when decrypting the assertion encryption key.
22. Press **Enter**.

    The **Domain Security - Secure Connection** section appears.

Configure secure communication in the domain

Enter TLS certificate details to configure secure communication in the domain.

1. Enter the path to a custom keystore directory that contains a keystore file in .jks format.
2. Enter the keystore password.
3. Enter the path to a custom truststore directory.
4. Enter the truststore password.

The **Domain Configuration Repository** section appears.

Configure the domain configuration repository

After you configure domain security, you can configure the domain repository details. The domain configuration repository stores metadata for domain operations and user authentication. Ensure that repository database is accessible to the gateway node in the domain.

1. Select the database for the domain configuration repository details.

   The following table lists the databases you can use for the domain configuration repository:

Prompt	Description
Database type	Type of database for the domain configuration repository. Select from the following options: - 1 - Oracle - 2 - SQL Server - 3 - DB2 - 4 - Sybase - 5 - PostgreSQL Default is Oracle.

2. Enter the properties for the database user account.

   The following table lists the properties for the database user account:

Property	Description
Database User ID	Name for the domain configuration database user account.
User Password	Password for the domain configuration database user account.

3. If you do not create a secure domain configuration repository, enter the parameters for the database.
   a. If you select **IBM DB2**, select whether to configure a tablespace and enter the tablespace name.

Property	Description
Configure tablespace	In a single-partition database, if you select **No**, the installer creates the tables in the default tablespace. In a multi-partition database, you must select **Yes**. Select whether to specify a tablespace: - 1 - No - 2 - Yes
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, enter the name of the tablespace in which to create the tables. In a multi-partition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

   b. If you select **Microsoft SQL Server** or **PostgreSQL**, enter the schema name for the database.

      Enter the name of the schema that will contain the domain configuration tables. If the parameter is blank, the installer creates the tables in the default schema.

4. Choose whether to enter secure database parameters.

   You can create a domain configuration repository in a database secured with TLS. To enter secure database parameters, press **1**. If you don't want to enter secure database parameters, press **2**.

5. If you create a secure domain configuration repository, enter the parameters for the secure database.

   The following table describes the options available to create a secure domain configuration repository database:

Property	Description
Database Truststore File	Absolute path to the truststore file for the secure database.
Database Truststore Password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

The following table describes the secure database parameters to configure:

Database parameter	Description
EncryptionMethod	Required. Indicates whether data is encrypted when transmitted over the network. Set to `SSL`.
ValidateServerCertificate	Optional. Indicates whether Informatica validates the certificate that the database server sends. If this parameter is set to True, Informatica validates the certificate that the database server sends. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate. If this parameter is set to False, Informatica doesn't validate the certificate that the database server sends. Informatica ignores any truststore information that you specify
HostNameInCertificate	Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the certificate.
cryptoProtocolVersion	Required. Specifies the cryptographic protocol to use to connect to a secure database. Based on the cryptographic protocol used by the database server, set to one of the following values: - cryptoProtocolVersion=TLSv1.1 - cryptoProtocolVersion=TLSv1.2

Provide a JDBC connection string that includes the security parameters for the database.

Note: You cannot configure a secure connection to a Sybase database.

The following table provides the database connection string syntax:

Database	Connection string syntax
IBM DB2	`jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
Oracle	`jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=<service name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
Micrososft SQL Server	`jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
PostgreSQL	`jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`

Note: The installer doesn't validate the connection string. Verify that the connection string contains all the connection parameters and security parameters required by your database.

Enter encryption key details

After you configure the domain repository, you can configure the encryption key.

1. Enter the encryption key directory for the CDI-PC domain.

   By default, the encryption key is created in the following directory: `<USER_INSTALL_DIR>/Informatica/platform/usr/config/isp/config/keys`. The installer creates a siteKey file and sets different permissions to the directory and the files in the directory.

2. Enter **1** to back up the site key that the installer generates.

   The site key generated is a unique key. If you lose the site key, you can't generate it again. Create a backup of the site key before you continue.

Configure the domain and node

After you configure the encryption key, you can configure the domain and node.

1. Enter the information for the domain and node that you want to create.

   The following table describes the properties that you set for the domain and node.

Property	Description
Domain name	Name of the CDI-PC domain to create. Use the following guidelines for the domain name: - Use 7-bit ASCII. - The name can't exceed 128 characters. - The name can't contain a space or any of the following characters: ` ` % * + ; " ? , < > \ / Default is Domain.
Node host name	Host name or IP address of the machine on which to create the node. If the machine has a single network name, use the default host name. If the machine has multiple network names, you can modify the default host name to use an alternate network name. **Note:** The node host name can't contain the underscore (_) character. Use a name that explicitly identifies the machine. Don't use localhost.
Node name	Name of the node to create.
Node port number	Port number for the node. The default port number for the node is 6005. If the port number is not available on the machine, the installer displays the next available port number.
Domain user name	User name for the domain administrator. You can use this user name to initially log in to Informatica Administrator. Use the following guidelines: - The name is not case sensitive and cannot exceed 128 characters. - The name cannot include a tab, newline character, or the following special characters: % * + / ? ; < >. - The name can include an ASCII space character except for the first and last character. Other space characters are not allowed.

2. Choose whether you want to enable password complexity to secure sensitive data in the domain.

The following table describes the password complexity:

Prompt	Description
Password complexity	Choose whether you want to enable password complexity. If you choose Yes, the password must meet the following requirements: It must be at least eight characters long and contain at least one alphabetic character, one numeric character, and one special character.
Configure password policy	Choose whether you want to configure a password policy. If you choose Yes, you can configure password complexity rules. If you choose No, the default Informatica password policy rules apply.
Number of special characters	The minimum number of special characters required in a password. You can use the following special characters: [! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~] You can enter a value between 0 and 128. Default is 1.
Number of alphabetic characters	The minimum number of alphabetic characters required in a password. You can enter a value between 0 and 128. Default is 1.
Number of numeric characters	The minimum number of numeric characters required in a password. You can enter a value between 0 and 128. Default is 1.
Minimum password length	The minimum number of characters required in a password. You can enter a value between 1 and 128. Default is 8.
Number of previous passwords to store	The number of consecutive previous passwords that can't be reused. You can enter a value between 0 and 12. Default is 0.
Password expiration in days	The duration of the validity of a password. If you don't want passwords to expire, set the value to 0. Default is 0.
Domain password	Password for the domain administrator. - If you don't enable password complexity, the password must be between 3 and 128 characters. - If you enable password complexity but use the Informatica default password policy, the password must be at least 8 characters long. - If you enable password complexity and configure a password policy, the password must be between 1 and 128 characters.
Confirm password	Enter the password again to confirm.

3. Choose whether to display the default ports for the domain and node components assigned by the installer.

   If you choose **1** for Yes, the installer displays the default port numbers assigned to the domain components. You can specify the port numbers to use for the domain and node components. You can also specify a range of port numbers to use for the service process that will run on the node. You can use the default port numbers or specify new port numbers. Verify that the port numbers you enter are not used by other applications.

4. If you display the port configuration page, enter new port numbers at the prompt or press **Enter** to use the default port numbers.

   The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

5. Choose whether you want to configure the CDI-PC Repository Service and CDI-PC Integration Service. If you choose No, the **Post-Installation Summary** section appears which indicates whether the installation completed successfully. You can exit the installer and configure the services later from the Administrator tool. Skip to the "After you create the domain" on page 70 section to continue.
6. If you choose to create the services from the installer, the CDI-PC Repository Service and CDI-PC Integration Service section appears. To create the services, you first log in to Informatica Intelligent Cloud Services and register the domain on the CDI-PC **Home** page. You can keep the installer window open and continue after you register the domain.

   For information about how to register the domain, see "Register the domain in CDI-PC " on page 70.

Create the CDI-PC Repository Service and the CDI-PC Integration Service

If you paused the installation to register the domain, you can configure the CDI-PC Integration Service and the CDI-PC Repository Service from the installer.

1. Choose the database to configure for the CDI-PC repository.

   You can configure the CDI-PC repository with one of the following databases:

   - 1 - Oracle

- 2 - Microsoft SQL Server
- 3 - IBM DB2
- 4 - Sybase
- 5 - PostgreSQL

Default is Oracle.

2. Enter the properties for the database user account.

   The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the CDI-PC repository database user account.
User password	Password for the CDI-PC repository database user account.
Database service name	Service or database name for the CDI-PC repository: - Oracle. Enter the service name. - Microsoft SQL Server. Enter the database name. - IBM DB2. Enter the service name. - PostgreSQL. Enter the database name. - Sybase. Enter the database name.
Database host name	Enter the CDI-PC repository database host name. Required for Microsoft SQL Server.

3. Enter a name for the CDI-PC Repository Service.
4. Enter a name for the CDI-PC Integration Service.
5. Select the CDI-PC Repository Service code page. Default is 7-bit ASCII.
6. Select the CDI-PC Integration Service code page. Default is 7-bit ASCII.

The **Post-Installation Summary** section indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration. Press **Enter** to exit the installer. If you use other services, you can create them in Informatica Administrator or run an infacmd command to create the services.

Run the installer in graphical mode

To create a CDI-PC domain, you run the installer and configure the communication and security settings for the domain and between the domain and clients.

1. Log in to the machine with a system user account.
2. Close all the other applications.
3. Go to the root of the directory for the installation files and run `install.bat` as administrator.

   To run the file as administrator, right-click the `install.bat` file and select **Run as administrator**.

   Note: If you do not run the installer as administrator, the Windows system administrator might encounter issues when accessing files in the CDI-PC installation directory.

   The CDI-PC page appears.
4. Select **Install CDI-PC**.

Informatica provides utilities to facilitate the CDI-PC installation process. Before you install CDI-PC, run the **Pre-Installation (i10Pi) System Check Tool** to check whether the machine on which you are installing CDI-PC services meets the system requirements for installation.
For more information about running the Pre-Installation (i10Pi) System Check Tool, see "Run the pre-installation system check tool in graphical mode" on page 37.

5. Click **Start**.

   The **Welcome** page appears.

6. Read the copyright information, and click **Next** to continue.

   The **Installation Prerequisites** page displays the installation requirements.

7. Verify that all requirements are met before you continue the installation.

8. Click **Next**.

   The **License and Installation Directory** page appears.

Provide the license key and installation directory path

Specify the installation directory and the path to the license key file.

1. On the **License and Installation Directory** page, enter the CDI-PC installation directory and license key information.

   - **Installation directory**. Absolute path to the installation directory. The directory names in the path can't contain spaces or the following special characters:
     ` % * + ; \ / " ? , < > @ # ! %) (} {] [' | &

     Default is the user home directory for the user that runs the installation.

     Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

   - **License key**. Absolute path to the license key.
     You can enter the license key of any version.

   If you enabled Kerberos network authentication, the **Network Security - Service Principal Level** section appears.

   If you did not enable Kerberos network authentication, the **Pre-Installation Summary** page appears. Review the installation information and click **Install** to continue. Skip to "Configure domain settings and secure communication" on page 61.

2. Click **Next**.

   If you enabled Kerberos network authentication, the **Network Security - Service Principal Level** section appears.

   If you did not enable Kerberos network authentication, the **Pre-Installation Summary** page appears. Review the installation information and click **Install** to continue. Skip to "Configure domain settings and secure communication" on page 61.

3. Select the level at which to set the Kerberos service principals for the domain.

   All nodes in a CDI-PC domain must use the same service principal level. When you join a node to a domain, select the same service principal level used by the gateway node in the domain.

Choose one of the following levels:

1. **Process Level**. Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node. The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.
2. **Node Level**. Configures the domain to share SPNs and keytab files on a node. This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Use the node level option for domains that do not require a high level of security, such as test and development domains.

The **Network Security - Kerberos Authentication** section appears.

4. Enter the parameters required for Kerberos authentication.
   - **Domain Name**. Name of the domain. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
   - **Node Name**. Name of the CDI-PC node.
   - **Node Host Name**. Fully qualified host name or the IP address of the machine on which to create the node. The node host name cannot contain the underscore (_) character.

     Note: Do not use localhost. The host name must explicitly identify the machine.
   - **Service Realm Name**. Name of the Kerberos realm to which the CDI-PC domain services belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
   - **User Realm Name**. Name of the Kerberos realm to which the CDI-PC domain users belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
   - **Keytab Directory**. Directory where all keytab files for the CDI-PC domain are stored. The name of a keytab file in the CDI-PC domain must follow a format set by Cloud Data Integration for PowerCenter (CDI-PC).
   - **Fully Qualified Path to the Kerberos Configuration File**. Path and file name of the Kerberos configuration file. Cloud Data Integration for PowerCenter (CDI-PC) requires the following name for the Kerberos configuration file: `krb5.conf`

   Important: If you configure the domain to run with Kerberos authentication, the domain and node name and the node host name must match the names you specified when you ran the Cloud Data Integration for PowerCenter (CDI-PC) Kerberos SPN Format Generator to generate SPN and keytab file names. If you use a different domain, node, or host name, generate the SPN and keytab file names again and ask the Kerberos administrator to add the new SPN to the Kerberos principal database and create the keytab files.

   The **Pre-Installation Summary** section appears.
5. Review the installation information, and click **Install** to continue.

   The installer copies the CDI-PC files to the installation directory. After the installer copies the files, the **Domain Selection** page appears.

Configure domain settings and secure communication

Choose to create a domain and enter port and keystore file information to configure secure configuration between the CDI-PC domain and the Administrator tool.

1. Select **Create a domain**.

   When you create a domain, the node that you create becomes a gateway node in the domain. The gateway node contains a Service Manager that manages all domain operations.
2. Enter the HTTPS port number for the Administrator tool.

   Default is 8443.
3. Enter the absolute path to the custom keystore file to configure secure communication between the Administrator tool and the domain.

   Use the keystore that's in `.jks` format.
4. Enter the keystore password.
5. To configure Security Assertion Markup Language (SAML) based single sign-on (SSO) support for web-based Informatica applications in an Informatica domain, select the checkbox to enable SAML authentication.

   If you do not want to enable SAML authentication option, skip to "Configure secure communication" on page 62.
6. Click **Next**.

   If you select the checkbox to enable SAML authentication option, the **SAML Authentication** page appears.
7. Enter the Identity Provider URL for the domain.
8. Specify the relying party trust name or the service provider identifier for the domain as defined in the identity provider.

   If you choose **No**, the service provider identifier is set to **Informatica**.
9. Specify whether or not the IdP will sign the SAML assertion.
10. Enter the identity provider assertion signing certificate alias name.
11. Provide the password to access the private key to use when decrypting the assertion encryption key.
12. Enter the directory where you store your custom TLS certificates to enable SAML authentication in the domain.

    Specify the directory only, not the full path to the file.
13. Specify the location and passwords of the keystore and truststore files.

    The following table describes the location and password of the truststore and keystore files:

Property	Description
Truststore Directory	The directory containing the custom truststore file. Specify the directory only, not the full path to the file.
Truststore Password	The password for the custom truststore file.
Keystore Directory	The directory containing the custom keystore file.
Keystore Password	The password for the custom keystore file.

14. To specify the **Authentication Context Comparison**, specify the strength comparison of the authentication mechanism used by the user with the IdP server.

    Supported values are MINIMUM, MAXIMUM, BETTER, or EXACT option. Default is MINIMUM.

15. To set the **Authentication Context Class**, specify the expected mechanism of first time authentication of the user with the IdP server.

    Supported values are PASSWORD or PASSWORDPROTECTEDTRANSPORT. Default is PASSWORD.

16. Specify whether or not you want to enable the webapp to sign the SAML authentication request.

    Default is disabled.

17. Specify the alias name of the private key that was imported to the node SAML keystore using which the SAML request should be signed.
18. Specify the password to access the private key used for signing the SAML request.
19. Specify the algorithm that the web application uses to sign the SAML request.

    Use one of the following values:

    `RSA_SHA256, DSA_SHA1, DSA_SHA256, RSA_SHA1, RSA_SHA224, RSA_SHA384, RSA_SHA512, ECDSA_SHA1, ECDSA_SHA224, ECDSA_SHA256, ECDSA_SHA384, ECDSA_SHA512, RIPEMD160, or RSA_MD5.`

20. Specify whether or not you want IdP to sign the SAML response.

    Choose this to enable the webapp to receive the signed SAML response. Default is disabled.

21. Specify whether or not IdP will encrypt the SAML assertion.

    Choose this to enable the webapp to receive an encrypted SAML assertion. Default is enabled.

22. Specify the alias name of the private key present in the gateway node SAML truststore that Informatica uses to decrypt the SAML assertion.
23. Provide the password to access the private key to use when decrypting the assertion encryption key.
24. Click **Next**.

    The **Domain Security - Secure Connection** page appears.

Configure secure communication

Enter TLS certificate details to configure secure communication in the domain.

1. Enter the path to a custom keystore directory that contains a keystore file in `.jks` format.
2. Enter the keystore password.
3. Enter the path to a custom truststore directory.
4. Enter the truststore password.

   The **Domain Configuration Repository** page appears.

Configure the domain configuration repository

After you configure domain security, you can configure the domain repository details. The domain configuration repository stores metadata for domain operations and user authentication. Ensure that repository database is accessible to the gateway node in the domain.

1. On the **Domain Configuration Repository** page, enter the database and user account information for the domain configuration repository.

The following table describes the properties that you specify for the database and user account.

Property	Description
Database type	Type of database for the domain configuration repository. Select from the following options: - IBM DB2 - Oracle - Microsoft SQL Server - PostgreSQL - Sybase Default is Oracle.
Database User ID	Name for the domain configuration database user account.
User Password	Password for the domain configuration database user account.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multi-partition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

If you select **Microsoft SQL Server** or **PostgreSQL**, enter the schema name for the database.
Enter the name of the schema that will contain the domain configuration tables. If the parameter is blank, the installer creates the tables in the default schema.

2. Enter the database connection information.

   If you do not create a secure domain configuration repository, you can specify the connection properties for the JDBC URL or provide the JDBC connection string.

   - To enter the connection information using the JDBC URL, select **JDBC URL** and specify the database connection properties.

The following table describes the JDBC URL properties that you specify:

Property	Description
Database Address	Host name and port number for the database in the format host_name:port_number.
Database Service Name	Service or database name. - Oracle. Enter the service name. - IBM DB2. Enter the service name. - Microsoft SQL Server. Enter the database name. - PostgreSQL. Enter the database name. - Sybase. Enter the database name.
JDBC Parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

- To connect using a custom JDBC connection string, select **Custom JDBC connection string** and type the connection string.

