Informatica®

Informatica® B2B Data Exchange
10.2.3

Installation and Configuration Guide

Informatica B2B Data Exchange Installation and Configuration Guide
10.2.3
November 2019

Publication Date: 2020-08-06

Table of Contents

Preface

Follow the instructions in the *B2B Data Exchange Installation and Configuration Guide* to install and configure Data Integration Hub. The guide also includes information about the pre-install tasks and post-install tasks that you need to perform to complete the installation.

Informatica Resources

Informatica provides you with a range of product resources through the Informatica Network and other online portals. Use the resources to get the most from your Informatica products and solutions and to learn from other Informatica users and subject matter experts.

Informatica Network

The Informatica Network is the gateway to many resources, including the Informatica Knowledge Base and Informatica Global Customer Support. To enter the Informatica Network, visit https://network.informatica.com.

As an Informatica Network member, you have the following options:

- Search the Knowledge Base for product resources.
- View product availability information.
- Create and review your support cases.
- Find your local Informatica User Group Network and collaborate with your peers.

Informatica Knowledge Base

Use the Informatica Knowledge Base to find product resources such as how-to articles, best practices, video tutorials, and answers to frequently asked questions.

To search the Knowledge Base, visit https://search.informatica.com. If you have questions, comments, or ideas about the Knowledge Base, contact the Informatica Knowledge Base team at KB_Feedback@informatica.com.

Informatica Documentation

Use the Informatica Documentation Portal to explore an extensive library of documentation for current and recent product releases. To explore the Documentation Portal, visit https://docs.informatica.com.

If you have questions, comments, or ideas about the product documentation, contact the Informatica Documentation team at infa_documentation@informatica.com.

Informatica Product Availability Matrices

Product Availability Matrices (PAMs) indicate the versions of the operating systems, databases, and types of data sources and targets that a product release supports. You can browse the Informatica PAMs at https://network.informatica.com/community/informatica-network/product-availability-matrices.

Informatica Velocity

Informatica Velocity is a collection of tips and best practices developed by Informatica Professional Services and based on real-world experiences from hundreds of data management projects. Informatica Velocity represents the collective knowledge of Informatica consultants who work with organizations around the world to plan, develop, deploy, and maintain successful data management solutions.

You can find Informatica Velocity resources at http://velocity.informatica.com. If you have questions, comments, or ideas about Informatica Velocity, contact Informatica Professional Services at ips@informatica.com.

Informatica Marketplace

The Informatica Marketplace is a forum where you can find solutions that extend and enhance your Informatica implementations. Leverage any of the hundreds of solutions from Informatica developers and partners on the Marketplace to improve your productivity and speed up time to implementation on your projects. You can find the Informatica Marketplace at https://marketplace.informatica.com.

Informatica Global Customer Support

You can contact a Global Support Center by telephone or through the Informatica Network.

To find your local Informatica Global Customer Support telephone number, visit the Informatica website at the following link:
https://www.informatica.com/services-and-training/customer-success-services/contact-us.html.

To find online support resources on the Informatica Network, visit https://network.informatica.com and select the eSupport option.

CHAPTER 1

Installation Overview

This chapter includes the following topics:

B2B Data Exchange Installation

B2B Data Exchange consists of the core application component and additional required and optional components. If you install B2B Data Exchange, PowerCenter® services, and the PowerCenter Client on the same machine, you can select all of the components in the installer. Otherwise, install each component on the required machine.

The B2B Data Exchange installation includes the following components:

B2B Data Exchange

Core application component. Includes the Operation Console, B2B Data Exchange server, and the B2B Data Exchange repository. The PowerCenter services must be running when you install B2B Data Exchange. You must set up the database user account before you install this component.

If you install B2B Data Exchange on an existing database, all data in the repository is preserved. All previous user accounts are still valid in the new installation, including the Operation Console administrator account. If the repository is from a previous version, the installer upgrades the repository.

B2B Data Exchange Partners Portal

On-premises Partners Portal component. The portal displays visual reports about data that B2B Data Exchange processes for partners. You can brand the portal with your organization logo.

You can install the Partners Portal either on the B2B Data Exchange node or on a different node in your organization.

B2B Data Exchange Dashboard and Reports

Business activity monitoring component. Includes the dashboard application and the operational data store repository. You must set up a different user account from the user account that you use for the B2B Data Exchange repository.

You must install the B2B Data Exchange component to install this component.

B2B Data Exchange PowerCenter server plug-in

PowerCenter repository plug-in that B2B Data Exchange uses to run B2B Data Exchange transformations in PowerCenter. The installation includes files to add to the classpath of the PowerCenter Integration

Service, and sample workflows. You must install this plug-in on the same machine as the PowerCenter services.

After you install this component, you must register the plug-in to the PowerCenter repository before you create and run B2B Data Exchange workflows.

B2B Data Exchange PowerCenter Client plug-in

PowerCenter Client plug-in that displays B2B Data Exchange transformation properties in PowerCenter mappings. You install this plug-in on all PowerCenter Client machines that you plan to use to build mappings and workflows for B2B Data Exchange transformations.

B2B Managed File Transfer

Managed File Transfer tool to use when you process files to and from partners with specific transfer protocols, such as FTP or AS2.

You must install the B2B Data Exchange component to install this component.

Additional Installation Components

B2B Data Exchange requires additional components to run. The components are installed as part of the B2B Data Exchange installation process.

The B2B Data Exchange includes the following additional applications and components:

B2B Data Exchange Server

Server environment that manages event processing in B2B Data Exchange.

JMS Broker Service

Manages JMS messages routing between B2B Data Exchange and PowerCenter.

Note: If you upgrade from earlier versions, backwards compatibility is not guaranteed.

Operation Console

Web interface to customize and monitor processing, manage users, and set preferences.

Apache Tomcat

Web server environment that runs the Operation Console client.

Java JDK

Java run-time environment in which the B2B Data Exchange server, B2B Data Exchange Operation Console, and B2B Data Exchange command line client tools run.

Samples

Sample workflows and readme files. The installer copies the samples to the following directory: `<DXInstallationDir>/samples`

For more information about the sample workflows, read the `readmefirst.txt` file in the folder of each sample.

CHAPTER 2

Before You Begin

This chapter includes the following topics:

User Accounts

Before you install, verify that you have the user names and passwords for the required database and domain accounts.

The following table describes the required user accounts:

User Account	Description

Database	Database user account that you use to log in to the database server and create tables and views for the B2B Data Exchange repository. If you install the Dashboard and Reports component, you also use a user account for the operational data store.
	You must install all the repositories on the same type of database server. You must create a separate user account for each repository.
	The user accounts must have privileges to perform the following actions:
	- Select data from tables and views.
	- Insert data into tables, delete data from tables, and update data in tables.
	- Create, change, and delete the following elements:
	  - Tables
	  - Views
	  - Synonyms
	  - Indexes
	  - Custom data types
	  - Triggers
	- Create, change, delete, and run stored procedures and functions.
	If you use a Microsoft SQL Server database, you must set up separate databases for each repository. It is recommended that you grant database owner privileges to the user accounts.

If you use B2B Data Exchange with Informatica domain authentication: Informatica domain administrator	Administrator account for the Informatica domain.
If you use B2B Data Exchange with Informatica domain authentication: Informatica security domain	User account for Informatica domain authentication. The user account must be created in the Informatica Administrator tool with the **manage roles/groups/users** privileges. The B2B Data Exchange administrator synchronizes the user account after the installation.

Port Numbers

The installer sets the default port numbers for the installation components. If another application uses the same port number as one of the installation components, a port conflict might prevent the component from running correctly or cause errors.