3. If you create a secure domain configuration repository, enter the parameters for the secure database.

   The following table describes the options available to create a secure domain configuration repository database:

Property	Description
Database Truststore File	Absolute path to the truststore file for the secure database.
Database Truststore Password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

The following table describes the secure database parameters to configure:

Database parameter	Description
EncryptionMethod	Required. Indicates whether data is encrypted when transmitted over the network. Set to `SSL`.
ValidateServerCertificate	Optional. Indicates whether Informatica validates the certificate that the database server sends. If this parameter is set to True, Informatica validates the certificate that the database server sends. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate. If this parameter is set to False, Informatica doesn't validate the certificate that the database server sends. Informatica ignores any truststore information that you specify

Database parameter	Description
HostNameInCertificate	Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the certificate.
cryptoProtocolVersion	Required. Specifies the cryptographic protocol to use to connect to a secure database. Based on the cryptographic protocol used by the database server, set to one of the following values: - cryptoProtocolVersion=TLSv1.1 - cryptoProtocolVersion=TLSv1.2

Provide a JDBC connection string that includes the security parameters for the database.

Note: You cannot configure a secure connection to a Sybase database.

The following table provides the database connection string syntax:

Database	Connection string syntax
IBM DB2	`jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
Oracle	`jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=<service name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
Micrososft SQL Server	`jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
PostgreSQL	`jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`

Note: The installer doesn't validate the connection string. Verify that the connection string contains all the connection parameters and security parameters required by your database.

4. Click **Test Connection** to verify that you can connect to the database, and then click **OK** to continue.
5. Click **Next**.

   The **Domain Security - Encryption Key** page appears.

Enter encryption key details

After you configure the domain repository, you can configure the encryption key.

1. On the **Domain Security - Encryption Key** page, enter the encryption key directory for the CDI-PC domain.

   By default, the encryption key is created in the following directory:

   `<CDIPC_INSTALL_DIR>/Informatica/platform/usr/config/isp/config/keys`

   The installer creates a siteKey file and sets different permissions to the directory and the files in the directory.

2. Select **Do you agree?** to back up the site key that the installer generates.

   The site key generated is a unique key.

   Note: If you lose the site key, you can't generate it again. Make sure that you save a copy of this key and do not share the unique site key with others. Create a backup of the site key before you continue.

3. Click **Next**.

   The **Domain and Node Configuration** page appears.

Configure the domain and node

After you configure the encryption key, you can configure the domain and node.

1. Enter the information for the domain and node that you want to create.

   The following table describes the properties that you set for the domain and node.

Property	Description
Domain Name	Name of the CDI-PC domain to create. Use the following guidelines for the domain name: - Use 7-bit ASCII. - The name can't exceed 128 characters. - The name can't contain a space or any of the following characters: ` % * + ; " ? , < > \ / Default is Domain.
Node Host name	Host name or IP address of the machine on which to create the node. If the machine has a single network name, use the default host name. If the machine has multiple network names, you can modify the default host name to use an alternate network name. **Note:** The node host name can't contain the underscore (_) character. Use a name that explicitly identifies the machine. Don't use localhost.
Node Name	Name of the node to create.
Node Port Number	Port number for the node. The default port number for the node is 6005. If the port number is not available on the machine, the installer displays the next available port number.
Domain User Name	User name for the domain administrator. You can use this user name to initially log in to Informatica Administrator. Use the following guidelines: - The name is not case sensitive and cannot exceed 128 characters. - The name cannot include a tab, newline character, or the following special characters: % * + / ? ; < >. - The name can include an ASCII space character except for the first and last character. Other space characters are not allowed.

2. Choose whether you want to enable password complexity to secure sensitive data in the domain.

The following table describes the password complexity:

Property	Description
Password complexity	Select whether you want to enable password complexity. If you select Yes, the password must meet the following requirements: It must be at least eight characters long and contain at least one alphabetic character, one numeric character, and one special character.
Configure password policy	Select whether you want to configure a password policy. If you select Yes, you can configure password complexity rules. If you select No, the default Informatica password policy rules apply.
Number of special characters	The minimum number of special characters required in a password. You can use the following special characters: [! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ ] ^ _ ` { | } ~] You can enter a value between 0 and 128. Default is 1.
Number of alphabetic characters	The minimum number of alphabetic characters required in a password. You can enter a value between 0 and 128. Default is 1.
Number of numeric characters	The minimum number of numeric characters required in a password. You can enter a value between 0 and 128. Default is 1.
Minimum password length	The minimum number of characters required in a password. You can enter a value between 1 and 128. Default is 8.
Number of previous passwords to store	The number of consecutive previous passwords that can't be reused. You can enter a value between 0 and 12. Default is 0.
Password expiration in days	The duration of the validity of a password. If you don't want passwords to expire, set the value to 0. Default is 0.
Domain password	Password for the domain administrator. - If you don't enable password complexity, the password must be between 3 and 128 characters. - If you enable password complexity but use the Informatica default password policy, the password must be at least 8 characters long. - If you enable password complexity and configure a password policy, the password must be between 1 and 128 characters.
Confirm password	Enter the password again to confirm.

3. To display the default ports for the domain and node components assigned by the installer, enable **Display advanced port configuration page**.

   If you display the port configuration page, the installer displays the default port numbers assigned to the domain and node. You can specify the port numbers to use for the domain and node components. You can also specify a range of port numbers to use for the service process that will run on the node. You can use the default port numbers or specify new port numbers. Verify that the port numbers you enter are not used by other applications. If you do not select the display the port configuration page, the installer does not display the default port numbers and you cannot modify the assigned port numbers.

4. Choose whether you want to configure the CDI-PC Repository Service and CDI-PC Integration Service during the installation.
5. If you don't want to configure the CDI-PC Repository Service and CDI-PC Integration Service, click **Next**.

   The **Post-Installation Summary** page appears which indicates whether the installation completed successfully.

   You can exit the installer and configure the services later from the Administrator tool. Skip to the "After you create the domain" on page 70 section to continue.
6. If you choose to create the services from the installer, the CDI-PC Repository Service and CDI-PC Integration Service section appears.

   To create the services, you first log in to Informatica Intelligent Cloud Services and register the domain on the CDI-PC **Home** page.

   You can keep the installer window open and continue after you register the domain.

   For information about how to register the domain, see "Register the domain in CDI-PC " on page 70.
7. If you selected to display the port configuration page, the **Port Configuration** page appears.

Configure the ports

You can update the port numbers for the Service Manager and Informatica Administrator.

1. On the **Port Configuration** page, enter the port numbers to use for the domain service manager and service processes that will run on the node.

   Verify that the port numbers you enter are not used by other applications.
   The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

2. Click **Next**.

   The **Windows Service Configuration** page appears.

Configure Windows service

1. If you do not select to display the port configuration page, the **Windows Service Configuration** page appears.
2. Select whether to run the Windows service under a different user account.

   The installer creates a service to start Informatica. By default, the service runs under the same user account as the account used for installation. You can run the Windows service under a different user account.

   The following table describes the properties that you set to run Informatica under a different account:

Property	Description
Run Informatica under a different user account	Indicates whether to run the Windows service under a different user account.
User name	User account with which to run the Informatica Windows service. Use the following format: `<domain name>\<user account>` This user account must have the Act as operating system permission.
Password	Password for the user account with which to run the Informatica Windows service.

3. Click **Next**.

   If you do not choose to create the services, the installer displays the **Post-Installation Summary** page. The **Post-Installation Summary** page indicates whether the installation completed successfully.

Create the CDI-PC Integration Service and the CDI-PC Repository Service

If you paused the installation to register the domain, you can configure the CDI-PC Integration Service and the CDI-PC Repository Service from the installer.

1. Choose the database to configure for the CDI-PC repository.

   You can configure the CDI-PC repository with one of the following databases:

   - Oracle
   - Microsoft SQL Server
   - IBM DB2
   - Sybase
   - PostgreSQL

   Default is Oracle.
2. Enter the properties for the database user account.

The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the CDI-PC repository database user account.
User password	Password for the CDI-PC repository database user account.
Database service name	Service or database name for the CDI-PC repository: - Oracle. Enter the service name. - Microsoft SQL Server. Enter the database name. - IBM DB2. Enter the service name. - PostgreSQL. Enter the database name. - Sybase. Enter the database name.
Database host name	Enter the CDI-PC repository database host name. Required for Microsoft SQL Server.

3. Enter a name for the CDI-PC Repository Service.
4. Enter a name for the CDI-PC Integration Service.
5. Select the CDI-PC Repository Service code page. Default is 7-bit ASCII.
6. Select the CDI-PC Integration Service code page. Default is 7-bit ASCII.

The **Post-Installation Summary** section indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

Click **Done** to exit the installer. If you use other services, you can create them in Informatica Administrator or run an infacmd command to create the services.

After you create the domain

After you create the domain, you need to perform the required post-requisite tasks before you can complete the installation and log in to the Administrator tool.

Perform the following tasks to complete the installation:

1. Register the domain on the CDI-PC **Home** page.
2. Log in to the Administrator tool and create the CDI-PC Repository Service and the CDI-PC Integration Service.

Register the domain in CDI-PC

Register the domain to establish communication between the domain and Informatica Intelligent Cloud Services.

To access the CDI-PC Home page, log in to Informatica Intelligent Cloud Services and select Cloud Data Integration for PowerCenter (CDI-PC).

If the domain uses Kerberos authentication, the TLS certificate of the Administrator tool must be imported into the browser before you can register or perform any tasks that require domain authentication. The operating system user and the domain administrator user must be the same, because the operating system

user details are used to authenticate with the domain. The user logged in to the system from where you open the browser must be a domain admin user and must be in the Active Directory configured to the domain.

1. Log in to Informatica Intelligent Cloud Services and select Cloud Data Integration for PowerCenter (CDI-PC).
2. On the **Home** page, click the **Add New Domain** button on the **Register a Domain** section.

   You can also open the **Explore** page from the navigation panel and click the **Add New Domain** button.
3. Enter the general properties.

   The following table lists the properties that you enter:

Property	Description
Domain Name	The name of the CDI-PC domain that you want to register.
Domain Display Name	A display name for the CDI-PC domain. By default, the display name is the same as the domain name. You can update the name if needed. The name can be different from the domain name, but the name must be unique in the organization.
Gateway Host	Host name of the gateway node machine.
Gateway Node Port	HTTPS port used by the gateway node.
Description	Optional. A description of the domain.

4. In the **Secure Agent Details** section, enter the name of the Secure Agent group.

   Secure Agents in the group require access to the domain.
5. In the **Domain Security Details** section, choose the authentication type.

   Choose Kerberos if the domain that you are registering uses Kerberos authentication.
6. In you choose non-Kerberos, enter the name of the security domain and the domain Administrator user name. If you choose Kerberos, enter the security domain. The service uses the operating system logged-in user details of the system from where you register the domain.
7. Click **Validate** to validate the details.

   Note: If the validation fails with a Read timed out error, retry validation.
8. When validation succeeds, click **Register** to register the domain.

If there is a break in connectivity, the domain might remain in Registering state indefinitely. Wait for at least 15 minutes and then click the **Refresh** button to refresh the information. If the domain status appears as offline, reconcile the domain status.

For information about reconciling a domain, see *Reconcile the status of a domain* in the Getting Started Guide.

Create the CDI-PC Repository Service in Informatica Administrator

Use the service creation options in the Administrator tool to create the service.

1. Log in to the Administrator tool and click the **Manage** tab.
2. Click **Actions** > **New** and select the CDI-PC Repository Service.

   The **New CDI-PC Repository Service** dialog box appears.

3. On the **New CDI-PC Repository Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. Consider the following guidelines when you name the service: - It is not case-sensitive. - It must be unique in the domain. - It can't exceed 128 characters. - It can't begin with @. - It can't contain the following special characters:` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [- You can't change the name of the service after you create it.
Description	Description of the service. It can't exceed 765 characters.
Location	Domain and folder where the service is created. Click **Browse** to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.
Primary Node	Required if you have high availability. The node where the service runs by default. Applicable for multi-node setups.
Backup Nodes	If your license includes high availability, nodes where the service can run if the primary node is unavailable. Applicable for multi-node setups.

4. Click **Next**.

   The **New CDI-PC Repository Service - Step 2 of 2** page appears.

5. Enter the following properties for the CDI-PC repository database:

Property	Description
Database Type	The type of the repository database.
Username	The database user name for the repository.
Password	7-bit ASCII password for the CDI-PC repository database user.
Connection String	Native connection string the CDI-PC Repository Service uses to access the repository database. Use the following native connect string syntax for each supported database: - `servername@databasename` for Microsoft SQL Server. - `databasename.world` as the database service name for Oracle. - `pgservice.conf` file as the database name for PostgreSQL.

Property	Description
Code Page	Repository database code page. The CDI-PC Repository Service uses the character set encoded in the database code page to write data. You cannot change the code page in the CDI-PC Repository Service properties after you create the service.
Tablespace Name	Name of the tablespace in which to create all the repository database tables. You cannot use spaces in the tablespace name. Available for IBM DB2 and Sybase databases. To improve repository performance on IBM DB2 EEE repositories, specify a tablespace name with one node.

6. Select **No content exists under specified connection string. Create new content.**
7. Optionally, choose to create a global repository.

   After you create the service, you can promote a local repository to a global repository, but you cannot change a global repository to a local repository.
8. If your license has the team-based development option, you can optionally enable version control of the repository.

   After you create the service, you can convert a non-versioned repository to a versioned repository, but you can't convert a versioned repository to a non-versioned repository.
9. Click **Finish**.

   The domain creates the CDI-PC Repository Service, starts the service, and creates content for the CDI-PC repository.

After you create the service, you can edit the properties or configure other properties.

Create the CDI-PC Integration Service in Informatica Administrator

Use the service creation options in the Administrator tool to create the service.

Before you create the service, verify that you created the CDI-PC Repository Service

1. Log in to the Administrator tool and click the **Manage** tab.
2. Click **Actions** > **New** and select the CDI-PC Integration Service.

   The **New CDI-PC Integration Service** dialog box appears.
3. On the **New CDI-PC Integration Service - Step 1 of 2** page, enter the following properties:

Property	Description
Name	Name of the service. Consider the following guidelines when you create the name: - It isn't case-sensitive. - It must be unique within the domain. - It can't exceed 128 characters. - It can't begin with @. - It can't contain spaces or the following special characters: ` ~ % ^ * + = { } \ ; : ' " / ? . , < > | ! ( )] [
Description	Description of the service. The description cannot exceed 765 characters.

Property	Description
Location	Domain and folder where the service is created. Click **Browse** to choose a different folder. You can move the service after you create it.
License	License object that allows use of the service.
Node	Node on which the service runs.
Assign	Select **Node** to configure the service to run on a node.
Primary Node	Required if you have high availability. The node where the service runs by default. Applicable for multi-node setups.
Backup Nodes	If you have high availability, nodes where the service can run if the primary node is unavailable. Applicable for multi-node setups.

4. Click **Next**.
5. On the **New CDI-PC Integration Service - Step 2 of 2** page, enter the following properties:

Property	Description
CDI-PC Repository Service	The CDI-PC Repository Service that you want to associate with the service.
Username	User name that the service uses to access the CDI-PC Repository Service. Enter the CDI-PC repository user that you created.
Password	Password associated with the CDI-PC repository user.
Security Domain	The LDAP security domain for the CDI-PC repository user. Appears when the CDI-PC domain contains an LDAP security domain.

6. Select the data movement mode that determines how the CDI-PC Integration Service handles character data. Choose ASCII or Unicode. Default is ASCII.

   In ASCII mode, the CDI-PC Integration Service recognizes 7-bit ASCII and EBCDIC characters and stores each character in a single byte. In Unicode mode, the service recognizes multibyte character sets as defined by the supported code pages. Use Unicode mode when the sources or targets use 8-bit or multibyte character sets and contain character data.
7. Click **Finish**.
8. On the **Specify Code Pages** dialog box, assign a code page for the CDI-PC Integration Service.

   Verify that the code page for the service is compatible with the code page of the associated repository.
9. Click **OK**.

   The domain creates the CDI-PC Integration Service. The domain does not enable the service during the service creation process.
10. To enable the CDI-PC Integration Service, verify that the CDI-PC Repository Service is available. Then select the CDI-PC Integration Service in the Navigator, and click **Actions** > **Enable Service**.

After you create the service, you can edit the properties or configure other properties.

Configure JVM parameters

CDI-PC includes script files that you can use to set environment variables used in infaservice and infasetup commands.

You can use script files, infasetupconfig.sh and infaserviceconfig.sh, to set environment variables. You can find the script files in the following location: `<CDI-PC installation directory>/Informatica/platform/usr/bin/`

If you use environment variables such as INFA_JAVA_OPTS or INFA_JAVA_CMD_OPTS to set customized values for JVM parameters that infaservice and infasetup commands use, set the variables and values in the configuration file for each command.

For example, to set the maximum heap size to 4 GB for each of the commands, configure each file as follows:

- infaserviceconfig.sh. `INFA_JAVA_OPTS="-Xmx4096m -XX:MaxMetaspaceSize=256m ${INFA_JAVA_OPTS}"`
- infasetupconfig.sh. `INFA_JAVA_CMD_OPTS="-Xmx4096m -XX:MaxMetaspaceSize=128m ${INFA_JAVA_CMD_OPTS}"`

Note: Any values that you edit in the infasetup.sh and infaservice.sh files might be overwritten when you apply updates.

Post-installation step for Data Quality

When you run the CDI-PC server installer, the installer installs the Data Quality libraries and files.

Ensure to update the following files with correct values:

- `AD50.cfg`. Stores configuration properties for address reference data
- `CLASSIFIER.properties`. Stores configuration properties for classifier model data.
- `IDQTx.cfg`. Stores configuration properties for identity population data.
- `NER.properties`. Stores configuration properties for probabilistic model data.

CHAPTER 5

Join a CDI-PC domain

You can join a domain if you are installing on multiple machines and you created a domain on another machine. You can run the installer to join a CDI-PC domain in console mode, graphical mode, or run the installer in silent mode.

When you install on additional machines, you create gateway or worker nodes that you join to the domain. When you run the installer, it installs files for services. If you run the installer in console mode, you can create the services during the installation process, or you can manually create them after installation.

Verify the hardware sizing requirements and prerequisites before you begin installation.

Note: Verify that the domain you want to join is registered in Informatica Intelligent Cloud Services.