You can change the port numbers after installation. Before you start B2B Data Exchange, verify that the port numbers do not conflict with other applications and change the port numbers in B2B Data Exchange to prevent port conflicts.

The following table describes the default port numbers:

Port Number	Description
18000	UDP multicast port that B2B Data Exchange uses for internal communications.
18005	Operation Console shutdown port. Only required to be available on the machine where B2B Data Exchange is installed.
18050	Port that the Operation Console uses for internal communications.
18080	Operation Console HTTP port. Required only if you use an HTTP port for the Operation Console.
18095	RMI port for B2B Data Exchange server startup and shutdown.
18095 and 18096	RMI ports that the Operation Console and PowerCenter workflows use to communicate with the B2B Data Exchange server.
18100	Port that the B2B Data Exchange server uses for internal communications.
18443	Operation Console HTTPS port. Required only if you use an HTTPS port for the Operation Console.
18616	Port for the B2B Data Exchange JNDI provider. This port is also the JMS listener port for the B2B Data Exchange JMS Broker.

CHAPTER 3

Pre-Installation Tasks

This chapter includes the following topics:

Pre-Installation Tasks Overview

Before you install B2B Data Exchange, set up the machines to meet the installation requirements, verify that you have all the user account credentials, and prepare your environment for installing and running B2B Data Exchange.

Note: B2B Data Exchange and the PowerCenter Integration Service that B2B Data Exchange uses must be installed on the same type of operating system. Both must be installed either on a machine or machines that are running Windows operating systems, or on a machine or machines that are running non-Windows operating systems.

The following components must reside on machines with the same locale and the same time zone:

- B2B Data Exchange server
- B2B Data Exchange repositories
- B2B Data Exchange Operation Console clients
- PowerCenter Repository Service that B2B Data Exchange uses
- PowerCenter Integration Service that B2B Data Exchange uses

Verify the Minimum System Requirements

Verify that your system meets the minimum requirements.

The following table describes the minimum system requirements:

System	Requirement
Operating system	- Microsoft Windows - IBM AIX - Sun Solaris - Red Hat Linux - SUSE Linux
Processor	- Minimum: 2 CPU cores - Recommended: 8 CPU cores
RAM	8 GB
Disk space	- Minimum: 3 GB - Recommended: 8 GB
Browser	- Microsoft Internet Explorer - Google Chrome - Microsoft Edge

The following table describes the minimum system requirements to run the installer:

System	Requirement
RAM	512 MB
Disk space	1 GB

For more information about product requirements and supported platforms, see the Product Availability Matrix on Informatica Network:
https://network.informatica.com/community/informatica-network/product-availability-matrices

Verify the Database Requirements

Verify that your database meets the requirements for running B2B Data Exchange.

The following table describes the database requirements for B2B Data Exchange:

Database Component	Description
Database System	Type of database on which to install the repositories. You can use one of the following database systems: - Oracle - Microsoft SQL Server If you install the Dashboard and Reports component, you do not need to install the operational data store on the same machine on which you install B2B Data Exchange. **Note:** If you install the Dashboard and Reports component, your B2B Data Exchange and operational data store repositories are installed on Microsoft SQL Servers, and you use PowerCenter version 10, you must configure the repository connections in PowerCenter Workflow Manager. For details, see "Configuring Repository Connections on PowerCenter Version 10" on page 126.
Disk space	512 MB of disk space for the core application. You also need additional space based on the number of messages that you need to process and the type of processing required. The frequency of message archiving also affects the disk space requirement.
Database connections	One or more database connections must always be available. The number of required connections depends on the number of endpoints and the number of documents processed concurrently. Use the following formula to calculate the number of required database connections : (NumberOfEndpoints + Maximum number of concurrent processes + 3) X 3 + 2 If you do not have enough database connections available, B2B Data Exchange might fail or encounter database deadlocks.

Database Unicode Support

If you require Unicode support, create the B2B Data Exchange repository database with the following settings:

- Oracle databases: use the AL32UTF8 Unicode character set.
- Microsoft SQL Server: it is recommended that you use data types that support Unicode data: nchar, nvarachar, and ntext.

Microsoft SQL Server Collation

If you use Microsoft SQL Server, the collation for the B2B Data Exchange repository must not be case sensitive.

Install the Prerequisite Software

Install the prerequisite software on your machine.

- PowerCenter. Install PowerCenter before you install B2B Data Exchange. Make sure to install PowerCenter services on a machine that is accessible to B2B Data Exchange. After you install PowerCenter, verify that the PowerCenter Web Services Hub is running.
  If you do not install the PowerCenter services on the same machine that you install B2B Data Exchange, install the PowerCenter pmrep command line utility on the machine where you install B2B Data Exchange. Verify that B2B Data Exchange and PowerCenter can be accessed with the same drive and file path..
- **Data Transformation.** Install Data Transformation on the machine where you install B2B Data Exchange before you install the B2B Data Exchange server plug-in for PowerCenter.
- Java Development Kit (JDK). On IBM AIX operating systems, install the IBM JDK version 8.0.5.16 (8.0 Service Refresh 5 Fix Pack 16) and configure the INFA_JDK_HOME environment variable before you install B2B Data Exchange. Verify that the login shell can access the INFA_JDK_HOME environment variable. For more information about Java installation, see the Java website at the following address: https://www.ibm.com/developerworks/java/jdk/fixes/8/index.html
  The software available for download at the referenced links belongs to a third party or third parties, not Informatica LLC. 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 more information about product requirements and supported platforms, see the Product Availability Matrix on Informatica Network:
  https://network.informatica.com/community/informatica-network/product-availability-matrices
- Microsoft Visual C++ 2008 Redistributable Package (x86). Install this package if you use the B2B Data Exchange PowerCenter Client plug-in on a Windows Server 2008 64-bit operating system.
  The software available for download at the referenced links belongs to a third party or third parties, not Informatica LLC. 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.
- Java Cryptography Extension (JCE). Install this package if you are installing B2B Data Exchange with Managed File Transfer on an IBM AIX operating system.

Install and Configure the PowerCenter pmrep Command Line Utility

If you do not install the PowerCenter services on the same machine that you install B2B Data Exchange, you install and configure the PowerCenter pmrep command line utility on the machine where you install B2B Data Exchange.

To download the utility, contact Informatica Shipping. The utility version must match the PowerCenter version.

1. Extract the ZIP file on your local machine to a directory that is accessible by the B2B Data Exchange installer.

   By default, the installer searches for the utility in the following directory: `<LocalDrive>\Informatica \version`

2. Configure the utility settings based on your operating system.

   For information about the utility settings, see the *Informatica Repository Guide*.

To test the utility settings, run the utility from the command line and verify that no errors appear in the run results.

Note: If you upgrade the pmrep command line utility at a later time, clean up all CNX files from the `Tmp` folder on your home directory.

Configure Environment Variables

After you install PowerCenter or the PowerCenter pmrep command line utility on the machine where you install B2B Data Exchange, configure environment variables.

1. Set the INFA_HOME environment variable to point to the Informatica installation directory.
2. Set the INFA_DOMAINS_FILE environment variable to the path and the file name of the `domains.infa` file.
3. On Solaris and Linux, add `<INFA_HOME>/server/bin` to the LD_LIBRARY_PATH environment variable.
4. On AIX, add `<INFA_HOME>/server/bin` to the LIBPATH environment variable.
5. Verify that the pmrep utility code page matches the PowerCenter Repository Service code page. You specify the code page in the INFA_CODEPAGENAME environment variable of the utility.
6. To reduce the length of time to wait before the pmrep utility reports an error when connecting to PowerCenter, change the value of the INFA_CLIENT_RESILIENCE_TIMEOUT environment variable in the utility.