Run the installer in console mode

To join a CDI-PC domain, you run the installer to provide details of the domain that you want to join and to configure the security settings for the node.

Run the Pre-Installation (i10Pi) System Check Tool before you install. For information about running the Pre-Installation (i10Pi) System Check Tool, see "Run the pre-installation system check tool in console mode" on page 35.

1. Log in to the machine with a system user account.
2. Clear the DISPLAY variable on the machine.
3. Use the unset command to clear the following variables:

   `INFA_HOME`, `INFA_NODE_NAME`, and `INFA_DOMAINS_FILE`
4. Close all the other applications.
5. On a shell command line, run the install.sh file.

   The installer displays the message to verify that the locale environment variables are set.
6. Press **1** to install CDI-PC.

   Default is 1.
7. Press **2** to migrate an existing Informatica PowerCenter domain to a CDI-PC domain.
8. Press **1** to run the installer.

   The installer displays the following options based on the platform you are installing on:

   1. Press **1** to run the Pre-Installation System Check Tool.

2. Press **2** to run the Cloud Data Integration for PowerCenter (CDI-PC) installer.

   Default is 2.

9. Press **2** to run the Cloud Data Integration for PowerCenter (CDI-PC) installer.

   The **Welcome** section appears.

10. Read the copyright information and press **Enter** to continue.

    The Installation Prerequisites section displays the installation requirements.

11. Verify that all requirements are met before you continue the installation and press **Enter** to continue.

    The **License and Installation Directory** section appears.

Provide the license key and installation directory path

Specify the installation directory and the path to the license key file.

1. Enter the absolute path to the installation directory.

   The directory names in the path can't contain spaces or the following special characters:

   ` % * + ; \ / " ? , < > @ # ! %) (} {] [' | &

   Default is the user home directory for the user that runs the installation.

   Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

2. Enter the absolute path to the license key and press **Enter**.

   You can enter the license key of any version.

3. Choose **1** to enable Kerberos network authentication, otherwise choose **2** and press **Enter**.

   Default is 1.

   Note: You can enable either Kerberos authentication or Security Assertion Markup Language (SAML) authentication in the domain. You cannot enable both authentication modes.

   If you enabled Kerberos network authentication, the **Network Security - Service Principal Level** section appears.

   If you did not enable Kerberos network authentication, the **Pre-Installation Summary** section appears. Review the installation information and press Enter to continue. Skip to "Configure domain settings and secure communication" on page 50.

4. Select the level at which to set the Kerberos service principals for the domain.

   All nodes in a CDI-PC domain must use the same service principal level. When you join a node to a domain, select the same service principal level used by the gateway node in the domain.
   Choose one of the following levels:

   1. **Process Level**. Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node. The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.
   2. **Node Level**. Configures the domain to share SPNs and keytab files on a node. This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Use the node level option for domains that do not require a high level of security, such as test and development domains.

   The **Network Security - Kerberos Authentication** section appears.

5. Enter the parameters required for Kerberos authentication.
   - **Domain Name**. Name of the domain. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
   - **Node Name**. Name of the CDI-PC node.
   - **Node Host Name**. Fully qualified host name or the IP address of the machine on which to create the node. The node host name cannot contain the underscore (_) character.

     Note: Do not use localhost. The host name must explicitly identify the machine.
   - **Service Realm Name**. Name of the Kerberos realm to which the CDI-PC domain services belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
   - **User Realm Name**. Name of the Kerberos realm to which the CDI-PC domain users belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
   - **Keytab Directory**. Directory where all keytab files for the CDI-PC domain are stored. The name of a keytab file in the CDI-PC domain must follow a format set by Cloud Data Integration for PowerCenter (CDI-PC).
   - **Fully Qualified Path to the Kerberos Configuration File**. Path and file name of the Kerberos configuration file. Cloud Data Integration for PowerCenter (CDI-PC) requires the following name for the Kerberos configuration file: `krb5.conf`

   Important: If you configure the domain to run with Kerberos authentication, the domain and node name and the node host name must match the names you specified when you ran the Cloud Data Integration for PowerCenter (CDI-PC) Kerberos SPN Format Generator to generate SPN and keytab file names. If you use a different domain, node, or host name, generate the SPN and keytab file names again and ask the Kerberos administrator to add the new SPN to the Kerberos principal database and create the keytab files.

   The **Pre-Installation Summary** section appears.
6. Review the installation information and press **Enter** to continue.

   The installer copies the CDI-PC files to the installation directory. After the installer copies the files, the **Domain Selection** page appears.

Join an existing domain

After you review the pre-installation summary, you can enter the domain information.

1. Press **2** to join a domain.

   The installer creates a node on the machine where you install.
2. Choose the type of node you want to create.

   Press **1** to configure a gateway node or **2** to configure a worker node.
3. If you configure a gateway node, you can choose to enable SAML authentication.

The **Domain Configuration** section appears.

Configure secure communication

Enter the TLS certificate details to configure secure communication in the domain. If you configured the node as a gateway node, you can configure SAML authentication for the node.

1. Enter the path to a custom keystore directory that contains a keystore file in .jks format.
2. Enter the keystore password.

3. Enter the path to a custom truststore directory.
4. Enter the truststore password.
5. Applicable for gateway nodes. Choose whether to enable Security Assertion Markup Language (SAML) authentication to configure SAML-based single sign-on (SSO) support for web-based Informatica applications in an Informatica domain.

   Press **1** to enable and configure SAML authentication. Press **2** to disable SAML authentication and skip to "Configure the domain configuration repository" on page 79.
6. If you chose to enable SAML authentication, enter the keystore and truststore directory and password.

The **Domain Configuration Repository** section appears.

Configure the domain configuration repository

After you select the domain options, you can configure the details of the domain you want to join.

- Enter the information for the domain that you want to join.

  The following table describes the properties that you specify for the domain:

Property	Description
Domain name	Name of the domain to join.
Gateway node host	Host name of the machine that hosts the gateway node for the domain.
Gateway node port	Port number of the gateway node.
Domain user name	User name of the administrator for the domain you want to join.
Domain password	Password for the domain administrator.
Confirm password	Enter the password for the domain administrator to confirm.

The **Domain Security - Encryption Key** section appears.

Enter encryption key details

After you configure the domain details, you can configure the encryption key.

- Enter the encryption key and directory details of the CDI-PC domain.

The following table describes the encryption key parameters to configure when you join a domain:

Prompt	Description
Enter the CDI-PC encryption key	The absolute path to the encryption key of the CDI-PC domain that you want to join. All nodes in the domain use the same encryption key. Specify the encryption key file created on the gateway node for the domain that you want to join. You can copy the file from the gateway node to the machine on which you create the node and provide the path to the file on the machine. If you copied the encryption key file to a temporary directory to make it accessible to all nodes in the domain, specify the path and file name of the encryption key file in the temporary directory.
CDI-PC encryption key directory	Directory in which to store the encryption key on the node created during this installation. The installer copies the domain encryption key file to the encryption key directory on the new node. You can enter the default path or provide a custom path to store the key file.

The **Join Domain Node Configuration** section appears.

Configure the node

After you configure the encryption key, you can configure the details for the node.

1. Enter the information for the node that you want to create in the domain.

   The following table describes the properties that you set for the current node:

Property	Description
Node host name	The host name or IP address of the machine on which to create the node. If the machine has a single network name, use the default host name. If the machine has multiple network names, you can modify the default host name to use an alternate network name. **Note:** The node host name cannot contain the underscore (_) character. Use a host name that explicitly identifies the machine. Don't use localhost.
Node name	The name of the node to create.
Node port number	The port number for the node. The default port number for the node is 7436. If the port number isn't available on the machine, the installer displays the next available port number.

2. Choose whether to display the advanced port configurations for the domain and node components assigned by the installer.

   If you select **1**, the installer doesn't display the port configurations.

   If you select **2** to create the ports, the **Port Configuration** section appears.

   The installer displays the default port numbers assigned to the domain components.

   You can specify the port numbers to use for the domain and node components. You can also specify a range of port numbers to use for the service process that will run on the node. You can use the default port numbers or specify new port numbers. Verify that the port numbers you enter aren't used by other applications.

3. Choose whether to create the services. Press **1** to create the CDI-PC Repository Service and the CDI-PC Integration Service through the installer. Press **2** to create them later.

   If you choose to create the services, the CDI-PC Repository Service and CDI-PC Integration Service section appears.

   If you choose to create them later, the **Post-Installation Summary** section appears.

Create the CDI-PC Repository Service and the CDI-PC Integration Service

You can configure the CDI-PC Repository Service and the CDI-PC Integration Service.

1. Choose the database to configure for the CDI-PC repository.

   You can configure the CDI-PC repository with one of the following databases:

   - 1 - Oracle
   - 2 - Microsoft SQL Server
   - 3 - IBM DB2
   - 4 - Sybase
   - 5 - PostgreSQL

   Default is Oracle.

2. Enter the properties for the database user account.

   The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the CDI-PC repository database user account.
User password	Password for the CDI-PC repository database user account.
Database service name	Service or database name for the CDI-PC repository: - Oracle. Enter the service name. - Microsoft SQL Server. Enter the database name. - IBM DB2. Enter the service name. - PostgreSQL. Enter the database name. - Sybase. Enter the database name.
Database host name	Enter the CDI-PC repository database host name. Required for Microsoft SQL Server.

3. Enter a name for the CDI-PC Repository Service.
4. Enter a name for the CDI-PC Integration Service.
5. Select the CDI-PC Repository Service code page. Default is 7-bit ASCII.
6. Select the CDI-PC Integration Service code page. Default is 7-bit ASCII.

The **Post-Installation Summary** section indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration. Press **Enter** to exit the installer. If you use other services, you can create them in Informatica Administrator or run an infacmd command to create the services.

Run the installer in graphical mode

To join a CDI-PC domain, you run the installer and configure the communication and security settings for the domain and between the domain and clients.

1. Log in to the machine with a system user account.
2. Close all the other applications.
3. Go to the root of the directory for the installation files and run `install.bat` as administrator.

   To run the file as administrator, right-click the `install.bat` file and select **Run as administrator**.

   Note: If you do not run the installer as administrator, the Windows system administrator might encounter issues when accessing files in the CDI-PC installation directory.

   The CDI-PC page appears.
4. Select **Install CDI-PC**.

   Informatica provides utilities to facilitate the CDI-PC installation process. Before you install CDI-PC, run the **Pre-Installation (i10Pi) System Check Tool** to check whether the machine on which you are installing CDI-PC services meets the system requirements for installation.
   For more information about running the Pre-Installation (i10Pi) System Check Tool, see "Run the pre-installation system check tool in graphical mode" on page 37.
5. Click **Start**.

   The **Welcome** page appears.
6. Read the copyright information, and click **Next** to continue.

   The **Installation Prerequisites** page displays the installation requirements.
7. Verify that all requirements are met before you continue the installation.
8. Click **Next**.

   The **License and Installation Directory** page appears.

Provide the license key and installation directory path

Specify the installation directory and the path to the license key file.

1. On the **License and Installation Directory** page, enter the CDI-PC installation directory and license key information.
   - **Installation directory**. Absolute path to the installation directory. The directory names in the path can't contain spaces or the following special characters:
     ` % * + ; \ / " ? , < > @ # ! %) ( ) { } [ ] [' | &

     Default is the user home directory for the user that runs the installation.

     Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.
   - **License key**. Absolute path to the license key.
     You can enter the license key of any version.

   If you enabled Kerberos network authentication, the **Network Security - Service Principal Level** section appears.

   If you did not enable Kerberos network authentication, the **Pre-Installation Summary** page appears. Review the installation information and click **Install** to continue. Skip to "Configure domain settings and secure communication" on page 61.
2. Click **Next**.

If you enabled Kerberos network authentication, the **Network Security - Service Principal Level** section appears.

If you did not enable Kerberos network authentication, the **Pre-Installation Summary** page appears. Review the installation information and click **Install** to continue. Skip to "Configure domain settings and secure communication" on page 61.

3. Select the level at which to set the Kerberos service principals for the domain.

   All nodes in a CDI-PC domain must use the same service principal level. When you join a node to a domain, select the same service principal level used by the gateway node in the domain.
   Choose one of the following levels:

   1. **Process Level**. Configures the domain to use a unique service principal name (SPN) and keytab file for each node and each application service on a node. The number of SPNs and keytab files required for each node depends on the number of application service processes that run on the node. Use the process level option for domains that require a high level of security, such as productions domains.
   2. **Node Level**. Configures the domain to share SPNs and keytab files on a node. This option requires one SPN and keytab file for the node and all application services that run on the node. It also requires a separate SPN and keytab file for all HTTP processes on the node. Use the node level option for domains that do not require a high level of security, such as test and development domains.

   The **Network Security - Kerberos Authentication** section appears.

4. Enter the parameters required for Kerberos authentication.

   - **Domain Name**. Name of the domain. The name must not exceed 128 characters and must be 7-bit ASCII only. The name cannot contain a space or any of the following characters: ` % * + ; " ? , < > \ /
   - **Node Name**. Name of the CDI-PC node.
   - **Node Host Name**. Fully qualified host name or the IP address of the machine on which to create the node. The node host name cannot contain the underscore (_) character.

     Note: Do not use localhost. The host name must explicitly identify the machine.
   - **Service Realm Name**. Name of the Kerberos realm to which the CDI-PC domain services belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
   - **User Realm Name**. Name of the Kerberos realm to which the CDI-PC domain users belong. The realm name must be in uppercase. The service realm name and the user realm name must be the same.
   - **Keytab Directory**. Directory where all keytab files for the CDI-PC domain are stored. The name of a keytab file in the CDI-PC domain must follow a format set by Cloud Data Integration for PowerCenter (CDI-PC).
   - **Fully Qualified Path to the Kerberos Configuration File**. Path and file name of the Kerberos configuration file. Cloud Data Integration for PowerCenter (CDI-PC) requires the following name for the Kerberos configuration file: `krb5.conf`

   Important: If you configure the domain to run with Kerberos authentication, the domain and node name and the node host name must match the names you specified when you ran the Cloud Data Integration for PowerCenter (CDI-PC) Kerberos SPN Format Generator to generate SPN and keytab file names. If you use a different domain, node, or host name, generate the SPN and keytab file names again and ask the Kerberos administrator to add the new SPN to the Kerberos principal database and create the keytab files.

   The **Pre-Installation Summary** section appears.

5. Review the installation information, and click **Install** to continue.

   The installer copies the CDI-PC files to the installation directory. After the installer copies the files, the **Domain Selection** page appears.

Join an existing domain

You can join an existing domain and enter port and keystore file information to configure secure configuration between the CDI-PC domain and the Administrator tool.

1. Select **Join a domain**.

   The installer joins a node on the machine where you install.
2. Select the type of node you want to create.

   If you configure the node as a gateway, you can enable a secure HTTPS connection to the Informatica Administrator.
3. If you enable HTTPS connection for the Informatica Administrator, enter an HTTPS port number to use to secure the connection.
4. To configure Security Assertion Markup Language (SAML) based single sign-on (SSO) support for web-based Informatica applications in an Informatica domain, select the checkbox to enable SAML authentication.
5. Click **Next**.

   If you select the checkbox to enable SAML authentication option, the **SAML Authentication** page appears.
6. Enter the Identity Provider URL for the domain.
7. Specify the relying party trust name or the service provider identifier for the domain as defined in the identity provider. If you choose No, the service provider identifier is set to "Informatica".
8. Specify whether IdP will sign SAML assertion or not.
9. Enter the identity provider assertion signing certificate alias name.
10. If you provide the security certificates, specify the location and passwords of the keystore and truststore files.

    The following table describes the location and password of the truststore and keystore files:

Property	Description
Truststore Directory	Specify the directory containing the custom truststore file on gateway nodes within the domain. Specify the directory only, not the full path to the file.
Truststore Password	The password for the custom truststore file.
Keystore Directory	Specify the directory containing the custom keystore file.
Keystore Password	The password for the custom keystore file.

11. To specify the Authentication Context Comparison, specify the strength comparison of the authentication mechanism used by the user with the IdP server.

    Supported values are MINIMUM, MAXIMUM, BETTER, or EXACT option. Default is MINIMUM.
12. To set the Authentication Context Class, specify the expected mechanism of first time authentication of the user with the IdP server.

Supported values are PASSWORD or PASSWORDPROTECTEDTRANSPORT. Default is PASSWORD.

13. Specify if you want to enable the webapp to sign the SAML authentication request or not?

    Default is disabled.

14. Specify the alias name of the private key that was imported to the node SAML keystore using which the SAML request should be signed.
15. Specify the password to access the private key used for signing the SAML request.
16. Specify the algorithm that the web application uses to sign the SAML request.

    Supported values are `RSA_SHA256, DSA_SHA1, DSA_SHA256, RSA_SHA1, RSA_SHA224, RSA_SHA384, RSA_SHA512, ECDSA_SHA1, ECDSA_SHA224, ECDSA_SHA256, ECDSA_SHA384, ECDSA_SHA512, RIPEMD160, or RSA_MD5`.

17. Specify whether you want IdP to sign the SAML response or not?

    Choose to select to enable the webapp to receive the signed SAML response or not. Default is disabled.

18. Specify whether IdP will encrypt SAML assertion or not.

    Select to enable the webapp to receive an encrypted SAML assertion. Default is enabled.

19. Specify the alias name of the private key present in the gateway nodes gateway node SAML truststore that used for Informatica uses to decrypt decrypting the SAML assertion.
20. Provide the password to access the private key to use when decrypting the assertion encryption key.
21. Click **Next**.

If you do not enable secure communication for the domain, the **Domain Configuration** page appears. Skip to step that describes the Domain Configuration Repository page. If you selected the checkbox to enable secure communication for the domain, the **Domain Security - Secure Communication** page appears.

Configure secure communication

Enter TLS certificate details to configure secure communication in the domain.

1. Enter the path to a custom keystore directory that contains a keystore file in `.jks` format.
2. Enter the keystore password.
3. Enter the path to a custom truststore directory.
4. Enter the truststore password.

   The **Domain Configuration Repository** page appears.

Configure the domain configuration repository

After you select the domain options, you can configure the details of the domain you want to join.

- Enter the information for the domain that you want to join.

  The following table describes the properties that you specify for the domain:

Property	Description
Domain name	Name of the domain to join.
Gateway node host	Host name of the machine that hosts the gateway node for the domain.

Property	Description
Gateway node port	Port number of the gateway node.
Domain user name	User name of the administrator for the domain you want to join.
Domain password	Password for the domain administrator.
Confirm password	Enter the password for the domain administrator to confirm.