   The default timeout waiting time is 180 seconds.

Create a Data Source Name for Microsoft Azure SQL Database

If you install B2B Data Exchange repositories on a Microsoft Azure SQL database, create data source names on the operating system of the machine on which PowerCenter is installed.

Create data source names on the operating system as provided in the following sections:

- "Creating a Data Source Name on a Windows Operating System" on page 21
- "Creating a Data Source Name on a Unix Operating System" on page 22

Creating a Data Source Name on a Windows Operating System

This section describes how to create a data source name on the Windows operating system on which B2B Data Exchange is installed.

Note: Ensure that you configure a separate Data Source Name (DSN) entry for every database on which B2B Data Exchange is installed.

1. Open **ODBC Data Sources** from the Windows environment and select **64-bit ODBC Data Source for DataDirect 7.1 New SQL Server Wire Protocol**.

   The **ODBC DataSource Administrator** window is displayed.
2. Select **System DSN** and click **Add New**.

   The **Create New DataSource** window is displayed.
3. Select the following driver: **DataDirect 7.1 New SQL Server Wire Protocol**.

   The **ODBC SQL Server Wire Protocol Driver Setup** window is displayed.
4. Enter the following details in the **General** tab:
   - **DataSource Name**. Name of the data source.
   - **Host Name**. Host name of the machine where the database server is installed.
   - **Port Number**. Port number of the database. The default port number for Microsoft Azure SQL Database is 1433.
   - **Database**. Name of the database instance.
5. Select **Advanced** > **Extended Options** and add **WorkArounds2=2**.

   Note: Enabling the WorkArounds2=2 option, causes the driver to ignore the column size, decimal digits, or datetime values specified by the application and use the database defaults instead. Some applications incorrectly specify the column size or decimal digits when binding timestamp parameters.
6. Select **Security** and update the following information:
   - **User Name**. Name of the Microsoft Azure SQL Database user.
   - Select any **Encryption Method**.
7. Click **Save**.

   Data Source Name (DSN) details are saved.
8. Test the driver with credentials of the user that you have provided in the procedure and ensure that the connection passes.

Creating a Data Source Name on a Unix Operating System

This section describes how to create data source names on a Unix operating system, on which B2B Data Exchange is installed.

Note: Ensure that you configure a separate Data Source Name (DSN) entry for every database on which B2B Data Exchange is installed. The driver should point to the `DWsqls27.so` driver by using an absolute path.

Perform the following steps in the PowerCenter installation directory:

1. Navigate to the `<pwc_install_path>/ODBC7.1` folder in the PowerCenter installation directory and edit the `odbc.ini` driver to update the following information:
   - **Driver**. Enter a path to the driver.
     An example of the path is as follows: `/data/Informatica/10.1.1/ODBC7.1/lib/DWsqls27.so`.
   - **Description**. Enter the description of the DSN entry.
     An example of the description is as follows: `Azure SQL DATABASE Connection for ODL`
   - **Address**. Enter the host name of the machine where the database server is installed.
   - **LogonID**. Enter name for the Microsoft Azure SQL Database user.
   - **Password**. Enter a password for the Microsoft Azure SQL Database user.
   - **QuotedId**. Select `No`.
   - **AnsiNPW**. Select `Yes`.
   - **EncryptionMethod**. Enter a numerical value that corresponds to the encryption method that you want to select.
   - Enter `WorkArounds2=2`.

     Note: Enabling the WorkArounds2=2 option causes the driver to ignore the column size or decimal digits specified by the application and use the database defaults instead. Some applications incorrectly specify the column size or decimal digits when binding timestamp parameters.
   - If the `$ODBINI` environment variable pointing to the `odbc.ini` file was not configured, then configure the `$ODBINI` environment variable as follows:`$ODBCINI=<pwc_install_path>/ODBC7.1/odbc.ini`.

     Note: ODBC environment variables are configured before installing PowerCenter.

   An example of the configuration is as follows:

   ```
   Driver=<PwC_Install_Loc>/ODBC7.1/lib/DWsqls27.so
   Description=Azure SQL DATABASE Connection for ODL
   Address=<server_name>
   Database= <db_name>
   LogonID=<usn>
   Password=<pwd>
   QuotedId=No
   AnsiNPW=Yes
   EncryptionMethod=1
   ValidateServerCertificate=0
   WorkArounds2=2
   ```
2. If you configure the environment variable while creating data source name on the operating system as described in this procedure, then restart PowerCenter services.

Set Up a Directory for the Document Store

Set up a directory for the B2B Data Exchange document store.

The document store directory must be accessible to B2B Data Exchange, Apache Tomcat, Data Transformation, and PowerCenter with the same drive and file path.

Configure Access to the Data Transformation Service

Configure the PowerCenter Integration Service to access the Data Transformation service.

When you run workflows for B2B Data Exchange that include an Unstructured Data transformation, the PowerCenter Integration Service must be able to access a Data Transformation service.

Configure the Microsoft SQL Server Database

If you install B2B Data Exchange repositories on a Microsoft SQL Server database, enable the `READ_COMMITTED_SNAPSHOT` database option. If you install the Dashboard and Reports component, enable the `READ_COMMITTED_SNAPSHOT` option on the operational data store as well.

Note: If you use Microsoft SQL Server 2012, you can set the option **Is read committed snapshot on** in Microsoft SQL Server Management Studio to **true** instead.

1. Open an SQL query for the database server with rights to set database options.
2. Run the following SQL statements:

```
ALTER DATABASE [<database_name>] SET SINGLE_USER WITH ROLLBACK IMMEDIATE
```

3. Run the following SQL query:

```
ALTER DATABASE <database_name> SET READ_COMMITTED_SNAPSHOT ON
```

4. To verify that this option is set, run the following SQL query:

```
SELECT is_read_committed_snapshot_on FROM sys.databases WHERE name =
'<database_name>'
```

   If the option is set, the query returns the value 1. If the option is not set, the query returns the value 0.

5. Run the following SQL statement to forcefully disconnect all users from the system:

```
ALTER DATABASE [<database_name>] SET MULTI_USER
```

Opening Ports to the Partners Portal

If you want to install the Partners Portal, enable access to the portal in the firewall by opening the HTTP or HTTPS ports from the external network to the Portal server.

Configure the firewall to allow URLs that start with the suffix `/dx-portal` and `/dx-portal-help` only.

To ensure that outside access to the Partners Portal is securely performed, assign the external hostname URL for the portal to the **dx.portal.url** system property. For more information about configuring system properties in the B2B Data Exchange Operation Console, see the *B2B Data Exchange Administror Guide*.

CHAPTER 4

B2B Data Exchange Installation

This chapter includes the following topics:

Installing B2B Data Exchange on a Windows Operating System

Install B2B Data Exchange on Windows operating systems in graphical mode. On UNIX operating systems, install B2B Data Exchange in console mode.

Before you install, verify that your environment meets the minimum system requirements, perform the pre-installation tasks, and verify that the PowerCenter services are running.

Note: During the installation, B2B Data Exchange saves log files in the home directory of the user in the subdirectory named `DXLogs`. If the installation does not complete successfully, you can view the log files in this location.