The **Domain Security - Encryption Key** section appears.

Enter encryption key details

After you configure the domain repository, you can configure the encryption key.

1. On the **Domain Security - Encryption Key** page, enter the encryption key directory for the CDI-PC domain.

   By default, the encryption key is created in the following directory:

   ```
   <CDIPC_INSTALL_DIR>/Informatica/platform/usr/config/isp/config/keys
   ```

   The installer creates a siteKey file and sets different permissions to the directory and the files in the directory.

2. Select **Do you agree?** to back up the site key that the installer generates.

   The site key generated is a unique key.

   Note: If you lose the site key, you can't generate it again. Make sure that you save a copy of this key and do not share the unique site key with others. Create a backup of the site key before you continue.

3. Click **Next**.

   The **Domain and Node Configuration** page appears.

Configure the node

After you configure the encryption key, you can join the domain and node.

1. Enter the information for the domain and node that you want to join.

   The following table describes the properties that you set for the domain and node.

Property	Description
Node Host name	Host name or IP address of the machine on which to create the node. If the machine has a single network name, use the default host name. If the machine has multiple network names, you can modify the default host name to use an alternate network name. **Note:** The node host name can't contain the underscore (_) character. Use a name that explicitly identifies the machine. Don't use localhost.
Node Name	Name of the node to create.
Node Port Number	Port number for the node. The default port number for the node is 6005. If the port number is not available on the machine, the installer displays the next available port number.

2. Select whether to display the advanced port configurations for the domain and node components assigned by the installer.

   If you disable the port configurations option, the installer does not display the port configurations.

   If you enable the port configurations option, the **Port Configuration** section appears.

   The installer displays the default port numbers assigned to the domain components.
   You can specify the port numbers to use for the domain and node components. You can also specify a range of port numbers to use for the service process that will run on the node. You can use the default port numbers or specify new port numbers. Verify that the port numbers you enter are not used by other applications.
3. Select whether you want to configure the CDI-PC Repository Service and CDI-PC Integration Service during the installation.
4. If you don't want to configure the CDI-PC Repository Service and CDI-PC Integration Service, click **Next**.

   You can exit the installer and configure the services later from the Administrator tool.

   Skip to the "After you create the domain" on page 70 section to continue.
5. If you choose to create the services from the installer, the CDI-PC Repository Service and CDI-PC Integration Service section appears.

   To create the services, you first log in to Informatica Intelligent Cloud Services and register the domain on the CDI-PC **Home** page.

   You can keep the installer window open and continue after you register the domain.

   For information about how to register the domain, see "Register the domain in CDI-PC " on page 70.

The **Post-Installation Summary** page indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

Configure the ports

You can update the port numbers for the Service Manager and Informatica Administrator.

1. On the **Port Configuration** page, enter the port numbers to use for the domain service manager and service processes that will run on the node.

   Verify that the port numbers you enter are not used by other applications.
   The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.

Port	Description
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

2. Click **Next**.

   The **Windows Service Configuration** page appears.

Configure Windows service

1. If you do not select to display the port configuration page, the **Windows Service Configuration** page appears.
2. Select whether to run the Windows service under a different user account.

   The installer creates a service to start Informatica. By default, the service runs under the same user account as the account used for installation. You can run the Windows service under a different user account.

   The following table describes the properties that you set to run Informatica under a different account:

Property	Description
Run Informatica under a different user account	Indicates whether to run the Windows service under a different user account.
User name	User account with which to run the Informatica Windows service. Use the following format: `<domain name>\<user account>` This user account must have the Act as operating system permission.
Password	Password for the user account with which to run the Informatica Windows service.

3. Click **Next**.

   If you do not choose to create the services, the installer displays the **Post-Installation Summary** page. The **Post-Installation Summary** page indicates whether the installation completed successfully.

CDI-PC Repository Service and the CDI-PC Integration Service

If you paused the installation to register the domain, you can configure the CDI-PC Integration Service and the CDI-PC Repository Service from the installer.

1. Choose the database to configure for the CDI-PC repository.

You can configure the CDI-PC repository with one of the following databases:

- Oracle
- Microsoft SQL Server
- IBM DB2
- PostgreSQL
- Sybase

Default is Oracle.

2. Enter the properties for the database user account.

   The following table lists the properties for the database user account:

Property	Description
Database user ID	Name for the CDI-PC repository database user account.
User password	Password for the CDI-PC repository database user account.
Database service name	Service or database name for the CDI-PC repository: - Oracle. Enter the service name. - Microsoft SQL Server. Enter the database name. - IBM DB2. Enter the service name. - PostgreSQL. Enter the database name. - Sybase. Enter the database name.
Database host name	Enter the CDI-PC repository database host name. Required for Microsoft SQL Server.

3. Enter a name for the CDI-PC Repository Service.
4. Enter a name for the CDI-PC Integration Service.
5. Select the CDI-PC Repository Service code page. Default is 7-bit ASCII.
6. Select the CDI-PC Integration Service code page. Default is 7-bit ASCII.

The **Post-Installation Summary** section indicates whether the installation completed successfully. The summary also shows the status of the installed components and their configuration.

Click **Done** to exit the installer. If you use other services, you can create them in Informatica Administrator or run an infacmd command to create the services.

Post-installation step for PowerExchange

After installing CDI-PC on an additional node that you join to the domain, if you use PowerExchange and you do not use the default dbmover.cfg location of usr/config/pwx, you must specify the dbmover.cfg location in one of the following ways before starting the CDI-PC node or running the script that starts CDI-PC:

- Set the PWX_CONFIG parameter to point to the dbmover.cfg location in the usr/config/pwx/overrides.cfg file.
- Set the PWX_CONFIG environment variable to point to the PowerExchange dbmover.cfg configuration file location on the machine where you installed the client.

CDI-PC searches for the dbmover.cfg file in the following order:

1. The PWX_CONFIG parameter in the usr\config\pwx\overrides.cfg file
2. The PWX_CONFIG environment variable
3. The usr\config\pwx\dbmover.cfg file

Note: If the CDI-PC Integration Service is running when you set the environment variable, you'll need to restart it for the environment variable to take effect.

Configure JVM parameters

CDI-PC includes script files that you can use to set environment variables used in infaservice and infasetup commands.

You can use script files, infasetupconfig.sh and infaserviceconfig.sh, to set environment variables. You can find the script files in the following location: `<CDI-PC installation directory>/Informatica/platform/usr/bin/`

If you use environment variables such as INFA_JAVA_OPTS or INFA_JAVA_CMD_OPTS to set customized values for JVM parameters that infaservice and infasetup commands use, set the variables and values in the configuration file for each command.

For example, to set the maximum heap size to 4 GB for each of the commands, configure each file as follows:

- infaserviceconfig.sh. `INFA_JAVA_OPTS="-Xmx4096m -XX:MaxMetaspaceSize=256m ${INFA_JAVA_OPTS}"`
- infasetupconfig.sh. `INFA_JAVA_CMD_OPTS="-Xmx4096m -XX:MaxMetaspaceSize=128m ${INFA_JAVA_CMD_OPTS}"`

Note: Any values that you edit in the infasetup.sh and infaservice.sh files might be overwritten when you apply updates.

CHAPTER 6

Run the silent installer

To install without user interaction, install in silent mode. Use a properties file to specify the installation options. The installer reads the file to determine the installation options.

Copy the installation files to the machine where you plan to create or join the domain. If you install on a remote machine, verify that you can access and create files on the remote machine.

To install in silent mode, complete the following tasks:

1. Configure the installation properties file and specify the installation options in the properties file.
2. Run the installer with the installation properties file.
3. After the install succeeds, perform the post-install steps.
   a. Register the domain on the CDI-PC Home page in Informatica Intelligent Cloud Services.
   b. Log in to the Administrator tool and create the services. Wait for at least a minute to log in to the Administrator tool to create the services.

Create the properties file

Informatica provides a SilentInput.properties installation properties file. The file is stored in the installer download directory. Use the properties file to create or join a CDI-PC domain without user interaction.

The file contains default values for many configuration properties. You can customize the file to specify your options. After you customize the file, save it with the file name SilentInput.properties.

1. Go to the root of the directory that contains the installation files.
2. Find the SilentInput.properties file and back it up.
3. Use a text editor to open the SilentInput.properties file and update the property values.

   The properties file contains property descriptions and default values where applicable.
4. Save the properties file with the name SilentInput.properties.

Run the installer in silent mode on Linux

After you configure the properties file, open a Linux shell to start the silent installation.

1. Go to the root of the directory that contains the installation files.
2. Verify that the directory contains the SilentInput.properties file that you edited and saved.

3. Run the following command to start the silent installation: `./silentinstall.sh`

   The silent installer runs in the background. The process can take a while. The installation is complete when install log file is created in the following location: `<CDI-PC installation directory>/informatica/`.

The silent installation fails if you incorrectly configure the properties file or if the installation directory is not accessible. Correct errors in the error log and run the silent installation again. You can find the error log in the following location: `<CDI-PC installation directory>/informatica/`

Perform the post-requisite steps to complete the installation.

Run the installer in silent mode on Windows

After you configure the properties file, open a command prompt to start the silent installation.

1. Go to the root of the directory that contains the installation files.
2. Verify that the directory contains the SilentInput.properties file that you edited and saved.
3. Run the silent installation.

   The silent installer runs in the background. The process can take a while. The installation is complete when install log file is created in the following location: `<CDI-PC installation directory>/informatica/`.

The silent installation fails if you incorrectly configure the properties file or if the installation directory is not accessible. Correct errors in the error log and run the silent installation again. You can find the error log in the following location: `<CDI-PC installation directory>/informatica/`

Perform the post-requisite steps to complete the installation.

CHAPTER 7

Resuming an installation

If you paused the installation to register the domain, you can resume the installation process to configure the CDI-PC Integration Service and the CDI-PC Repository Service from the installer. After domain configuration, if the installation process stops midway, you can resume the installation from the point of failure or exit.

When the service installation process fails, you can resume from the previous service configuration and recover the last entered details for that service installation. The install process might fail for reasons such as network outage, when you exit the installation before completing the entire installation process, or because of incorrect information entered.

Consider the following guidelines for resuming the installation:

- If a service fails or if the installation process fails during a service creation, you can resume the installation process with the server installer. To resume the installation process, ensure that the domain is up and running from the installation log.
  To resume the installation, run the installer again.

  When you resume the installer while creating a service, the installer retains all the service and database specific information, such as the create service status, service name, service enabled or disabled status. You can confirm and use the previously entered values or specify new values for the service and resume the installation process.
- You cannot resume the installer to join a domain or migrate a domain.

Before you resume the installer

When the installation process stops midway, you can resume the installation from the point of failure or exit.

Before you can resume the installer, complete the following prerequisites:

1. In the installation log file present in the installation directory, verify that the domain is created. You can find the error log in the following location: `<CDI-PC installation directory>/informatica/`
2. Ensure that you do not delete the `installInst.obj` object file present in the tools folder of the user installation directory.
3. To resume the installation through the silent installer, ensure that `RESUME_INSTALLATION` is set to true in the `SilentInput.properties` file.

Resuming the installer in console mode

After you complete prerequisite tasks, you can resume the installer in console mode.

1. Open a command prompt and navigate to the location of the installation files.
2. Run the console installer.
3. When the regular installer runs, you might get a prompt confirming whether you want to resume previous installer or not.
   - If you do not want to resume installation, enter 1 for No. Default is 1.
   - If you want to resume installation, enter 2 for Yes.

Resuming the installer in graphical mode

After you complete prerequisite tasks, you can resume the installer in graphical mode.

1. Log in to the machine with a system user account.
2. Close all the other applications.
3. Go to the root of the directory for the installation files and run `install.bat` as administrator.

   To run the file as administrator, right-click the `install.bat` file and select **Run as administrator**.

   Note: If you do not run the installer as administrator, the Windows system administrator might encounter issues when accessing files in the CDI-PC installation directory.

   The CDI-PC page appears.
4. Select **Install CDI-PC**.
5. Click **Start**.

   The **Welcome** page appears.
6. Read the copyright information.
7. Select the option to resume the install process.
8. Click **Next**.

   The installation starts and resumes the service creation process.

Resuming the installer in silent mode

After you complete prerequisite tasks, you can resume the installer for silent installation.

To resume the installation through the silent installer, ensure that `RESUME_INSTALLATION` is set to true in the `SilentInput.properties` file.

1. Go to the root of the directory that contains the installation files.
2. Verify that the directory contains the SilentInput.properties file that you edited and saved.

3. Run the silent installation.

   The silent installer runs in the background. The process can take a while. The installation is complete when install log file is created in the following location: `<CDI-PC installation directory>/informatica/`.

CHAPTER 8

Before you migrate the Informatica domain

Before you run the installer to migrate the Informatica domain to a CDI-PC domain, perform the prerequisite tasks. You can migrate the domain on the same machine or to a different machine. The prerequisite tasks differ based on how you choose to migrate the domain.

A CDI-PC domain uses TLS with host name verification. You can use existing custom TLS certificates if they contain SAN entries for host details. If the custom TLS certificates don't contain SAN entries, generate custom TLS certificates before you migrate the domain. You can't use default certificates included with the Informatica domain. After you migrate, you can't convert a CDI-PC domain to non TLS or change the certificates to the default certificates that you used with the Informatica domain.

Before you migrate the Informatica domain, truncate the PowerCenter workflow and sessions logs. Use the `pmrep TruncateLog` command or the Repository Manager to remove workflow and session logs from the repository. The `TruncateLog` command increases performance by reducing the time that it takes the PowerCenter repository to access and write to the logs. Run the `pmrep UpdateStatistics` command immediately before and after you truncate workflow and session logs.

Shut down the domain and back up the domain configuration metadata before you migrate.

Note: Although the installer backs up the domain configuration during migration, it doesn't back up the domain if you choose to migrate to a different host or update domain configuration details.

If the Informatica domain has multiple nodes, migrate a gateway node first and then migrate other nodes.

You can't migrate an Informatica domain with the following specifications:

- Application services other than the following services:
  - PowerCenter Repository Service
  - PowerCenter Integration Service
  - Web Services Hub Service
  - PowerCenter SAP BW Service
  - PowerExchange Listener Service
  - PowerExchange Logger Service

Copy folders to a common location

The migration process copies most, but not all, of the Informatica files to the CDI-PC domain. The migration process doesn't migrate files in the infa_shared folder or custom keystore and truststore files.

To ensure that you can access the files after you migrate, copy the files to a common location before you migrate.

Migrated files and directories

The migration process migrates the following files and directories within the Informatica installation directory:

/server/bin/sapnwrfc.ini/

/server/ComparisonUtility.url/

/tomcat/bin/ner/

/tomcat/bin/classifier/

/tomcat/shared/classes/idp.properties/

/tomcat/bin/target/

/tomcat/bin/scheduler/temp/

/isp/bin/plugins/sats/com.informatica.ilm.sats.ispservice.cmdcli.jar/

/plugins/acplugins/com.informatica.ilm.sats.ispservice.adminconsole.jar/

DataTransformation/CMConfig.xml

DataTransformation/autoInclude/user

DataTransformation/externLibs/user

DataTransformation/ServiceDB

DataTransformation/CDELicense.cfg

isp/config/nodemeta.xml

<KEY_SRC_LOCATION>/sitekey

Non-migrated files and directories

The migration process doesn't migrate files in the following infa_shared directory:

/SrcFiles

/log

/WorkflowLogs

/TgtFiles

/SessLogs

/LkpFiles

/Cache

/BadFiles

/Backup

/BWParam

/Storage

/Temp

Custom keystore and truststore files

If you store your custom keystore and truststore certificates within the Informatica installation directory, complete the following tasks:

1. Move the files to a location accessible to the machine where you create the CDI-PC domain.
2. Update the INFA_KEYSTORE and INFA_TRUSTSTORE environment variable values.

If the CDI-PC domain domain can't access the certificates, you won't be able to register the domain after you migrate.

Set up keystore and truststore files for the CDI-PC domain

CDI-PC requires a TLS setup with custom certificates. You can't use the default certificates available with the Informatica domain. Generate keystore and truststore certificates to use with CDI-PC. If you use custom certificates that don't include SAN information for host name validation in your Informatica domain, you can't use the same certificates.

Set up files for secure communication within the CDI-PC domain and for a secure connection to the Administrator tool and Secure Agent. CDI-PC requires certificates configured for host name validation. Ensure that the host name mentioned in the certificate matches the host that you apply it on. To create the required files, you can use the following programs:

keytool

You can use keytool to create a TLS certificate or a Certificate Signing Request (CSR) as well as keystores and truststores in JKS format.

OpenSSL

You can use OpenSSL to create a TLS certificate or CSR as well as convert a keystore in JKS format to PEM format.

For more information about OpenSSL, see the documentation on the following website: https://www.openssl.org/docs/

For a higher level of security, send your CSR to a Certificate Authority (CA) to get signed certificates. If you use CA-signed certificates, you get a certificate chain with an ordered list of certificates that include the root certificate, one or more intermediate certificates, and the user certificate. Enter all certificates in the chain when you generate the PEM format.

For information about how to generate and configure custom keystore and truststore certificates, see the following KB article: Configure keystore and truststore for Cloud Data Integration for PowerCenter

The software available for download at the referenced links belongs to a third party or third parties, not Informatica. The download links are subject to the possibility of errors, omissions or change. Informatica assumes no responsibility for such links and/or such software, disclaims all warranties, either express or implied, including but not limited to, implied warranties of merchantability, fitness for a particular purpose, title and non-infringement, and disclaims all liability relating thereto.

Secure communication within the domain

Before you enable secure communication within the domain, verify that the following requirements are met:

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

Note that RSA encryption requires more than 512 bits.

You have a signed TLS certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into keystores.

Ensure that you have keystores in the following formats:

- PEM format, named infa_keystore.pem
- JKS format, named infa_keystore.jks

If you use CA-signed certificates, ensure that the keystore files contain the root and intermediate TLS certificates.

Note: Use the same password for the keystore in JKS format and the private key pass phrase used to generate the TLS certificate.

You imported the certificate into truststores.

Ensure that you have truststores in the following formats:

- PEM format, named infa_truststore.pem
- JKS format, named infa_truststore.jks

Ensure that the truststore files contain the root, intermediate, and end user TLS certificates.

The keystores and truststores are in the correct directory.

Ensure that the keystore and truststore are in a directory that is accessible to the installer.

Secure connection to the Administrator tool

Before you secure the connection to the Administrator tool, verify that the following requirements are met:

You created a certificate signing request (CSR) and private key.

You can use keytool or OpenSSL to create the CSR and private key.

Note that RSA encryption requires more than 512 bits.

You have a signed TLS certificate.

The certificate can be self-signed or CA signed. Informatica recommends a CA signed certificate.

You imported the certificate into a keystore in JKS format.

A keystore can't contain more than one certificate. If you use a unique certificate for each web application service, create a separate keystore for each certificate. Alternatively, you can use a shared certificate and keystore.

Update the node to add or replace the certificates

If you plan to migrate the domain to a different machine, you need to ensure that the domains uses TLS protocol and to add or replace existing certificates with the ones that you generated.

Convert the domain to use TLS

If the domain doesn't use TLS protocol, run the following infacmd to convert it to TLS:

```
./infacmd.sh updateDomainOptions -dn <domain name> -un <user name> -pd <password> -sdn
<security domain> -do TLSMode=true
```

Add or replace certificates

To add or replace TLS certificates with the ones that you generated, perform the following tasks:

1. Shut down the domain.
2. Run the following command infasetup command:

```
./infasetup.sh updateGatewayNode -tls true
-nk <Custom keystore directory>
-nkp <The keystore .jks file password>
-nt <Custom truststore directory>
-ntp <truststore .jks file password>
-hs <HTTPS port number to secure connection to the Administrator tool>
-kf <Keystore file that contains the keys and certificates>
-kp <A plain-text password for the keystore file>
```

3. Start the domain.

Run the TLS Utility to validate the certificates

CDI-PC requires valid custom keystore and truststore certificates to secure communication between Informatica Intelligent Cloud Services and the domain, and between the domain and clients. The TLS utility verifies that the certificates are valid for communication between two hosts. You can choose to run the utility to validate your certificates.

1. Download the TLS utility from Informatica Intelligent Cloud Services.

   For information about how to download the utility, see "Download the installers from Informatica Intelligent Cloud Services" on page 11
2. Copy the certificates that you want to validate to the same machine.

   After you validate the certificates, you can copy them to the host machine.
3. Extract the ZIP file to any location on the machine.
4. Open a command prompt from the directory where you extracted the utility, and run the following command to start the utility:

   ```
   java -jar CDI-PC_TLS_Utility.jar
   ```

   The utility prompts you for the details of the first host.
5. Enter certificate details of the domain, Secure Agent, or CDI-PC Client machine.

   If you have multiple domain nodes or multiple Secure Agents, enter the certificate details of all the domain, Secure Agent, or CDI-PC Client machines.
6. Enter the following details for the first host and press **Enter** after each entry:
   - First host keystore path. The absolute path to the keystore file on the first host.

- First host keystore password. The keystore password.
- First host truststore path. The absolute path to the truststore file on the first host.
- First host truststore password. The keystore password.
- First host DNS or IP address. The DNS or IP address of the host on which you use the certificate. If you enter the DNS, enter the fully qualified host name and the short name of the host. Enter comma-separated values. If the certificate includes wildcards in the host details, enter the DNS information for each host on which you use the certificate.

7. Enter the details for the second host.

   With details of both hosts, the utility tries to connect from the first host to the second host and verifies the host entries in the certificates against details entered. If the second host certificates are present on the first host and host entries are validated, the utility returns a message to indicate that the validation is successful.

8. If the certificates of the second host are not present in the truststore of the first host, you can choose whether you want the utility to import the certificates. The import modifies the truststore of the first host. Enter `Y` to import the certificates and continue or `N` to exit.

   If you choose to import the certificates, the utility imports the certificates and continues the validation.

9. The utility then tries to connect from the second host to the first host. If connection and host entry verification succeed, the utility returns a successful validation message. You might be prompted to import the certificates of the first host into the second host if they aren't present in the truststore of the second host.

   If connection and host entry verification succeed, the utility returns a successful validation message.

Back up the PowerCenter repository

Back up the PowerCenter repository if you want to migrate it to a different database.

1. Log in to the Administrator tool.
2. Select the Repository Service.
3. Click **Domain Actions** > **Repository Contents** > **Backup**.

Back up essential Data Transformation files

Before you run the installer to migrate Informatica domain to a CDI-PC domain, you must back up the Data Transformation files of the Informatica domain. After you complete the installation, copy the files to the new installation directories to get the same custom global components as in the previous version.

The following table lists the files or directories that you must back up:

File or Directory	Default Location
Repository	<Informatica installation directory>\DataTransformation\ServiceDB
Custom Global Components directory (TGP files)	<Informatica installation directory>\DataTransformation\autoInclude\user
Custom Global Components directory (DLL and JAR files)	<Informatica installation directory>\DataTransformation\externLibs\user
Configuration file	<Informatica installation directory>\DataTransformation\CMConfig.xml
License file	<Informatica installation directory>\DataTransformation\CDELicense.cfg

By default, the migration process copies the Data Transformation files to the CDI-PC domain. Do not copy the Data Transformation library files. Instead, install the Data Transformation libraries again.

Shut down the Informatica domain

Shut down the domain before you back it up.

1. Stop all application services.
2. Find the infaservice.sh command. By default, it's in the following location:

   ```
   <Informatica installation directory>/tomcat/bin
   ```

3. Run the following command to stop the daemon:

   ```
   infaservice.sh shutdown
   ```

Back up the Informatica domain

If you migrate from Informatica version 10.4.x and choose to allow node and host configuration changes, the installer doesn't back up the domain. Before you migrate the domain, back up the configuration metadata for the domain.

Perform the following steps to back up the domain:

1. Run the infasetup BackupDomain command to back up the domain configuration database tables to a file.

2. Back up the metadata configuration files.

Back up the domain configuration

Use theinfasetup BackupDomain command to back up the domain. You can find infasetup in the following directory:

```
<Informatica installation directory>/isp/bin
```

To back up the domain with infasetup, use the following syntax:

```
BackupDomain
<<-DatabaseAddress|-da> database_hostname:database_port|

<-DatabaseConnectionString|-cs> database_connection_string>

<-DatabaseUserName|-du> database_user_name

<-DatabasePassword|-dp> database_password

<-DatabaseType|-dt> database_type

[<-DatabaseServiceName|-ds> database_service_name]

<-BackupFile|-bf> backup_file_name

[<-Force|-f>]

<-DomainName|-dn> domain_name

[<-Tablespace|-ts> tablespace_name (used for IBM DB2 only)]

[<-SchemaName|-sc> schema_name (used for Microsoft SQL Server only)]

[<-DatabaseTlsEnabled|-dbtls> database_tls_enabled]

[<-DatabaseTruststorePassword|-dbtp> database_truststore_password]

[<-TrustedConnection|-tc> trusted_connection (used for Microsoft SQL Server only)]

[<-EncryptionKeyLocation|-kl> encryption_key_location]
```

Back up the domain metadata configuration files

Back up the metadata configuration files to any directory accessible by the machines where you migrate the domain.

The following table describes the metadata files and the locations where you can find them:

Metadata File	Description
nodemeta.xml	Contains metadata for a node. Stored in the <Informatica installation directory>/isp/config directory on the node.
domains.infa	Contains connectivity information for the gateway nodes. Stored in one of the following locations: - The Informatica installation directory on the client and server machines. - The location configured through the INFA_DOMAINS_FILE environment variable.

Import the CDI-PC domain truststore certificates to the Secure Agent truststore

Put the domain certificates on the Secure Agent machine to ensure that the Secure Agent can communicate with the domain.

If you ran the TLS utility to validate your certificates, you don't need to perform this task. The TLS utility validates the certificates and verifies that the domain and the Secure Agent can communicate. The verification process exchanges the certificates if they aren't already present.

To import the CDI-PC domain certificates to the Secure Agent truststore, run the following command:

```
keytool -importcert -file <absolute path to the domain certificate file>.crt -keystore
<JKS Truststore name>.jks -alias <Any other alias name> -deststoretype JKS -v -
trustcacerts
```

CHAPTER 9

Migrate the domain

You can run the installer to migrate an Informatica domain to a CDI-PC domain. To migrate, you enter details of the Informatica domain and the directory where you want to create a CDI-PC domain. You also configure secure communication for the domain.

If you are migrating a multi-node domain, shut down all nodes except one gateway node before you migrate. If you shut down all gateway nodes, the migration process doesn't run.

Migrate the gateway nodes before you migrate the worker nodes.

You can't use the backup of an Informatica domain to create a CDI-PC domain. The restore of a 10.4.x domain generates an error. No error appears if you restore the backup of a 10.5.0, 10.5.1, 10.5.2, 10.5.3, 10.5.4, or 10.5.5 domain, but the domain doesn't work as expected. To migrate an Informatica domain, run the installer and choose the option to migrate.

You can migrate a domain in console mode, graphical mode, or silent mode. Use the same user account to migrate that you used to install Informatica services. Ensure that you review and complete all prerequisite tasks before you start the migration. After you migrate the domain, perform all post-requisite tasks to ensure that you can start the domain and view the migrated services in the Administrator tool.

You can restore the following versions of PowerCenter repository to a CDI-PC repository:

- 10.4.x

  To restore 10.4.x PowerCenter repository, migrate the PowerCenter domain containing such repositories to CDI-PC domain first, and then upgrade the repositories to CDI-PC.
- 10.5.0
- 10.5.1
- 10.5.2
- 10.5.3
- 10.5.4
- 10.5.5

Note: You can migrate Informatica domain versions 10.4.x through 10.5.5.

Run the installer in console mode

Run the installer to migrate an Informatica domain to a CDI-PC domain.

1. Log in to the machine with a system user account.
2. Clear the DISPLAY variable on the machine.

3. Use the unset command to clear the following variables:

   `INFA_HOME`, `INFA_NODE_NAME`, and `INFA_DOMAINS_FILE`
4. Close all the other applications.
5. On a shell command line, run the install.sh file.

   The installer displays the message to verify that the locale environment variables are set.
6. Press **2** to migrate the domain.
7. Read the copyright information and press **Enter** to continue.

Enter the Informatica service directory details

Specify the Informatica installation directory. If migrating from a 10.4.x version, you can specify if you want to allow changes to the node configuration details when you migrate.

1. Enter the absolute path to the Informatica installation directory.
2. Applicable if you migrate an Informatica 10.4.x domain. Choose whether you want to make changes to the node configuration when you migrate.
   a. Enter **1** to allow changes to the host name, port numbers, or domain configuration repository. Enter **2** to migrate the domain without changes to the node configuration.
   b. If you choose to allow changes, choose whether to make changes to the host machine. Enter **1** to allow changes to the host machine or **2** to migrate on the same host machine.

      For information about how to migrate with node configuration changes, see Chapter 10, “Migrate the domain with changes to node configuration” on page 111.

The **Informatica Domain and Node Details** section appears.

Confirm the domain and node details

When you enter the Informatica installation directory, the installer detects and displays the domain details.

1. View the domain details that appear based on the directory that you enter.
2. Enter the domain user name and password to validate the domain details.

   The installer checks the domain for migration requirements and an assessment summary appears.
3. Verify the results of the assessment.

   Depending on the type of migration, the installer checks requirements based on the following factors:

   - Transport Layer Security (TLS)
   - Domain
   - Database and version
   - Operating system
   - Domain services

   For example, all of the checks are performed on the first gateway node that you migrate. On worker nodes and all other gateway nodes, only TLS, domain, and operating system checks are performed. If you choose to allow node and host configuration changes, only some checks are performed on all nodes.

   The results of the migration check are saved to the Summary_<date and time stamp>.log file in the following location: `...<installer directory>/`
4. To continue to migrate, press **Enter** to continue.

The **Migration Directory** section appears.

Enter the migration directory and backup preferences

You can specify the directory where you want to migrate the domain, and whether you want to back up the Informatica domain.

1. Enter the absolute path to the CDI-PC domain installation directory.

   The directory names in the path can't contain spaces or the following special characters:

   ` % * + ; \ / " ? , < > @ # ! %) (} {] [' | &

   Default is the user home directory for the user that runs the installation.

   Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

2. Choose whether you want to back up the Informatica domain.

   Enter **1** to back it up or **2** to continue without backing it up.

   If you choose to back up the domain, you can save the file in the default location or a custom location.

The **Domain Security - Encryption Key** section appears.

Configure encryption key details

The Informatica installation creates a unique site key. When you migrate from an Informatica domain, you use the same site key. The installer detects and displays the absolute path to the encryption key file of the Informatica installation. You specify the directory path where you want to copy the encryption key for the CDI-PC domain.

1. Verify the path to the Informatica domain encryption key file.
2. Enter the full path to the directory to store the CDI-PC domain encryption key. You can choose the default location or enter a custom path.
3. Applicable if you migrate from a version that either doesn't use TLS or uses TLS with the Informatica default TLS certificates. Enter the following information:
   - The HTTPS port to connect to the Administrator tool. Default is 8443.
   - The absolute path to the custom keystore file.
   - The keystore password.
   - The full path to the directory that contains the custom keystore files to secure communication within the domain.
   - The truststore password.
   - The full path to the directory that contains the custom truststore files to secure communication within the domain.
   - The truststore password.
4. If you are migrating from Informatica 10.4.x, view the domain details in the **Domain Configuration Repository** section.
5. Press **Enter** to start the migration.

   When the migration completes, the **Post-migration Summary** page appears with the migration status, log file, and domain information. A migration log file is generated in the following location: `<CDI-PC installation directory>/Informatica`.
6. Press **Enter** to exit the installer.

Before you can log in to the Administrator tool to view the migrated services, perform all post-requisite tasks. For more information, see Chapter 12, “After you migrate the domain” on page 131.

Run the installer in graphical mode

Run the CDI-PC domain installer to migrate an Informatica domain to a CDI-PC domain.

1. Log in to the machine with a system user account.
2. Close all the other applications.
3. Go to the root of the directory for the installation files and run `install.bat` as administrator.

   To run the file as administrator, right-click the `install.bat` file and select **Run as administrator**.

   Note: If you do not run the installer as administrator, the Windows system administrator might encounter issues when accessing files in the CDI-PC installation directory.

   The CDI-PC page appears.
4. Select **Migrate to CDI-PC**.
5. Click **Start**.

   The **Welcome** page appears.
6. Read the copyright information and click **Next** to continue.

   The **Migration Prerequisites** page displays the installation requirements. Verify that all requirements are met before you continue the installation.
7. Click **Next**.

   The **Informatica Services Installation Directory** page appears.

Enter the Informatica service directory details

Specify the Informatica installation directory.

1. Enter the absolute path to the Informatica installation directory.
2. Select the necessary options if you want to make changes to the node configuration when you migrate.
   - To configure a new host machine, select the option to change the node host name, port numbers, or domain configuration repository.
   - To allow changes to the node configuration during migration, select the option to change the host machine configuration.
3. Click **Next**.

   The **Informatica Domain and Node Details** page appears.

Confirm the domain and node details

When you enter the Informatica installation directory, the installer detects and displays the domain details.

1. View the domain details that appear based on the directory that you enter.
2. Enter the domain user name and password to validate the domain details.

   The installer checks the domain for migration requirements and an assessment summary appears.
3. Verify the results of the assessment.

   Depending on the type of migration, the installer checks requirements based on the following factors:
   - Transport Layer Security (TLS)
   - Domain

- Database and version
- Operating system
- Domain services

For example, all of the checks are performed on the first gateway node that you migrate. On worker nodes and all other gateway nodes, only TLS, domain, and operating system checks are performed. If you choose to allow node and host configuration changes, only some checks are performed on all nodes.

The results of the migration check are saved to the Summary_<date and time stamp>.log file in the following location: `...<installer directory>/`

4. To continue to migrate, click **Next**.

   The **Migration Directory** page appears.

Enter the migration directory and backup preferences

You can specify the directory where you want to migrate the domain, and whether you want to back up the Informatica domain.

1. Enter the absolute path to the CDI-PC domain installation directory.

   The directory names in the path can't contain spaces or the following special characters:

   ` % * + ; \ / " ? , < > @ # ! %) (} {] [' | &

   Default is the user home directory for the user that runs the installation.

   Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

2. Choose whether you want to back up the Informatica domain.
3. If you choose to back up the domain, enter the path where you want to save the backup file. You can save the file in the default location or a custom location.
4. Click **Next**.

   The **Domain Security - Encryption Key** page appears.

Configure secure communication

The Informatica installation creates a unique site key. When you migrate from an Informatica domain, you use the same site key. The installer detects and displays the absolute path to the encryption key file of the Informatica installation. You specify the directory path where you want to copy the encryption key for the CDI-PC domain.

1. Verify the path to the Informatica domain encryption key file.
2. Enter the full path to the directory to store the CDI-PC domain encryption key. You can choose the default location or enter a custom path.
3. Applicable if you migrate from a version that either doesn't use TLS or uses TLS with the Informatica default TLS certificates. Enter the following information:
   - The HTTPS port to connect to the Administrator tool. Default is 8443.
   - The absolute path to the custom keystore file.
   - The keystore password.
   - The full path to the directory that contains the custom keystore files to secure communication within the domain.

- The truststore password.
- The full path to the directory that contains the custom truststore files to secure communication within the domain.
- The truststore password.

4. If you are migrating from Informatica 10.4.x, view the domain details in the **Domain Configuration Repository** section.
5. Click **Next**.

   The **Migration Summary** page appears.
6. Verify the installation details and click **Install**.

   When the migration completes, the **Post-migration Summary** page appears with the migration status, log file, and domain information. A migration log file is generated in the following location: `<CDI-PC installation directory>/Informatica`.
7. Exit the installer.

Perform all post-requisite tasks before you can log in to the Administrator tool to view the migrated services. For more information, see the Chapter 12, “After you migrate the domain” on page 131.

CHAPTER 10

Migrate the domain with changes to node configuration

To prepare for the migration, you'll perform tasks based on the kind of change that you plan to make to the node configuration. You can migrate the domain configuration repository to a different database. Or, you can migrate the Informatica services installation to a different machine.

You can choose to change the node configuration to allow changes to the node host name, port numbers, or domain configuration repository database.

To migrate an Informatica services installation to a different machine, choose to change the node configuration and configure the node on the new machine. To migrate the domain configuration repository to a different database, choose to change the node configuration to configure the new database.

Complete the pre-migration tasks before you run the installer.

Migrate the gateway nodes before you migrate the worker nodes.