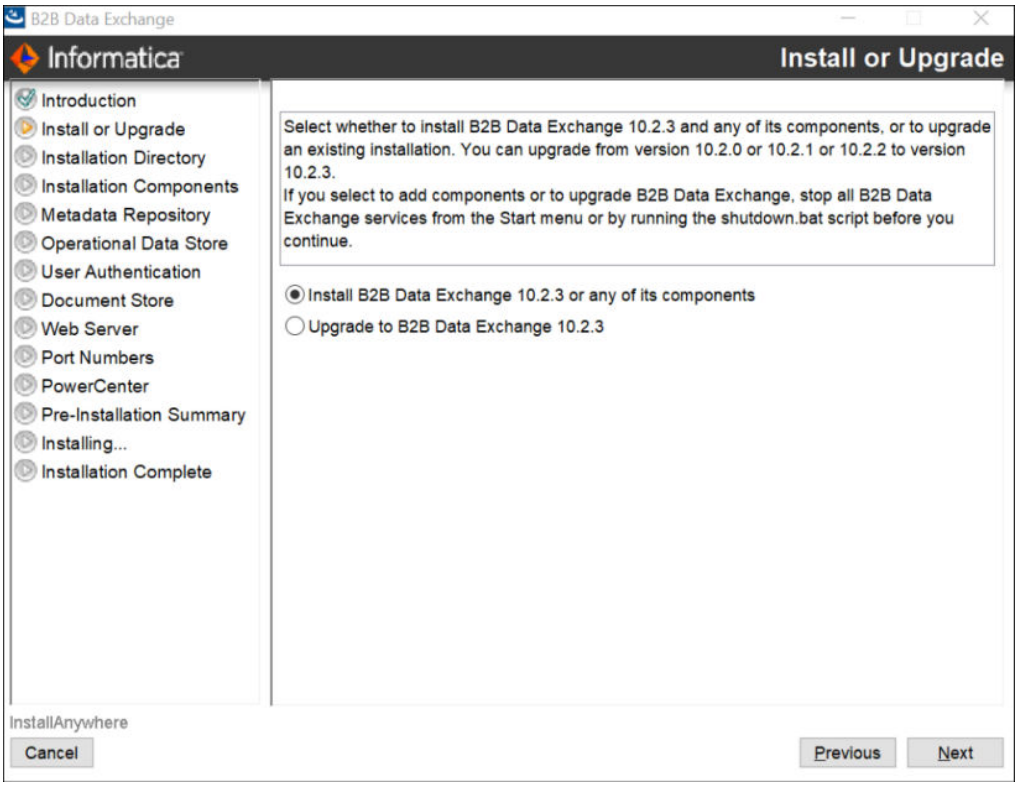
Step 1. Run the Installer

1. Log in to the machine with the user account that you want to use to install B2B Data Exchange.

   To prevent permission errors, use the same account to install B2B Data Exchange and PowerCenter.
2. Close all other applications.
3. Run `Install.exe` from the directory where you downloaded the installer.

   The **Introduction** page appears.
4. Read the instructions, and then click **Next**.

The **Install or Upgrade** page appears.

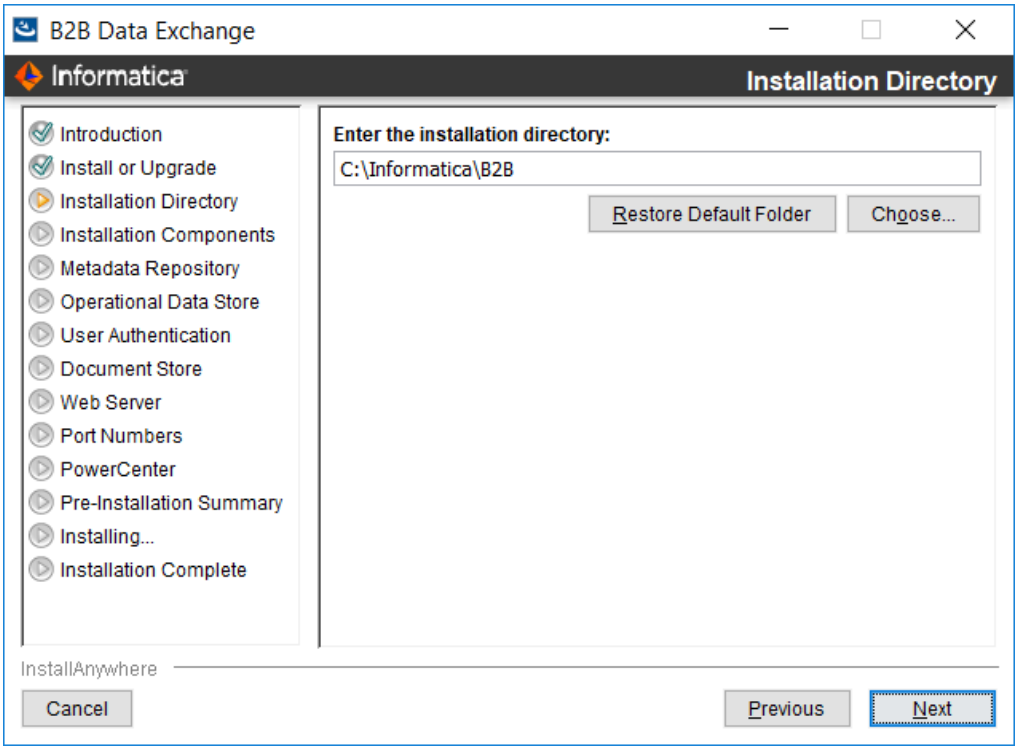


5. Select the option to install B2B Data Exchange, and then click **Next**.

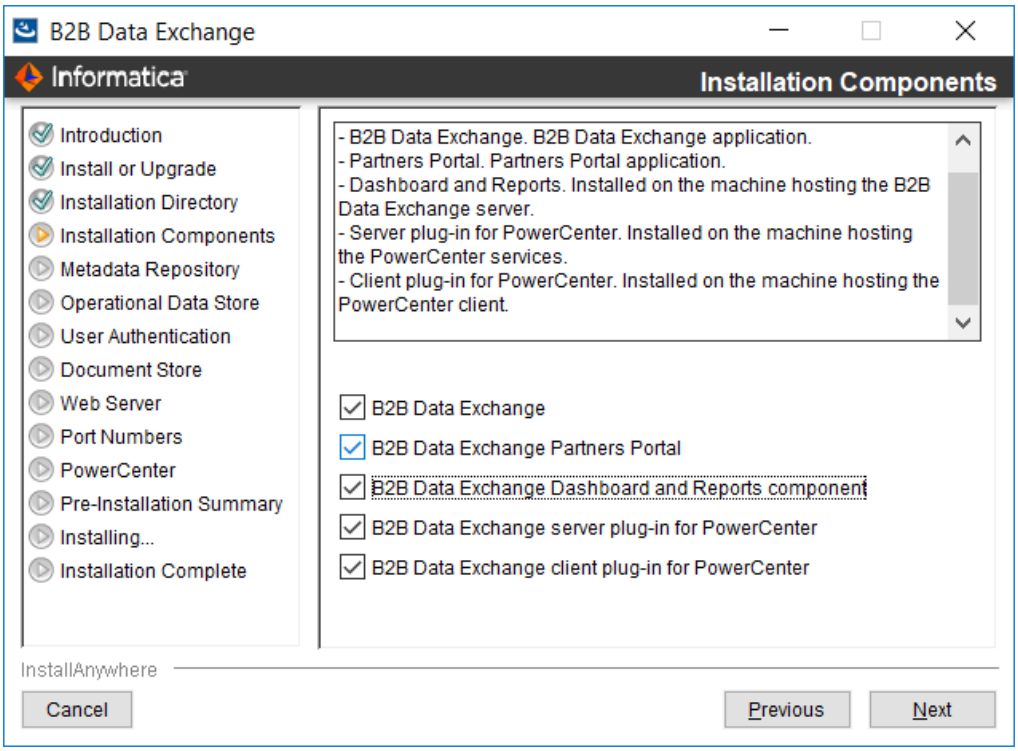
   The **Installation Directory** page appears.