Migrate the domain configuration repository to a different database

If the domain configuration repository database type or version is not supported, migrate the repository to a different supported database. Migrate the repository in the Informatica instance before you migrate the domain.

Perform the following tasks to migrate the repository to a different database:

1. Shut down the domain.
2. Verify that you backed up the domain configuration database tables to a file with the infasetup BackupDomain command.
3. Create a database schema and a user account in a supported database.
4. Run i10Pi from the installer with the database user account created to test whether the installation supports the different database. Verify that i10Pi shows the database users as supported for the version to which you are about to migrate. For more information about the i10Pi configuration, see "Run the pre-installation system check tool in console mode" on page 35.
5. Restore the domain configuration in the backup file to the specified database schema with the infasetup RestoreDomain command or from Informatica Administrator.

6. Run the installer to migrate.
   When you migrate a gateway node, select the **Allow changes to the node host name and port number** option. When you select this option, you can configure the gateway node to connect to the new domain configuration repository database. All gateway nodes require a connection to the domain configuration repository to retrieve and update the domain configuration. When you migrate a worker node, clear the **Allow changes to the node host name and port number** option. The installer prompts for a confirmation on whether you want to change the host. Enter the option for No if you don't want to change the host, else enter the option for Yes.

Migrate the installation to a different machine

If the Informatica domain is running on a machine with an operating system that isn't supported, you must migrate the installation to a different machine before you migrate the domain.

To migrate the domain, complete the following steps on the machine where you want to migrate to CDI-PC:

1. Run i10Pi from the installer to test the installation support of the new machine. For information, see "Run the pre-installation system check tool in console mode" on page 35.
2. Copy the installation directory with all the installation binaries from the previous machine to the new machine.
3. Verify port requirements.
4. Create a system user account.
5. Configure native connectivity for all services that require access to databases.
6. Install database client software.
7. Configure database client environment variables.
8. Run the installer to migrate to a different machine.
   When you migrate a gateway node, select the **Allow changes to the node host name and port number** option. When you upgrade a worker node, clear the **Allow changes to the node host name and port number** option.

Copy the installation directory

Copy the directory of the Informatica version that you want to migrate to the target machine.

1. Shut down the domain.
2. Copy the directory and subdirectories maintaining the same directory structure as the Informatica domain.

When you run the installer, specify the installation directory on the new machine as the one where you want to migrate.

Verify port requirements

The installer sets up the ports for components in the domain and it designates a range of dynamic ports to use for some application services.

You can specify the port numbers to use for the components and a range of dynamic port numbers to use for the application services. You can choose to use the default port numbers provided by the installer. Verify that the port numbers are available on the machines where you install the Informatica services.

The following table describes the port numbers that you can set:

Port	Description
Node port	Port number for the node created during installation. Default is 6005.
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.
Range of dynamic ports for application services	Range of port numbers that can be dynamically assigned to application service processes as they start up. When you start an application service that uses a dynamic port, the Service Manager dynamically assigns the first available port in this range to the service process. The number of ports in the range must be at least twice the number of application service processes that run on the node. Default is 6014 to 6114.
Static ports for application services	Static ports have dedicated port numbers assigned that do not change. When you create the application service, you can accept the default port number, or you can manually assign the port number.

Note: Services and nodes can fail to start if there is a port conflict. You can update the range of ports for application services after you migrate.

Configure native connectivity on service machines

To establish native connectivity between an application service and a database, install the database client software for the database that you want to access.

Native drivers are packaged with the database server and client software. Configure connectivity on the machines that need to access the databases. To ensure compatibility between the application service and the database, install the client software associated with relational source systems and the repository databases.

The following table describes where to install the client software and configure connectivity:

CDI-PC Integration Service Configuration	Where to configure
On a single node or on primary and back-up nodes	All machines that run the CDI-PC Integration Service
On a grid	All machines that represent a node with the compute role or with both the compute and service roles

Install database client software

Install the database clients on the required machines based on the types of databases that the application services access.

To ensure compatibility between the application service and the database, use the database client libraries and install a client software that is compatible with the database version.

Install the following database client software based on the type of database that the application service accesses:

IBM DB2 Client Application Enabler (CAE)

Configure connectivity on the required machines by logging in to the machine as the user who starts Informatica services.

Microsoft SQL Server 2014 Native Client

Install the Microsoft SQL Server 2014 Native Client for the existing mappings to work.

Download the client from the Microsoft website.

Oracle Client

Install compatible versions of the Oracle client and Oracle database server. Install the same version of the Oracle client on all machines that require it. To verify compatibility, contact Oracle.

PostgreSQL Client (psql)

Install and run psql, a terminal-based front-end to PostgreSQL that allows you to interactively enter, edit, and run SQL commands.

Install and run the software dependency packages to build PostgreSQL, such as GCC compiler package, readline and readline-devel packages, and zlib-devel compression library package.

You can also run the required library files with the yum install commands.

For more information about psql, see psql client documentation.

PostgreSQL on Linux

Install the following PostgreSQL libraries:

```
postgresql10-10.10-1PGDG.rhel7.x86_64
postgresql10-libs-10.10-1PGDG.rhel7.x86_64
```

Sybase Open Client (OCS)

Install an Open Client version that is compatible with the Sybase ASE database server. You must also install the same version of Open Client on the machines hosting the Sybase ASE database and Informatica. To verify compatibility, contact Sybase.

Run the installer in console mode

When you migrate from Informatica versions 10.4.x, you can change the node configuration to migrate the domain to a different machine or to a different domain configuration repository database.

When you run the installer in console mode, the words Quit and Back are reserved words. Don't use them as input text.

1. Log in to the machine with a system user account.
2. Clear the DISPLAY variable on the machine.
3. Use the unset command to clear the following variables:

   `INFA_HOME`, `INFA_NODE_NAME`, and `INFA_DOMAINS_FILE`
4. Close all the other applications.
5. On a shell command line, run the install.sh file.

   The installer displays the message to verify that the locale environment variables are set.
6. Press **2** to migrate the domain.
7. Read the copyright information and press **Enter** to continue.

Enter the Informatica service directory details

Specify the Informatica installation directory. If migrating from a 10.4.x version, you can specify if you want to allow changes to the node configuration details when you migrate.

1. Enter the absolute path to the Informatica installation directory.
2. Choose to make changes to the node configuration when you migrate.
   a. Enter **1** to allow changes to the host name, port numbers, or domain configuration repository.
   b. If you choose to allow changes, choose whether to make changes to the host machine. Enter **1** to allow changes to the host machine or **2** to migrate on the same host machine.

The **Informatica Domain and Node Details** section appears.

Confirm the domain and node details

When you enter the Informatica installation directory, the installer detects and displays the domain details.

1. View the domain details that appear based on the directory that you enter.
2. Enter the domain user name and password to validate the domain details.

   The installer checks the domain for migration requirements and an assessment summary appears.
3. Verify the results of the assessment.

   Depending on the type of migration, the installer checks requirements based on the following factors:
   - Transport Layer Security (TLS)
   - Domain
   - Database and version
   - Operating system
   - Domain services

For example, all of the checks are performed on the first gateway node that you migrate. On worker nodes and all other gateway nodes, only TLS, domain, and operating system checks are performed. If you choose to allow node and host configuration changes, only some checks are performed on all nodes.

The results of the migration check are saved to the Summary_<date and time stamp>.log file in the following location: `...<installer directory>/`

4. To continue to migrate, press **Enter** to continue.

The **Migration Directory** section appears.

Enter the migration directory

Specify the directory where you want to migrate the domain.

- Enter the absolute path to the CDI-PC domain installation directory.

  The directory names in the path can't contain spaces or the following special characters:

  ` % * + ; \ / " ? , < > @ # ! %) (} {] [' | &

  Default is the user home directory for the user that runs the installation.

  Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

The **Domain Security - Encryption Key** section appears.

Configure secure communication

The Informatica installation creates a unique site key. When you migrate from an Informatica domain, you use the same site key. The installer detects and displays the absolute path to the encryption key file of the Informatica installation. You specify the directory path where you want to copy the encryption key for the CDI-PC domain.

1. Verify the path to the Informatica domain encryption key file.
2. Enter the full path to the directory to store the CDI-PC domain encryption key. You can choose the default location or enter a custom path.
3. Applicable if you migrate from a version that either doesn't use TLS or uses TLS with the Informatica default TLS certificates. Enter the following information:
   - The HTTPS port to connect to the Administrator tool. Default is 8443.
   - The absolute path to the custom keystore file.
   - The keystore password.
   - The full path to the directory that contains the custom keystore files to secure communication within the domain.
   - The truststore password.
   - The full path to the directory that contains the custom truststore files to secure communication within the domain.
   - The truststore password.

The **Domain Configuration Repository** section appears. You can configure the domain configuration repository details and port number details.

Configure the domain configuration repository

If you chose to make configuration changes to the repository, you can configure the domain configuration repository.

1. Select the database for the domain configuration repository details.

   The following table lists the databases you can use for the domain configuration repository:

Prompt	Description
Database type	Type of database for the domain configuration repository. Select from the following options: - 1 - Oracle - 2 - SQL Server - 3 - DB2 - 4 - Sybase - 5 - PostgreSQL Default is Oracle.

2. Enter the properties for the database user account.

   The following table lists the properties for the database user account:

Property	Description
Database User ID	Name for the domain configuration database user account.
User Password	Password for the domain configuration database user account.

3. If you do not create a secure domain configuration repository, enter the parameters for the database.

   a. If you select **IBM DB2**, select whether to configure a tablespace and enter the tablespace name.

Property	Description
Configure tablespace	In a single-partition database, if you select **No**, the installer creates the tables in the default tablespace. In a multi-partition database, you must select **Yes**. Select whether to specify a tablespace: - 1 - No - 2 - Yes
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single-partition database, enter the name of the tablespace in which to create the tables. In a multi-partition database, specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

   b. If you select **Microsoft SQL Server** or **PostgreSQL**, enter the schema name for the database.

      Enter the name of the schema that will contain the domain configuration tables. If the parameter is blank, the installer creates the tables in the default schema.

4. Choose whether to enter secure database parameters.

   You can create a domain configuration repository in a database secured with TLS. To enter secure database parameters, press **1**. If you don't want to enter secure database parameters, press **2**.

5. If you create a secure domain configuration repository, enter the parameters for the secure database.

   The following table describes the options available to create a secure domain configuration repository database:

Property	Description
Database Truststore File	Absolute path to the truststore file for the secure database.
Database Truststore Password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

   The following table describes the secure database parameters to configure:

Database parameter	Description
EncryptionMethod	Required. Indicates whether data is encrypted when transmitted over the network. Set to `SSL`.
ValidateServerCertificate	Optional. Indicates whether Informatica validates the certificate that the database server sends. If this parameter is set to True, Informatica validates the certificate that the database server sends. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate. If this parameter is set to False, Informatica doesn't validate the certificate that the database server sends. Informatica ignores any truststore information that you specify
HostNameInCertificate	Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the certificate.
cryptoProtocolVersion	Required. Specifies the cryptographic protocol to use to connect to a secure database. Based on the cryptographic protocol used by the database server, set to one of the following values: - cryptoProtocolVersion=TLSv1.1 - cryptoProtocolVersion=TLSv1.2

   Provide a JDBC connection string that includes the security parameters for the database.

   Note: You cannot configure a secure connection to a Sybase database.

The following table provides the database connection string syntax:

Database	Connection string syntax
IBM DB2	`jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
Oracle	`jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=<service name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
Micrososft SQL Server	`jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
PostgreSQL	`jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`

Note: The installer doesn't validate the connection string. Verify that the connection string contains all the connection parameters and security parameters required by your database.

The **Port Configuration** section appears.

Configure the node details

If you chose to make configuration changes to the node, you can enter the node details.

1. Verify the domain and node name.
2. Enter the node host name for the CDI-PC domain.
3. Enter the port number. Default is 6041.

The **Port Configuration** section appears.

Configure port numbers

You can configure port numbers for the Service Manager, application services, and the Administrator tool.

1. Enter new port numbers at the prompt or press **Enter** to use the default port numbers.

The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

2. Press **Enter** to continue.

   When the migration completes, the **Post-migration Summary** page appears with the migration status, log file, and domain information. A migration log file is generated in the following location: `<CDI-PC installation directory>/Informatica`.

3. Press **Enter** to exit the installer.

Perform all post-requisite tasks before you can log in to the Administrator tool to view the migrated services. For more information, see the Chapter 12, “After you migrate the domain” on page 131.

Run the installer in graphical mode

When you migrate from Informatica versions 10.4.x or 10.5.x, you can change the node configuration to migrate the domain to a different machine or to a different domain configuration repository database.

1. Log in to the machine with a system user account.
2. Close all the other applications.
3. Go to the root of the directory for the installation files and run `install.bat` as administrator.

   To run the file as administrator, right-click the `install.bat` file and select **Run as administrator**.

   Note: If you do not run the installer as administrator, the Windows system administrator might encounter issues when accessing files in the CDI-PC installation directory.

   The CDI-PC page appears.

4. Select **Migrate to CDI-PC**.
5. Click **Start**.

   The **Welcome** page appears.
6. Read the copyright information and click **Next** to continue.

   The **Migration Prerequisites** page displays the installation requirements. Verify that all requirements are met before you continue the installation.
7. Click **Next**.

   The **Informatica Services Installation Directory** page appears.

Enter the Informatica service directory details

Specify the Informatica installation directory. If migrating from a 10.4.x or 10.5.x version, you can specify if you want to allow changes to the node configuration details when you migrate.

1. Enter the absolute path to the Informatica installation directory.
2. Select the necessary options if you want to make changes to the node configuration when you migrate.
   - To configure a new host machine, select the option to change the node host name, port numbers, or domain configuration repository.
   - To allow changes to the node configuration during migration, select the option to change the host machine configuration.
3. Click **Next**.

   The **Informatica Domain and Node Details** page appears.

Confirm the domain and node details

When you enter the Informatica installation directory, the installer detects and displays the domain details.

1. View the domain details that appear based on the directory that you enter.
2. Enter the domain user name and password to validate the domain details.

   The installer checks the domain for migration requirements and an assessment summary appears.
3. Verify the results of the assessment.

   Depending on the type of migration, the installer checks requirements based on the following factors:
   - Transport Layer Security (TLS)
   - Domain
   - Database and version
   - Operating system
   - Domain services

   For example, all of the checks are performed on the first gateway node that you migrate. On worker nodes and all other gateway nodes, only TLS, domain, and operating system checks are performed. If you choose to allow node and host configuration changes, only some checks are performed on all nodes.

   The results of the migration check are saved to the Summary_<date and time stamp>.log file in the following location: `...<installer directory>/`
4. To continue to migrate, click **Next**.

   The **Migration Directory** page appears.

Enter the migration directory

Specify the directory where you want to migrate the domain.

1. Enter the absolute path to the CDI-PC domain installation directory.

   The directory names in the path can't contain spaces or the following special characters:

   ` % * + ; \ / " ? , < > @ # ! %) (} {] [' | &

   Default is the user home directory for the user that runs the installation.

   Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.

2. Click **Next**.

   The **Domain Security - Encryption Key** page appears.

Configure secure communication

The Informatica installation creates a unique site key. When you migrate from an Informatica domain, you use the same site key. The installer detects and displays the absolute path to the encryption key file of the Informatica installation. You specify the directory path where you want to copy the encryption key for the CDI-PC domain.

1. Verify the path to the Informatica domain encryption key file.
2. Enter the full path to the directory to store the CDI-PC domain encryption key. You can choose the default location or enter a custom path.
3. Applicable if you migrate from a version that either doesn't use TLS or uses TLS with the Informatica default TLS certificates. Enter the following information:
   - The HTTPS port to connect to the Administrator tool. Default is 8443.
   - The absolute path to the custom keystore file.
   - The keystore password.
   - The full path to the directory that contains the custom keystore files to secure communication within the domain.
   - The truststore password.
   - The full path to the directory that contains the custom truststore files to secure communication within the domain.
   - The truststore password.

The **Domain Configuration Repository** page appears. You can configure the domain configuration repository details and port number details.

Configure the domain configuration repository

If you chose to make configuration changes to the repository, you can configure the domain configuration repository.

1. On the **Domain Configuration Repository** page, enter the database and user account information for the domain configuration repository.

The following table describes the properties that you specify for the database and user account.

Property	Description
Database type	Type of database for the domain configuration repository. Select from the following options: - IBM DB2 - Oracle - Microsoft SQL Server - PostgreSQL - Sybase Default is Oracle.
Database User ID	Name for the domain configuration database user account.
User Password	Password for the domain configuration database user account.

If you select IBM DB2, specify the tablespace for the repository tables:

Property	Description
Tablespace	Name of the tablespace in which to create the tables. Specify a tablespace that meets the pageSize requirement of 32768 bytes. In a single partition database, if this option is not selected, the installer creates the tables in the default tablespace. In a multi-partition database, select this option and specify the name of the non-partitioned tablespace that resides in the catalog partition of the database.

If you select **Microsoft SQL Server** or **PostgreSQL**, enter the schema name for the database.
Enter the name of the schema that will contain the domain configuration tables. If the parameter is blank, the installer creates the tables in the default schema.

2. Enter the database connection information.

   If you do not create a secure domain configuration repository, you can specify the connection properties for the JDBC URL or provide the JDBC connection string.

   - To enter the connection information using the JDBC URL, select **JDBC URL** and specify the database connection properties.

The following table describes the JDBC URL properties that you specify:

Property	Description
Database Address	Host name and port number for the database in the format host_name:port_number.
Database Service Name	Service or database name. - Oracle. Enter the service name. - IBM DB2. Enter the service name. - Microsoft SQL Server. Enter the database name. - PostgreSQL. Enter the database name. - Sybase. Enter the database name.
JDBC Parameters	Optional parameters to include in the database connection string. Use the parameters to optimize database operations for the database. Verify that the parameter string is valid. The installer does not validate the parameter string before it adds the string to the JDBC URL. If not selected, the installer creates the JDBC URL string without additional parameters.

- To connect using a custom JDBC connection string, select **Custom JDBC connection string** and type the connection string.

3. If you create a secure domain configuration repository, enter the parameters for the secure database.

   The following table describes the options available to create a secure domain configuration repository database:

Property	Description
Database Truststore File	Absolute path to the truststore file for the secure database.
Database Truststore Password	Password for the truststore file.
Custom JDBC Connection String	JDBC connection string to connect to the secure database, including the host name and port number and the security parameters for the database.