Step 2. Define Installation Settings

1. On the **Installation Directory** page, enter the absolute path to the installation directory or accept the default directory, and then click **Next**.



The **Installation Components** page appears:



2. Select the components to install:

B2B Data Exchange

Installs the core B2B Data Exchange application.
Selected by default.

B2B Data Exchange Partners Portal

Installs the B2B Data Exchange Partners Portal component. You must install B2B Data Exchange to install the Partners Portal component.
Selected by default.

B2B Data Exchange Dashboard and Reports

Installs the B2B Data Exchange Dashboard and Reports component. You must install B2B Data Exchange to install the Dashboard and Reports component.
Cleared by default.

Note:

- If you install the Dashboard and Reports component, you must import the operational data store event loader after you install B2B Data Exchange.
- If you install the Dashboard and Reports component, your B2B Data Exchange and operational data store repositories are installed on Microsoft SQL Servers, and you use PowerCenter version 10, you must configure the repository connections in PowerCenter Workflow Manager. For details, see "Configuring Repository Connections on PowerCenter Version 10" on page 126.
- If you do not install the Dashboard and Reports component, the Dashboard will not be available in the Partners Portal.

B2B Data Exchange PowerCenter server plug-in

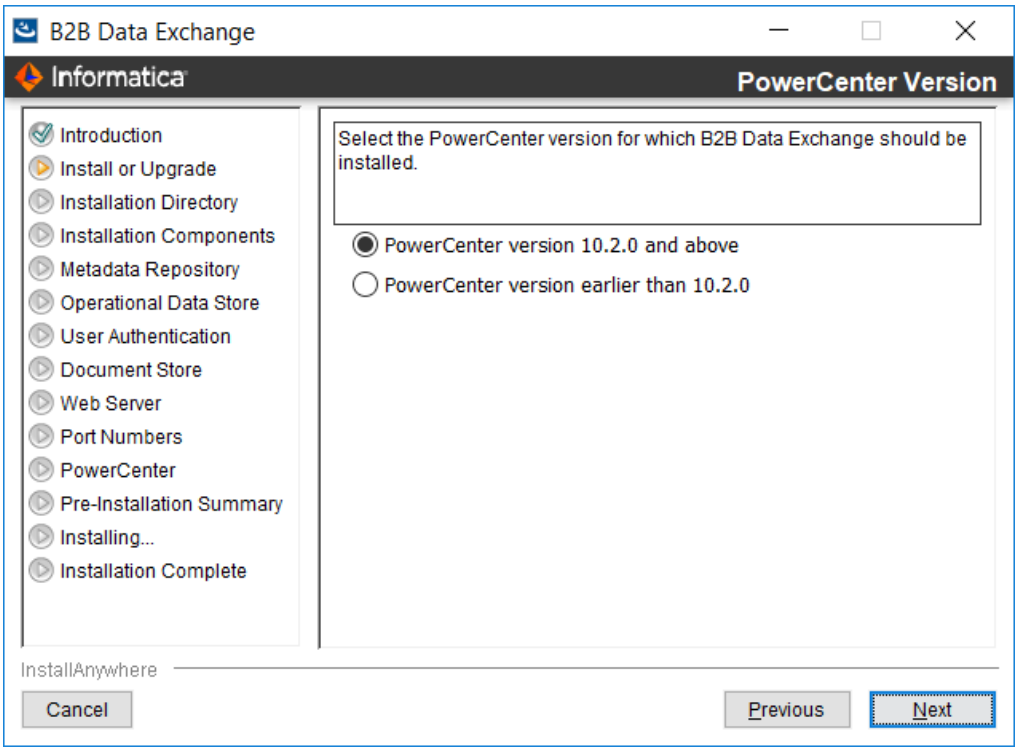
Installs the B2B Data Exchange plug-in for the PowerCenter services. After the installation, you register the plug-in to the PowerCenter repository.
Selected by default.

B2B Data Exchange PowerCenter client plug-in

Installs the B2B Data Exchange plug-in for the PowerCenter Client. Install this component on every machine that runs the PowerCenter Client.
Selected by default.

3. Click **Next**.

The **PowerCenter Version** page appears.



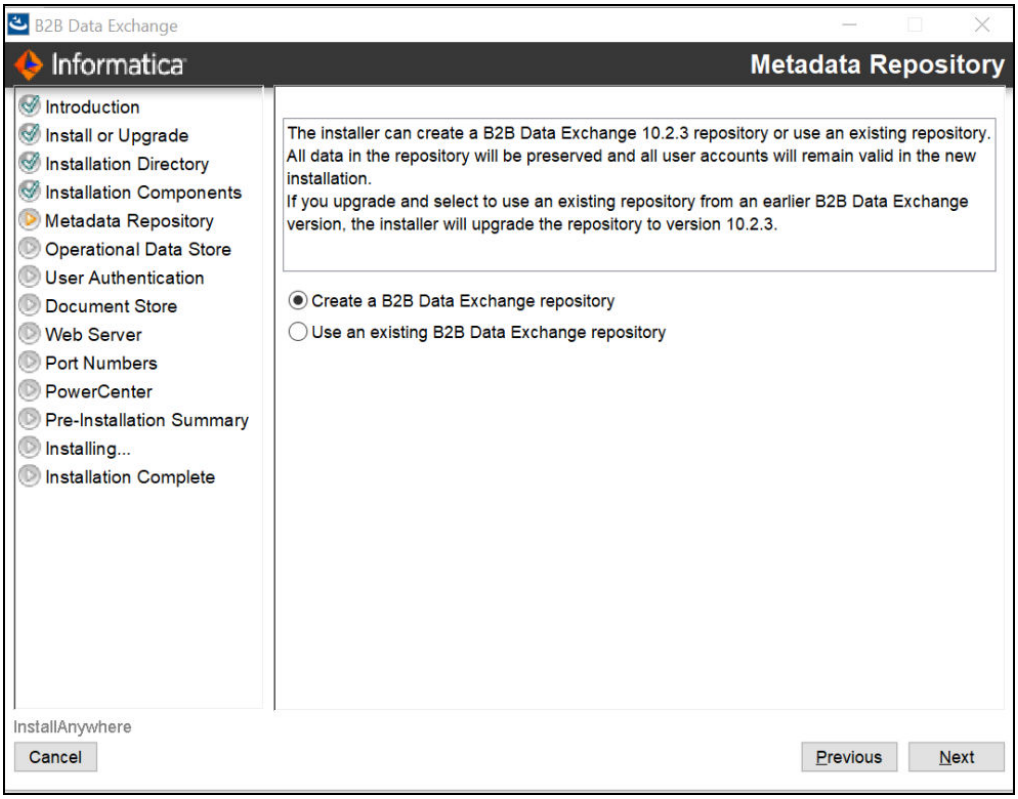
4. Select the PowerCenter version for which to install B2B Data Exchange and then click **Next**.

   The **Metadata Repository** page appears.

Step 3. Configure the B2B Data Exchange Repository

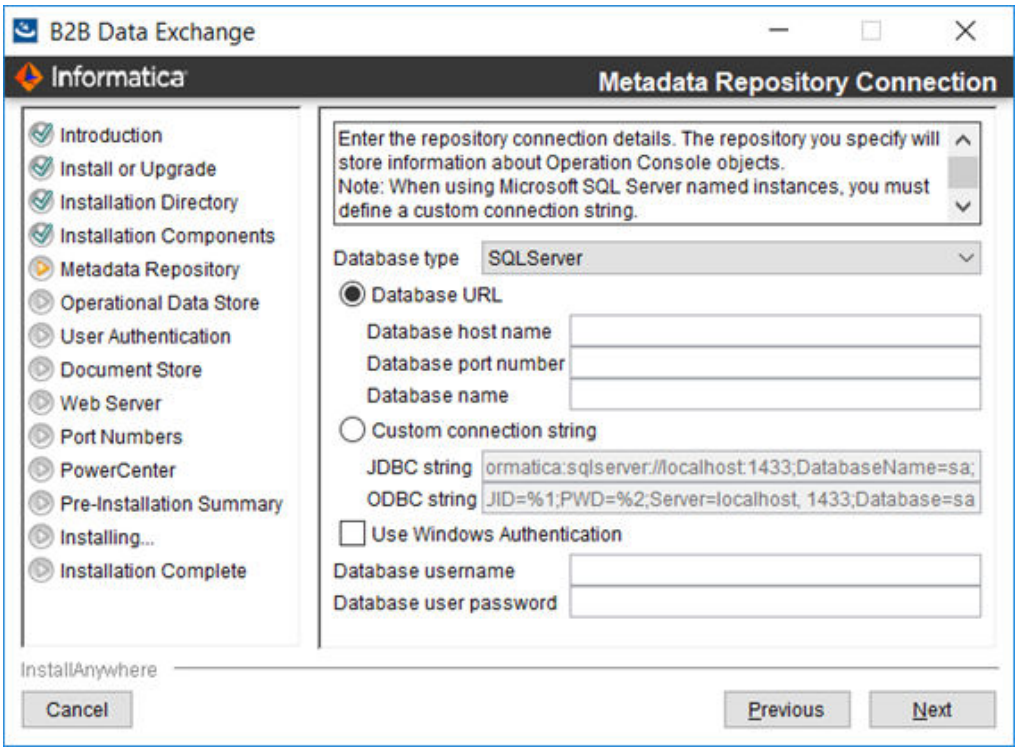
1. On the **Metadata Repository** page, select one of the following options:
   - **Create a B2B Data Exchange repository**. Creates a repository in the database.

- **Use an existing B2B Data Exchange repository**. Uses the tables and data in an existing B2B Data Exchange repository and upgrades the repository.



2. Click **Next**.

The **Metadata Repository Connection** page appears.



3. Enter values in the following fields:

Database type

Type of database to use for the B2B Data Exchange metadata repository. You can choose one of the following options:

- Oracle
- Microsoft SQL Server

Database URL

Location of the database.
If you select this option, enter the values in the following fields:

- **Database host name**. Host name of the machine where the database server is installed.
- **Database port**. Port number for the database. The default port number for Oracle is 1521. The default port number for Microsoft SQL Server is 1433.
- **Database SID**. System identifier for the database if the database is Oracle. Enter either a fully qualified ServiceName or a fully qualified SID.

  Note: It is recommended that you enter a ServiceName in this field.
- **Microsoft SQL Server database** . Database name.

Custom Connection String

Connection string to the database.
If you select this option, enter values in one of the following fields:

- **JDBC string**. JDBC connection string to the metadata repository.

- **ODBC string**. ODBC connection string to the metadata repository. Available if you install the PowerCenter Client plug-in. The installer cannot verify the validity of the ODBC string.

Use Windows Authentication

Instructs B2B Data Exchange to authenticate user names against the Microsoft Windows authentication mechanism. Available when you select a Microsoft SQL Server database.

Database username

Name of the database user account for the database where you do not use Windows authentication.

Database user password

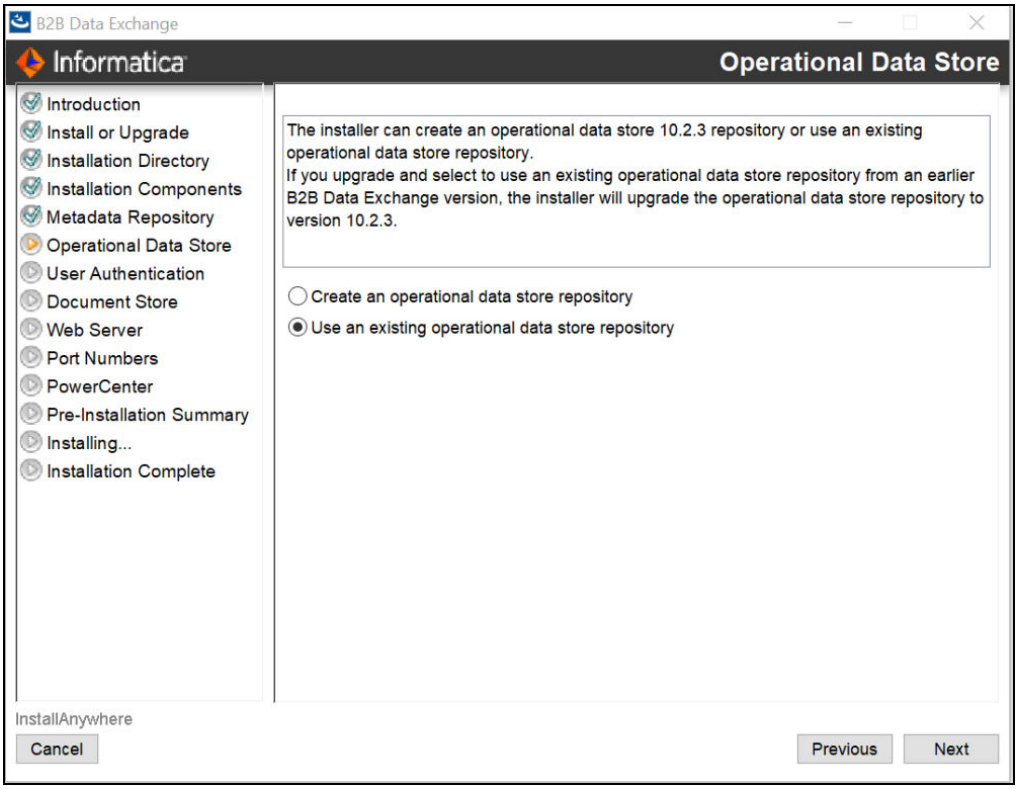
Password for the database account for the database where you do not use Windows authentication. B2B Data Exchange stores the password as an encrypted string.

4. Click **Next**.

If you selected the **B2B Data Exchange Dashboard and Reports** component, the **Operational Data Store** page appears. If you did not select the Dashboard and Reports component, go to "Step 5. Configure User Authentication" on page 34.

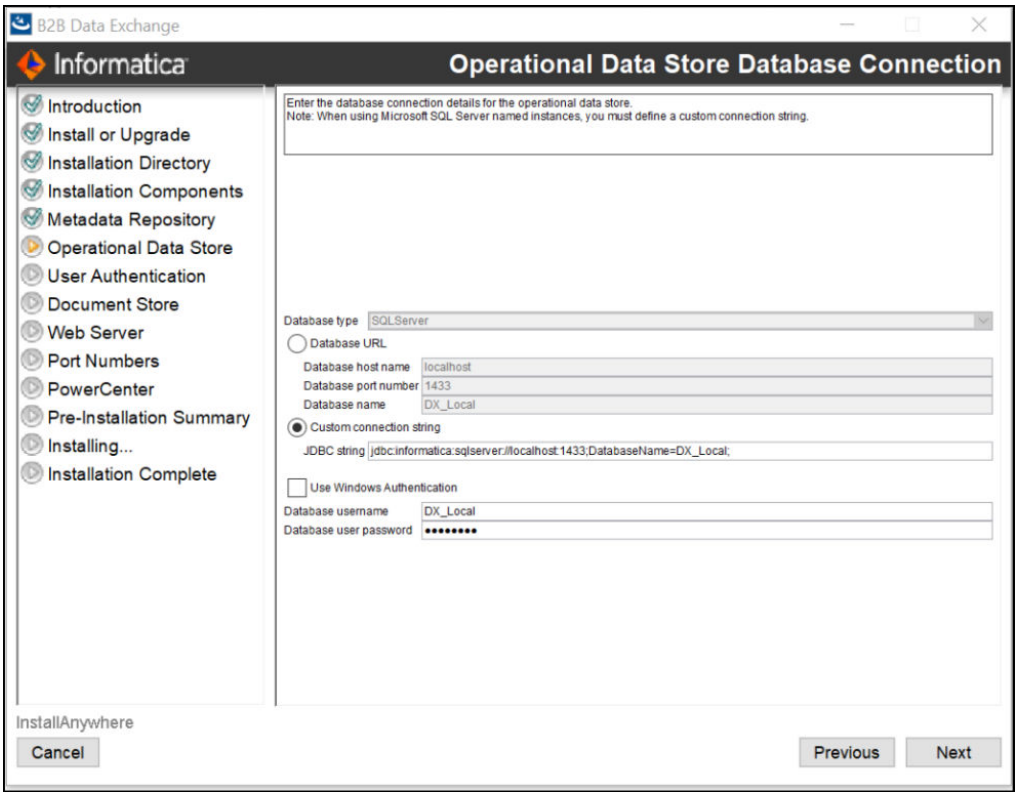
Step 4. Set Up the Operational Data Store