The following table describes the secure database parameters to configure:

Database parameter	Description
EncryptionMethod	Required. Indicates whether data is encrypted when transmitted over the network. Set to `SSL`.
ValidateServerCertificate	Optional. Indicates whether Informatica validates the certificate that the database server sends. If this parameter is set to True, Informatica validates the certificate that the database server sends. If you specify the HostNameInCertificate parameter, Informatica also validates the host name in the certificate. If this parameter is set to False, Informatica doesn't validate the certificate that the database server sends. Informatica ignores any truststore information that you specify

Database parameter	Description
HostNameInCertificate	Optional. Host name of the machine that hosts the secure database. If you specify a host name, Informatica validates the host name included in the connection string against the host name in the certificate.
cryptoProtocolVersion	Required. Specifies the cryptographic protocol to use to connect to a secure database. Based on the cryptographic protocol used by the database server, set to one of the following values: - cryptoProtocolVersion=TLSv1.1 - cryptoProtocolVersion=TLSv1.2

Provide a JDBC connection string that includes the security parameters for the database.

Note: You cannot configure a secure connection to a Sybase database.

The following table provides the database connection string syntax:

Database	Connection string syntax
IBM DB2	`jdbc:Informatica:db2://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
Oracle	`jdbc:Informatica:oracle://<host name>:<port number>;ServiceName=<service name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
Micrososft SQL Server	`jdbc:Informatica:sqlserver://<host name>:<port number>;SelectMethod=cursor;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`
PostgreSQL	`jdbc:Informatica:postgresql://<host name>:<port number>;DatabaseName=<database name>;EncryptionMethod=SSL;HostNameInCertificate=<database host name>;ValidateServerCertificate=<true or false>`

Note: The installer doesn't validate the connection string. Verify that the connection string contains all the connection parameters and security parameters required by your database.

The **Informatica Domain and Node Details** page appears.

Configure the node details

If you chose to make configuration changes to the node, you can enter the node details.

1. Verify the domain and node name.
2. Enter the node host name for the CDI-PC domain.
3. Enter the port number. Default is 6041.

The **Port Configuration** section appears.

Configure port numbers

You can configure port numbers for the Service Manager, application services, and the Administrator tool.

1. You can choose to enter new port numbers or use the default port numbers.

   The following table describes the ports that you can set:

Port	Description
Service Manager port	Port number used by the Service Manager on the node. The Service Manager listens for incoming connection requests on this port. Client applications use this port to communicate with the services in the domain. The Informatica command line programs use this port to communicate to the domain. This is also the port for the SQL data service JDBC/ODBC driver. Default is 6006.
Service Manager Shutdown port	Port number that controls server shutdown for the domain Service Manager. The Service Manager listens for shutdown commands on this port. Default is 6007.
Informatica Administrator port	Port number used by Informatica Administrator. Default is 6008.
Informatica Administrator HTTPS port	No default port. Enter the required port number when you create the service. Setting this port to 0 disables an HTTPS connection to the Administrator tool.
Informatica Administrator shutdown port	Port number that controls server shutdown for Informatica Administrator. Informatica Administrator listens for shutdown commands on this port. Default is 6009.
Minimum port number	Lowest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6014.
Maximum port number	Highest port number in the range of dynamic port numbers that can be assigned to the application service processes that run on this node. Default is 6114.

2. Click **Next** to continue.

   When the migration completes, the **Post-migration Summary** page appears with the migration status, log file, and domain information. A migration log file is generated in the following location: `<CDI-PC installation directory>/Informatica`.

3. Click **Done** to exit the installer.

Perform all post-requisite tasks before you can log in to the Administrator tool to view the migrated services. For more information, see the Chapter 12, “After you migrate the domain” on page 131.

Complete the node configuration changes

If you changed the node configuration, perform additional tasks before you upgrade the application services.

Note: If you migrated only the domain configuration repository, you don't need to complete changes to the node configuration.

Perform the following tasks:

Clear the browser cache

Before you access the Administrator tool, clear the browser cache. If you don't clear the browser cache, the previous Administrator tool URL is not redirected to the latest URL and some menu options may not appear.

Configure locale environment variables

All UNIX operating systems except Linux have a unique value for each locale. Linux allows different values to represent the same locale. For example, “utf8,” “UTF-8,” “UTF8,” and “utf-8” represent the same locale on a Linux machine. Informatica requires that you use a specific value for each locale on a Linux machine. Make sure that you set the LANG environment variable appropriately for all Linux machines.

For Oracle database clients, set NLS_LANG to the locale that you want the database client and server to use with the login. A locale setting consists of the language, territory, and character set. The value of NLS_LANG depends on the configuration.

For example, if the value is american_america.UTF8, set the variable in a C shell with the following command:

```
setenv NLS_LANG american_america.UTF8
```

To read multibyte characters from the database, set the variable with the following command:

```
setenv NLS_LANG=american_america.AL32UTF8
```

Set the correct variable on the CDI-PC Integration Service machine so that the CDI-PC Integration Service can read the Oracle data correctly.

Configure library path environment variables

Configure the LD_LIBRARY_PATH environment variable.

The following table describes the values that you set for the LD_LIBRARY_PATH for the different databases:

Database	Value
Oracle	<Database path>/lib
PostgreSQL	$PGHOME/lib:$ {LD_LIBRARY_PATH}

Configure Kerberos environment variables

If you configure the CDI-PC domain to run on a network with Kerberos authentication, you must set the Kerberos configuration and credential cache environment variables.

The following table describes the values that you set for the Kerberos environment variables:

Database	Value
KRB5_CONFIG	Use the `KRB5_CONFIG` environment variable to store the path and file name of the Kerberos configuration file. The name of the Kerberos configuration file is `krb5.conf`. You must set the `KRB5_CONFIG` environment variable on each node in the CDI-PC domain.
KRB5CCNAME	Set the `KRB5CCNAME` environment variable with the path and file name of the Kerberos user credential cache. Kerberos single sign-on requires Kerberos credential cache for user accounts. When you cache the user credential, you must use the forwardable option. For example, if you use `kinit` to get and cache the user credential, you must use the `-f` option to request forwardable tickets.

Verify the range of dynamic port numbers

When you migrate a node, the installer assigns a default range of port numbers that can be dynamically assigned to application service processes that run on the node.

The default range of dynamic port numbers is 6013 to 6113. Verify that the default range of port numbers are available on the machine that runs the new version of Informatica. If the range of port numbers are not available, use the Administrator tool to update the range. Configure the minimum and maximum dynamic port numbers for service processes in the **Advanced Properties** section of the node **Properties** view.

Verify the node backup directory

Verify that the backup directory for the node is accessible by the machine that runs the new version of CDI-PC. In the Administrator tool, view the **Backup Directory** property in the **Advanced Properties** section of the node **Properties** view.

Configure PowerExchange adapters

If your Informatica installation included PowerExchange adapters, configure the PowerExchange adapters on the machine that runs CDI-PC. If the PowerExchange adapter has an installer, re-install it.

CHAPTER 11

Migrate the domain in silent mode

To migrate without user interaction, migrate in silent mode. Use a properties file to specify the migration options. The installer reads the file to determine the options.

Copy the installation files to the machine that hosts the Informatica instance you plan to migrate.

To migrate in silent mode, complete the following tasks:

1. Create the migration properties file and specify the migration options.
2. Run the installer with the migration properties file.

Create the properties file

Informatica provides silent properties files in the installer download directory. Use the appropriate properties file to specify migration options to migrate an Informatica domain to a CDI-PC domain without user interaction.

The file contains default values for many configuration properties. You can customize the file to specify your options.

1. Go to the root of the directory that contains the installation files.
2. Back up the following files:
   - Silentinput.properties
   - SilentInputMigrate.properties or SilentInputMigrate_NewConfig.properties.

     Note: If you are migrating a 10.4.x domain and want to make node or host configuration changes, use the SilentInputMigrate_NewConfig.properties file.
3. Use a text editor to open the file and update the property values.

   The properties file contains property descriptions and default values where applicable.
4. You can run the installer in the following ways:
   - Save the properties file with the name SilentInput.properties and run the silent installer.
   - Save the properties file with the same name.

   If you don't rename the file, include the complete path to the file when you run the silent installer.

Run the installer in silent mode

After you create the properties file, open a command prompt to start the silent migration.

1. Open a Linux shell command prompt.
2. Go to the root of the domain installer directory.
3. Verify that the directory contains the file that you saved with the migration options.
4. Run the silentinstall.sh executable.
   If you retained the updated file name as SilentinputMigrate.properties, specify the path and file name when you run the command. For example: `sh silentinstall.sh <installer directory>/SilentInputMigrate.properties`

The migration runs in the background. The process can take a while. The process is complete when the Informatica_<Version>_Services_InstallLog<timestamp>.log is created in the `<CDI-PC installation directory>/Informatica` directory.

The migration fails if you incorrectly configure the properties file or if the migration directory is not accessible. If the migration fails, view the silentErrorLog.log file in the `installer/logs` directory and correct the errors. Then run the silent installer again.

The installer creates the migration log file in the user `<CDI-PC installation directory>/Informatica` directory and the error log file in the `installer/logs` directory.

CHAPTER 12

After you migrate the domain

After you migrate the domain, perform the post-requisite tasks such as registering the domain, updating environment variables, and configuring service properties.

After the migration completes, the assigned permissions in the `pmimpprocess` executable changes. Configure the `pmimpprocess` executable to change the ownership and access permissions required for each user.

Register the domain

Register the domain in Informatica Intelligent Cloud Services to establish communication between the domain and the cloud.

Start the CDI-PC domain before you register it.
If the domain uses Kerberos authentication, the TLS certificate of the Administrator tool must be imported into the browser before you can register or perform any tasks that require domain authentication. The operating system user and the domain administrator user must be the same, because the operating system user details are used to authenticate with the domain. The browser and the domain must be in the same Active Directory.

1. Log in to Informatica Intelligent Cloud Services and select Cloud Data Integration for PowerCenter (CDI-PC).
2. On the **Home** page, click the **Add New Domain** button on the **Register a Domain** section.

   You can also open the **Explore** page from the navigation panel and click the **Add New Domain** button.
3. Enter the general properties.

   The following table lists the properties that you enter:

Property	Description
Domain Name	The name of the CDI-PC domain that you want to register.
Domain Display Name	A display name for the CDI-PC domain. By default, the display name is the same as the domain name. You can update the name if needed. The name can be different from the domain name, but the name must be unique in the organization.
Gateway Host	Host name of the gateway node machine.

Property	Description
Gateway Node Port	HTTPS port used by the gateway node.
Description	Optional. A description of the domain.

4. In the **Secure Agent Details** section, enter the name of the Secure Agent group.

   Secure Agents in the group require access to the domain.
5. In the **Domain Security Details** section, choose the authentication type.

   Choose Kerberos if the domain that you are registering uses Kerberos authentication.
6. In you choose non-Kerberos, enter the name of the security domain and the domain Administrator user name. If you choose Kerberos, enter the security domain. The service uses the operating system logged-in user details of the system from where you register the domain.
7. Click **Validate** to validate the details.

   Note: If the validation fails with a Read timed out error, retry validation.
8. When validation succeeds, click **Register** to register the domain.

If there is a break in connectivity, the domain might remain in Registering state indefinitely. Wait for at least 15 minutes and then click the **Refresh** button to refresh the information. If the domain status appears as offline, reconcile the domain status.

For information about reconciling a domain, see *Reconcile the status of a domain* in the Getting Started Guide.

Update the backup directory location

If you set the backup directory to INFA_HOME or if the directory that you used is not accessible to the CDI-PC domain, update the backup location to the directory that you want to use with CDI-PC.

1. Verify that the backup directory for the node is accessible by the machine that runs the CDI-PC domain.
2. In the Administrator tool, update the backup directory.
   You can find the backup directory in the **Advanced Properties** of the Properties view.
3. Update the backup directory for each node in the domain.

Update the environment variables

If you set custom paths for environment variables in the Informatica domain or if you want to change the paths, verify and update the paths of environment variables.

The following table describes the environment variables:

Environment Variable	Description
INFA_TRUSTSTORE	The directory that contains the truststore files for the SSL certificates. Verify that it contains truststore files named infa_truststore.jks and infa_truststore.pem. Set INFA_TRUSTSTORE if you use the default SSL certificate provided by Informatica or a certificate that you provide.
INFA_TRUSTSTORE_PASSWORD	The encrypted password for the infa_truststore.jks that contains the SSL certificate. Use the command line program pmpasswd to encrypt the password.

Configure JVM parameters

Use script files to set environment variables for infaservice and infasetup commands. If you added custom values in your Informatica domain, copy the values to the corresponding script file after you migrate.

You can find the script files, infasestupconfig.sh and infaserviceconfig.sh, in the following location:

```
<CDI-PC installation directory>/Informatica/platform/usr/bin/
```

If you use environment variables such as INFA_JAVA_OPTS or INFA_JAVA_CMD_OPTS to set customized values for JVM parameters that infaservice and infasetup commands use, set the variables and values in the configuration file for each command.

For example, to set the maximum heap size to 4 GB for each of the commands, configure each file as follows:

- infaserviceconfig.sh. `INFA_JAVA_OPTS="-Xmx4096m -XX:MaxMetaspaceSize=256m ${INFA_JAVA_OPTS}"`
- infasetupconfig.sh. `INFA_JAVA_CMD_OPTS="-Xmx4096m -XX:MaxMetaspaceSize=128m ${INFA_JAVA_CMD_OPTS}"`

Note: Any values that you edit in the infasetup.sh and infaservice.sh files might be overwritten when you apply updates.

Enable the CDI-PC domain application services

Enable the application services from the Administrator tool.

1. Log in to the Administrator tool.
2. On the **Manage** tab, click the **Services and Nodes** view.
3. In the **Domain Navigator**, select the CDI-PC Repository Service.
4. If the service is in disabled state, on the **Manage** tab **Actions** menu, click **Enable the Service**.
5. In the **Domain Navigator**, select the CDI-PC Integration Service.
6. If the service is in disabled state, on the **Manage** tab **Actions** menu, click **Enable the Service**. If the service is in unavailable state, click **Recycle the Service**.
7. If you have other application services, on the **Domain Navigator**, select the service.
8. If the service is in disabled state, on the **Manage** tab **Actions** menu, click **Enable the Service**.

Upgrade the CDI-PC Repository Service content

If you migrated from an Informatica 10.4.x version, upgrade the CDI-PC Repository Service content.

1. In the Administrator tool, click **Manage** > **Services and Nodes**.
2. In the Domain Navigator, select the CDI-PC Repository Service for the repository you want to upgrade.
3. On the **Manage** tab, click **Actions** > **Repository Contents** > **Upgrade**.
4. Enter the repository administrator user name and password.
5. Click **OK**.

   The activity log displays the results of the upgrade operation.
6. Change the operating mode of the service to normal.

Update the configuration files

When you migrate the domain, the installer overwrites configuration files, such as odbc.ini, odbcinst.ini, sapnwrfc.ini, or infaservice.sh. If any of the configuration files contain customization, updated, or new properties, you can manually merge the changes from the PowerCenter domain location into the latest installed file. For instance, if infaservice.sh contains some variables or java options, you need to manually merge the changes to the latest install file paths.

Manually merge the latest configuration changes into the following install file paths after you update:

`$INFA_HOME/ODBC7.1/odbc.ini`

`$INFA_HOME/ODBC7.1/odbcinst.ini`

`$INFA_HOME/server/bin/sapnwrfc.ini`

`$INFA_HOME/tomcat/bin/infaservice.sh`

Here, `$INFA_HOME` denotes `<install_dir>/Informatica/platform/home` and `$INFA_HOME/ODBC7.1` is a softlink for `<install_dir>/Informatica/platform/usr/bin/ODBC7.1`.

The original files are available in the existing PowerCenter domain location.

Update $PMRootDir for the CDI-PC Integration Service

The migration moves the PowerCenter services and creates the CDI-PC Repository Service and the CDI-PC Integration Service To define the root directory for service process variables, update the path in CDI-PC $PMRootDir.

1. Log in to the Administrator tool.
2. Click the **Services and Nodes** tab and select the CDI-PC Integration Service.
3. Click **Processes** and expand the **General Properties** section.
4. Click **Edit** and update the path value in the $PMRootDir field.
5. Click **Save**.

6. Recycle the service.

CHAPTER 13

Install the CDI-PC Client

Install the CDI-PC Client to connect to the domain and configure and run tasks in a CDI-PC domain.

You can install the client in graphical or silent mode.

Before you install the client

Before you install the CDI-PC Client, verify system requirements and set environment variables.

Verify system requirements

Before you install the client, verify the installation requirements.

The following table lists the minimum system requirements to install the CDI-PC Client:

Operating system	Processor	Memory	Disk Space
Windows	1 CPU	1 GB	6 GB

Set the environment variables

When you enable secure communication within the domain, you also secure connections between the domain and CDI-PC Client applications. You need to specify the location and password for the truststore files in environment variables on each client host.

Set the following environment variables on each client host:

INFA_TRUSTSTORE

The directory that contains the truststore files for the TLS certificates. Ensure that the directory contains truststore files named infa_truststore.jks and infa_truststore.pem.

INFA_TRUSTSTORE_PASSWORD

The encrypted password for the infa_truststore.jks file. Use the command line program pmpasswd to encrypt the password.

Note: INFA_TRUSTSTORE_PASSWORD is optional if you use any PowerCenter thick client, or commands such as pmcmd or pmrep. Enter a password only for the infacmd commands.

Copy the infa_truststore.jks and infa_truststore.pem truststore files to each client host and specify the location of the files and the truststore password on each machine.

Install the CDI-PC Client in graphical mode

When you install the CDI-PC Client, you can verify the prerequisites and inter the path for the installation directory.

Verify that you have performed all prerequisite tasks before you install the CDI-PC Client.

1. Close all the other applications.
2. Go to the root of the directory for the installation files and run install.bat as administrator.

   To run the file as administrator, right-click the install.bat file and select **Run as administrator**.

   Note: If you do not run the installer as administrator, the Windows system administrator might encounter issues when accessing files in the installation directory.

   If you encounter problems when you run the install.bat file from the root directory, run the following file: `<installer files directory>\client\install.exe`
3. Select **Install CDI-PC Client** and click **Next**.

   The **Installation Pre-requisites** page displays the system requirements.
4. Verify that all installation requirements are met before you continue the installation.
5. On the **Installation Directory** page, enter the absolute path for the installation directory.