1. On the **Operational Data Store** page, select one of the following options:
   - **Create an operational data store repository**. Creates an operational data store repository in the database.
   - **Use an existing operational data store repository**. Uses the tables and data in an existing operational data store repository.



2. Click **Next**.

The **Operational Data Store Database Connection** page appears.



3. Enter values in the following fields:

Database URL

Location of the database. If you select this option, enter the values in the following fields:

- **Database host name**. Host name of the machine where the database server is installed.
- **Database port number**. Port number for the database. The default port number for an Oracle database is 1521. The default port number for a Microsoft SQL server is 1433.
- **Database SID**. System identifier for the database if you select Oracle as the database. Enter either a fully qualified ServiceName or a fully qualified SID.

  Note: It is recommended that you enter a ServiceName in this field.
- **Microsoft SQL Server database** . Database name.

Custom Connection String

Connection string to the database. If you select this option, enter values in one of the following fields:

- **JDBC string**. JDBC connection string to the Operational Data Store.
- **ODBC string**. ODBC connection string to the Operational Data Store. Available if you install the PowerCenter Client plug-in. The installer cannot verify the validity of the ODBC string.

Note: If you use a named Microsoft SQL Server database instance, you cannot connect to the database instance using the **Database URL** option. Use the **Custom Connection String** option.

For example:

```
jdbc:informatica:sqlserver://MYSQLSERVERCOMPUTERHOSTNAME
\MYDBINSTANCENAME;DatabaseName=MYDATABASENAME;
```

Use Windows Authentication

Instructs B2B Data Exchange to authenticate user names against the Microsoft Windows authentication mechanism. Available when you select a Microsoft SQL Server database.

Database username

Name of the operational data store user account for the database where you do not use Windows authentication.

Database user password

Password for the operational data store account for the database where you do not use Windows authentication. B2B Data Exchange stores the password as an encrypted string.

4. Click **Next**.

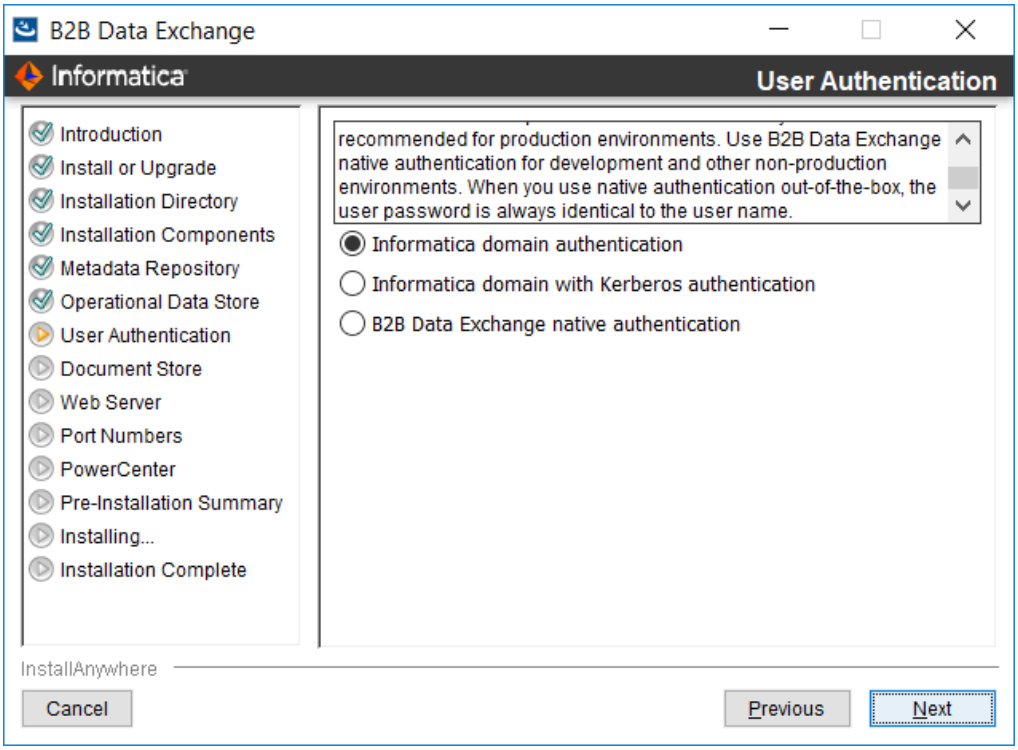
   If you create a repository in the database, the **User Authentication** page appears. If you select an existing repository, the installer selects the existing authentication method. Go to "Step 6. Configure Document Store, Web Server, and Port Numbers" on page 40.

Step 5. Configure User Authentication

1. On the **User Authentication page**, choose the type of user authentication that you want to use.
   - Choose **Informatica domain authentication** to manage user credentials in the Informatica domain and synchronize user information with B2B Data Exchange. Use Informatica domain authentication for production environments. For more information, see "Configure Settings for Informatica Domain Authentication " on page 35.

     Note: If your Informatica domain uses Kerberos authentication, choose the option **Informatica domain with Kerberos authentication**.
   - Choose **Informatica domain with Kerberos authentication** if the Informatica domain uses Kerberos authentication. Use Informatica domain with Kerberos authentication for production environments. For more information, see "Configure Settings for Informatica Domain with Kerberos Authentication" on page 37.

- Choose **B2B Data Exchange native authentication** to manage user credentials locally in B2B Data Exchange. Use native authentication in development and staging environments. For more information, see "Configure Settings for B2B Data Exchange Native Authentication" on page 38.