   The maximum length of the path must be less than 260 characters. The directory names in the path can't contain spaces or the following special characters: @|* $ # ! % ( ) { } [ ] , ; ' & < > \ /

   Note: Informatica recommends using alphanumeric characters in the installation directory path. If you use a special character such as á or €, unexpected results might occur at run time.
6. Click **Next**.
7. On the **Pre-Installation Summary** page, review the installation information, and click **Install**.

   The installer copies the files to the installation directory.

   The **Post-installation Summary** page indicates whether the installation completed successfully.
8. Click **Done** to close the installer.

You can view the installation log files to get more information about the tasks performed by the installer.

Install the CDI-PC Client in silent mode

To install the CDI-PC Client without user interaction, install in silent mode. Specify the installation options in the properties file. The installer reads the file to determine the installation options. You can use silent mode installation to install the clients on multiple machines on the network or to standardize installation across machines.

1. Configure the installation properties file.
   a. Find the SilentInput.properties file in the root of the directory that contains the installation files.
   b. Back up the SilentInput.properties file.
   c. Use a text editor to open and modify the values of the properties in the file.

The following table describes the installation properties that you can modify:

Property Name	Description
INSTALL_TYPE	Indicates whether to install or upgrade the clients. Use the default value of 0 to install the client.
USER_INSTALL_DIR	CDI-PC Client installation directory.

d. Save the properties file in the same folder.

2. Run the installer with the installation properties file.
   a. Open a command prompt as an administrator.
   b. Go to the root of the directory that contains the installation files.
   c. To run the silent installation, run silentInstall.bat.

      When the installation is complete, you can find the Informatica_<Version>_Client_InstallLog<timestamp>.log file in the installation directory.

If the installation fails, correct errors shown in the log file and run the installer again.

Post-installation step for PowerExchange

After installing the CDI-PC client, if you use PowerExchange but do not want to use the default dbmover.cfg location of usr/config/pwx, you must specify the dbmover.cfg location in one of the following ways before starting the CDI-PC node or running the script that starts CDI-PC:

- Set the PWX_CONFIG parameter to point to the dbmover.cfg location in the usr/config/pwx/overrides.cfg file.
- Set the PWX_CONFIG environment variable to point to the PowerExchange dbmover.cfg configuration file location on the machine where you installed the client.

CDI-PC searches for the dbmover.cfg file in the following order:

1. The PWX_CONFIG parameter in the usr\config\pwx\overrides.cfg file
2. The PWX_CONFIG environment variable
3. The usr\config\pwx\dbmover.cfg file

CHAPTER 14

Uninstall Cloud Data Integration for PowerCenter (CDI-PC)

To uninstall Cloud Data Integration for PowerCenter (CDI-PC), uninstall the CDI-PC domain, the CDI-PC Client, and the Secure Agent.

Read the following rules and guidelines before you uninstall theCloud Data Integration for PowerCenter (CDI-PC) components:

- Before you uninstall the domain, deregister and delete the domain on the CDI-PC Home page.
- Uninstalling the CDI-PC domain does not affect the repositories. The uninstaller removes the CDI-PC domain files. It does not remove repositories from the database. If you need to move the repositories, you can back them up before you remove the CDI-PC domain files, and restore them to another database.
- Uninstalling the CDI-PC domain does not remove the metadata tables from the domain configuration database. If you install theCDI-PC domain again using the same domain configuration database and user account, you must manually remove the tables or choose to overwrite the tables. You can use the infasetup BackupDomain command to back up the domain configuration database before you overwrite the metadata tables. To remove the metadata tables manually, use the infasetup DeleteDomain command before you run the uninstaller.
- Uninstalling the CDI-PC domain removes all installation files and subdirectories from the installation directory. Before you uninstall the CDI-PC domain, stop all CDI-PC domain services and processes and verify that all of the files in the installation directory are closed. At the end of the uninstallation process, the uninstaller displays the names of the files and directories that could not be removed.
- The CDI-PC domain installation creates the following folder for the files and libraries required by third party adapters built using the Informatica Development Platform APIs:
  `<CDI-PC installation directory>/Informatica/platform/home/services/shared/extensions`

  Uninstalling the CDI-PC domain deletes this folder and any subfolders created under it. If you stored adapter files in the `/extensions` folder, back up the folder before you start uninstallation.
- Back up the ODBC folder before you uninstall. Restore the folder after the uninstallation completes.

Uninstalling the CDI-PC domain in console mode

You can uninstall the CDI-PC domain in console mode.

Before you run the uninstaller, complete the following tasks:

- Stop all CDI-PC domain services and processes and verify that all files in the installation directory are closed.
- Add `JAVA_HOME` to the PATH environment variable.

1. Go to the following directory:

   ```
   <CDI-PC installation directory>/Informatica/Uninstaller_Server
   ```

2. Type the following command to run the uninstaller:

   ```
   ./uninstaller.sh
   ```

Uninstalling the CDI-PC domain in graphical mode

You can uninstall the CDI-PC domain in graphical mode.

Before you uninstall the CDI-PC domain, complete the following tasks:

- De-register the CDI-PC domain from Informatica Intelligent Cloud Services.
- Shut down the CDI-PC domain if you are uninstalling all the nodes in the domain. Otherwise shut down only the specific node that you want to uninstall.

1. Click **Start** > **Program Files** > **Informatica CDI-PC** > **Uninstaller**.

   The **Uninstallation** page appears.

2. Click **Uninstall** to begin the uninstallation.

   After the installer deletes all of the CDI-PC files from the directory, the **Post-Uninstallation Summary** page appears.

3. Click **Done** to close the uninstaller.

After you uninstall the CDI-PC domain, delete any remaining folders and files from the CDI-PC installation directory.

Log out of the machine and log back in. Then clear all the CDI-PC specific CLASSPATH and PATH environment variables.

Uninstalling the CDI-PC domain in silent mode

If you installed the CDI-PC domain in silent mode, uninstall the CDI-PC domain in silent mode.

1. Go to the following directory:

   ```
   <CDI-PC installation directory>/Informatica/Uninstaller_Server
   ```

2. Type the following command to run the silent uninstaller:

   ```
   ./uninstaller.sh
   ```

If you installed the CDI-PC in silent mode, the uninstaller launches in silent mode. The silent uninstaller runs in the background. The process can take a while. The silent uninstallation fails if the installation directory is not accessible.

After you uninstall the CDI-PC domain, delete any remaining folders and files from the CDI-PC installation directory.

CHAPTER 15

Uninstalling the CDI-PC Client

You can uninstall the CDI-PC Client in graphical mode and silent mode on Windows.

When you uninstall CDI-PC Client, the installer does not remove the environment variables, INFA_TRUSTSTORE, that it creates during installation. When you install a later version of CDI-PC Client, you must edit the environment variable to point to the new value of the SSL certificate.

Uninstalling the CDI-PC Client in graphical mode

You can uninstall the CDI-PC Client in graphical mode.

1. Browse to the `<client installation directory>\Uninstaller_Client\uninstaller.bat` or run the uninstaller application.

   The **Uninstallation** page appears.
2. Click **Next**.

   The **Application Client Uninstall** page appears.
3. Click **Uninstall** to start the uninstallation.
4. Click **Done** to close the uninstaller.

   After the uninstallation is complete, the **Post-Uninstallation Summary** page appears, displaying the results of the uninstallation.

After you uninstall the CDI-PC Client, delete any remaining folders and log files from the installation directory.

Log out of the machine and log back in. Then clear the Informatica-specific CLASSPATH and PATH environment variables.

Uninstalling the CDI-PC Client in silent mode

You can uninstall the client in silent mode. You don't need to specify uninstallation options in the properties file.

1. Open a command prompt.
2. Go to the root of the directory that contains the installation files.
3. Verify that the directory contains the SilentInput.properties file.
4. Go to `<CDI-PC installation directory>/Uninstaller_Client`.

5. To run the silent uninstallation, double-click the `uninstaller.bat` or `uninstaller.exe` file.

   The silent uninstaller runs in the background. The process can take a while. The silent uninstallation fails if the installation directory is not accessible.

After you uninstall the clients, delete any remaining folders and files from the installation directory. For example, client log files. Log out of the machine and log back in. Then clear the Informatica entries in the CLASSPATH and PATH environment variables.

Uninstalling the CDI-PC Client from the Control Panel

You can uninstall the client from the **Programs** section on the **Control Panel**.

1. Click **Start** and open the **Control Panel**.
2. Click **Programs** > **Programs and Features** to open the **Uninstall or change a program** page.
3. Select **Informatica Cloud Data Integration for PowerCenter Client** and click **Uninstall/Change**.
4. On the uninstaller window that opens, click **Uninstall** to start.
5. When the uninstallation is complete, delete any remaining folders, such as log files.
6. Log out of the machine and log in again and clear the Informatica CLASSPATH and PATH environment variables.

Uninstalling the CDI-PC Client from the shortcut

You can uninstall the client from the client uninstaller shortcut.

1. Click **Start** and scroll to **Informatica Cloud Data Integration for PowerCenter**.
2. Expand the Informatica Cloud Data Integration for PowerCenter folder to view the **Uninstaller_Client** shortcut.
3. Click **Uninstaller_Client** to open the uninstaller.
4. On the uninstaller window that opens, click **Uninstall** to start.
5. When the uninstall is complete, delete any remaining folders, such as log files.
6. Log out of the machine and log in again and clear the Informatica CLASSPATH and PATH environment variables.

CHAPTER 16

Uninstalling the Secure Agent

You can uninstall the Secure Agent on Linux and Windows.

Uninstall the Secure Agent if you no longer want to run the Secure Agent on the machine or if you want to reinstall the Secure Agent.

Uninstalling the Secure Agent on Linux

You can uninstall the Secure Agent. You might uninstall the Secure Agent if you no longer want to run the Secure Agent on the machine or if you want to reinstall the Secure Agent.

Before you uninstall the Secure Agent, verify that no connection or task is configured to use it.

1. From the command line, navigate to the following directory:

   ```
   <Secure Agent installation directory>/apps/agentcore
   ```

2. Stop the Secure Agent Linux process by entering the following command:

   ```
   ./infaagent shutdown
   ```

3. To uninstall the Secure Agent, run rm -rf on the directory where you installed the Secure Agent to remove Secure Agent files.

Uninstalling the Secure Agent on Windows

You can uninstall the Secure Agent. You might uninstall the Secure Agent if you no longer want to run the Secure Agent on the machine or if you want to reinstall the Secure Agent.

Before you uninstall the Secure Agent, verify that no connection or task is configured to use it.

1. Click **Start** > **All Programs** > **Informatica Cloud Secure Agent** > **Uninstall Informatica Cloud Secure Agent**.

   The Secure Agent uninstaller launches.

2. Click **Uninstall**.
3. When the uninstall completes, click **Done**.
4. Delete any remaining files in the installation directory.

   After you uninstall the Secure Agent, delete all files and directories associated with the Secure Agent installation.

Note: Uninstalling the Secure Agent does not delete log files from the Secure Agent directory. If you want to reinstall a Secure Agent on the machine, you must delete all files and directories associated with the Secure Agent installation or reinstallation will fail. If you want to save the log files, copy them to a different directory, and then delete the Secure Agent installation directory.

APPENDIX A

CDI-PC components

CDI-PC includes an on-premises domain that works similar to an Informatica domain in PowerCenter. Although CDI-PC and PowerCenter consist of similar components, they do have some differences. Some PowerCenter components are available in CDI-PC, while some components are new in CDI-PC and not available in PowerCenter.

Components

The following table describes the components in CDI-PC with the corresponding components in PowerCenter:

CDI-PC	PowerCenter	Description
CDI-PC domain	Informatica domain	On-premises A node that represent the machine on which the services run. If you install on a single machine, you create the domain and gateway node on the machine.
CDI-PC Integration Service	PowerCenter Integration Service	On-premises service An application service that runs sessions and workflows. Use the Administrator tool to manage the service.
CDI-PC Repository Service	PowerCenter Repository Service	On-premises service An application service that manages the repository. It performs all metadata transactions between the repository database and the repository clients.
Web Services Hub	Web Services Hub	On-premises An application service that exposes product functionality to external clients through web services. It processes requests from web service clients.
Domain configuration repository	Domain configuration repository	On-premises Stores configuration and user information from a domain.
CDI-PC repository	PowerCenter repository	On-premises Relational database that stores repository metadata. The Repository Service manages the repository and performs all metadata transactions between the repository database and repository clients.

CDI-PC	PowerCenter	Description
Informatica Administrator (the Administrator tool)	Informatica Administrator (the Administrator tool)	On-premises A web application to manage the domain and application services.
CDI-PC Client	PowerCenter Client	On-premises A thick client application to create and run workflows with sessions.
Secure Agent	None	On-premises A lightweight program that you install on an on-premises physical or virtual machine. Provides connectivity between the on-premises domain and Informatica Intelligent Cloud Services.
CDI-PC service	None	The Cloud Data Integration for PowerCenter (CDI-PC) service in Informatica Intelligent Cloud Services. Allows you to the monitor the domain status and manage updates to the domain.
Domain Management Service	None	A microservice that runs in Informatica Intelligent Cloud Services. Runs jobs related to registering domains, managing domains, and all jobs that you run on the CDI-PC Home page.
Domain Management App	None	A pluggable application that the Secure Agent uses. Connects the on-premises domains with Informatica cloud and handles backend tasks required for domain updates in CDI-PC.

The following table describes some of the differences between CDI-PC and PowerCenter:

Function	CDI-PC	PowerCenter
Application services	You can use the following application services in CDI-PC: - CDI-PC Integration Service - CDI-PC Repository Service - Web Services Hub Service - PowerCenter SAP BW Service - PowerCenter Listener Service - PowerCenter Logger Service	You can use multiple additional services in PowerCenter. For information about services that you can use in PowerCenter, see the PowerCenter documentation.
Monitor	CDI-PC includes a cloud service component that allows you to monitor your domains from Informatica Intelligent Cloud Services.	You can monitor an Informatica domain in PowerCenter by logging into the client applications for monitoring.

Function	CDI-PC	PowerCenter
Updates	CDI-PC runs automated update jobs from Informatica Intelligent Cloud Services to keep all domains on the latest version. You can choose an earlier date to apply the update or manually initiate an update. The service handles all tasks related to applying the update, including shutting down the domain and services before and starting the domain and services after applying the update.	You manually shut down the domain, run the installer to upgrade, and then start the domain and services.
Domain directory structure	The directory structure of CDI-PC includes separate directories for binaries, user configurations, logs, and common libraries. This structure makes it possible to apply updates in stages and to use common libraries with external services.	The directory structure of PowerCenter includes a single Informatica installation directory that contains Informatica binaries, user configuration files, log files, and common libraries. The structure makes upgrades difficult. You can't reuse the common libraries with external services.

The following directory structure represents the CDI-PC installation directory tree:

```
|_<USER_CONFIGURED_INSTALL_DIRECTORY>
|_Informatica/platform
|-- common
|   |-- lib
|                            |-- java
|                            |-- tomcat
|   |-- version.json
|-- home
|   |-- connectors
|                            |-- sdk
|   |-- DataTransformation
|                            |-- api
|                            |-- autoInclude
|                            |-- bin
|                            |-- CMConfig.xml
|                            |-- CMConfig.xsd
|                            |-- cminfo.xml
|                            |-- CommonDB
|                            |-- doc
|                            |-- externLibs
|                            |-- license.txt
|                            |-- readme_Birt.txt
|                            |-- samples
|                            |-- ServiceDB
|                            |-- setEnv.csh
|                            |-- setEnv.sh
|                            |-- setupTests
|   |-- domains.infa
|   |-- externaljdbcjars -> ../Informatica/platform/usr/bin/externaljdbcjars
|   |-- isp
|                            |-- bin
|                            |-- common
|                            |-- config -> ../RelUID/Informatica/platform/usr/config/isp/
config
|                            |-- webapps
|   |-- java -> ../Informatica/platform/common/lib/java/202404
|   |-- logs -> ../Informatica/platform/logs
|   |-- ODBC7.1 -> ../Informatica/platform/usr/bin/ODBC7.1
|   |-- plugins
|                            |-- acplugins
|                            |-- conf
|                            |-- dynamic
|                            |-- infa
```

```
|                             |-- osgi
|   |-- server
|                             |-- bin
|                             |-- cci
|                             |-- connectors
|                             |-- infa_shared -> ../RelUID/Informatica/platform/usr/data/
infa_shared
|                             |-- samples
|                             |-- tomcat
|                             |-- Tutorials
|   |-- services
|                             |-- AdministratorConsole
|                             |-- EmailService
|                             |-- ISPPlugins
|                             |-- PowerExchange
|                             |-- shared
|                             |-- WebServiceHub
|                             |-- work_dir
|   |-- thirdpartynotice
|   |-- tomcat
|                             |-- bin
|                             |-- conf -> ../RelUID/Informatica/platform/usr/config/
tomcat/conf
|                             |-- logs
|                             |-- temp
|                             |-- work
|   |-- tomcat9 -> ../Informatica/platform/common/lib/tomcat/202404
|   |-- tools
|    -- version.txt
|-- logs
|   |-- infasetup_cli.log
|   |-- infasetup_jsf.log
|   |-- upgrade_logs
|   |-- system_logs
|-- pwx
|    -- bin
|-- sys
|   |-- apps
|    -- data
|-- usr
    |-- bin
    |-- config
        |-- pwx
                        |-- dbmover.cfg
                        |-- overrides.cfg
    |-- custom
    |-- data

|-- Uninstaller_Server
        |-- Bundles
        |-- InstallScript.iap_xml
        |-- installvariables.properties
        |-- uninstaller
        |-- uninstaller.jar
        |-- uninstaller.lax
        |-- uninstaller.sh
```

The following directory structure represents the PowerCenter installation directory tree:

```
|_<INFA_HOME>
|_isp
|_config
|_tomcat
|_conf
|_tomcat9
|_java
|_logs
|_externaljdbcjars
|_ODBC7.1
|_plugins
|_pwxmfplugins
```

```
|_sdk
|_server
|_services
|_tools
```

INDEX

C

CDI-PC clients
  uninstalling 142

D

domain configuration repository
  Sybase database requirements 19

L

Linux
  uninstalling the Secure Agent 144

R

requirements
  Secure Agent 44

S

Secure Agent Manager
  launching 43
Secure Agents
  installing on Linux 42
  installing on Windows 44
  registering on Linux 42
  registering on Windows 44
  requirements on Windows 44
  starting on Windows 43
  uninstalling on Linux 144
  uninstalling on Windows 144
Sybase database requirements
  domain configuration repository 19