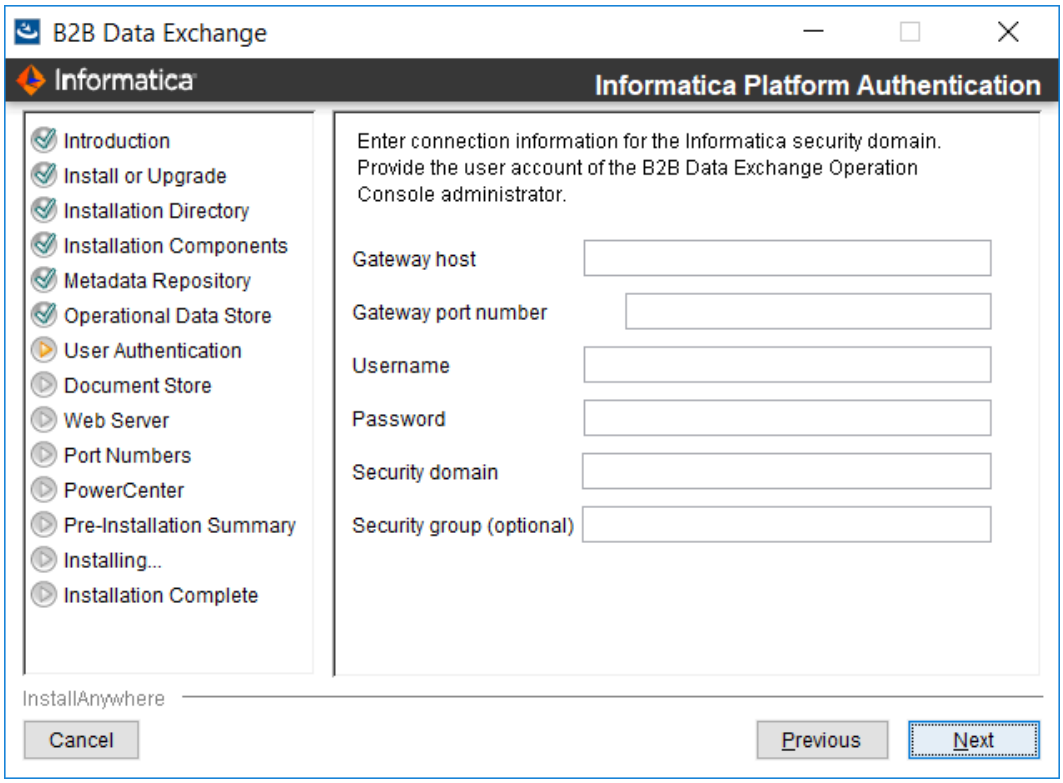
2. Enter the authentication information, and then click **Next**.

   The **Data Exchange Document Store** page appears.

Configure Settings for Informatica Domain Authentication

If you select the **Informatica Domain Authentication** option on the **User Authentication** page, you can configure the Informatica domain authentication settings on the **Informatica Platform Authentication** page.

The following image shows the **Informatica Platform Authentication** page.



The following table describes the settings that you need to configure for the **Informatica Platform Authentication** page:

Gateway host

Host name of the Informatica security domain server. B2B Data Exchange stores the host name in the `pwc.domain.gateway` system property.

Gateway port number

Port number for the Informatica security domain gateway. B2B Data Exchange stores the port number in the `pwc.domain.gateway` system property. Use the gateway HTTP port number to connect to the domain from the PowerCenter Client. You cannot use the HTTPS port number to connect to the domain.

Username

User name to access the Administrator tool. You must create the user in the Administrator tool and assign the **manage roles/groups/user** privilege to the user.

Password

Password of the Informatica security domain user.

Security domain

Name of the Informatica security domain where the user is defined.

Security group

Optional. Security group within the Informatica security domain where B2B Data Exchange users are defined in the following format:

```
<security group>@<domain>
```

If you leave the field empty, the Informatica security domain synchronizes only the B2B Data Exchange administrator user account.

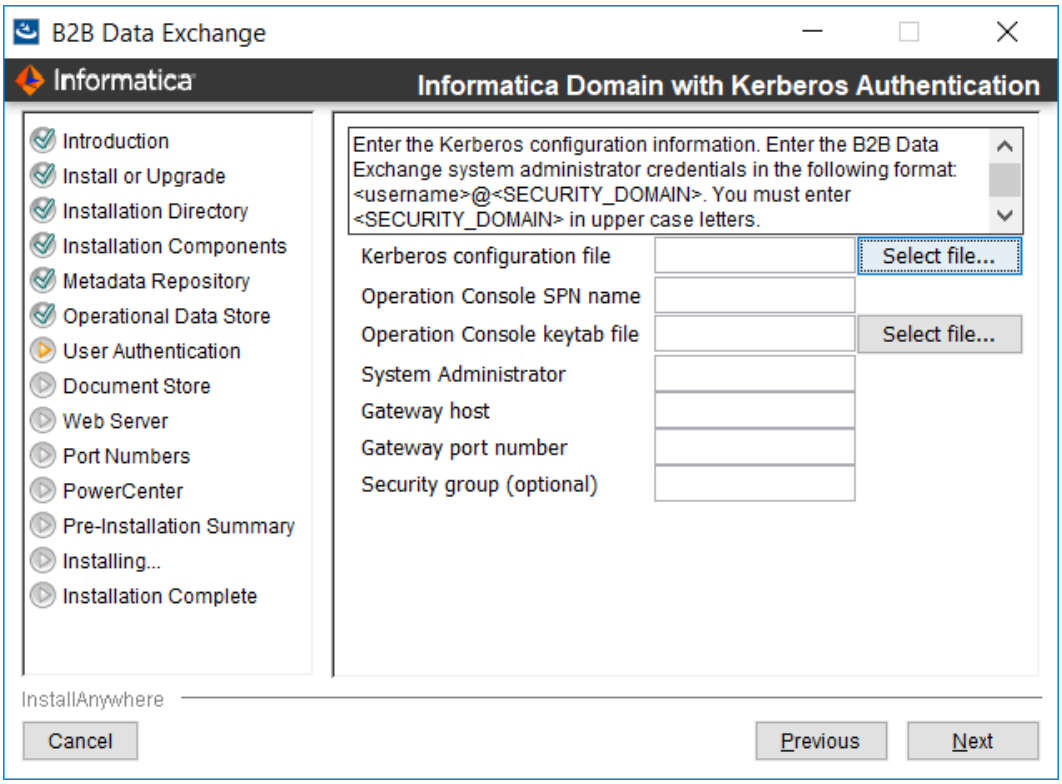
B2B Data Exchange stores the security group in the dx.authentication.groups system property in the following format:

```
<group name>@<security group>[;<groupname>@<security group>]
```

Configure Settings for Informatica Domain with Kerberos Authentication

If you select the **Informatica domain with Kerberos authentication** option on the **User Authentication** page, you can configure the authentication settings on the **Informatica Domain with Kerberos Authentication** page.

The following image shows the **Informatica Domain with Kerberos Authentication** page.



Enter the configuration information.

Kerberos configuration file

File that stores Keberos configuration information, usually named `krb5.conf`

The installation copies the file to the following location:

```
<DXInstallationDir>/shared/conf/security/krb5.conf
```

Operation Console SPN name

Service Principal Name (SPN) for the B2B Data Exchange Operation Console.

B2B Data Exchange stores the SPN in the `dx-security-config.properties` property file, in the dx.kerberos.console.service.principal.name property.

Operation Console keytab file

Location of the keytab file for the B2B Data Exchange Operation Console SPN.

The installer copies the file to the following location:

```
<DXInstallationDir>/shared/conf/security/HTTP_console.keytab
```

B2B Data Exchange stores the location of the keytab file in the `dx-security-config.properties` property file, in the dx.kerberos.console.keytab.file property.

If you change the property to point to a different file, you must enter the absolute path to the file using the following format:

```
file://<full_path>
```

System Administrator

B2B Data Exchange system administrator credentials.

Enter the credentials in the following format:

```
<username>@<SECURITY_DOMAIN>
```

Note: You must enter `<SECURITY_DOMAIN>` in uppercase letters.

Gateway host

PowerCenter domain gateway host.

Gateway port number

PowerCenter domain gateway port number.

Security group

Optional. Security group within the Informatica security domain where B2B Data Exchange users are defined in the following format:

```
<security group>@<domain>
```

If you leave the field empty, the Informatica security domain synchronizes only the B2B Data Exchange administrator user account.

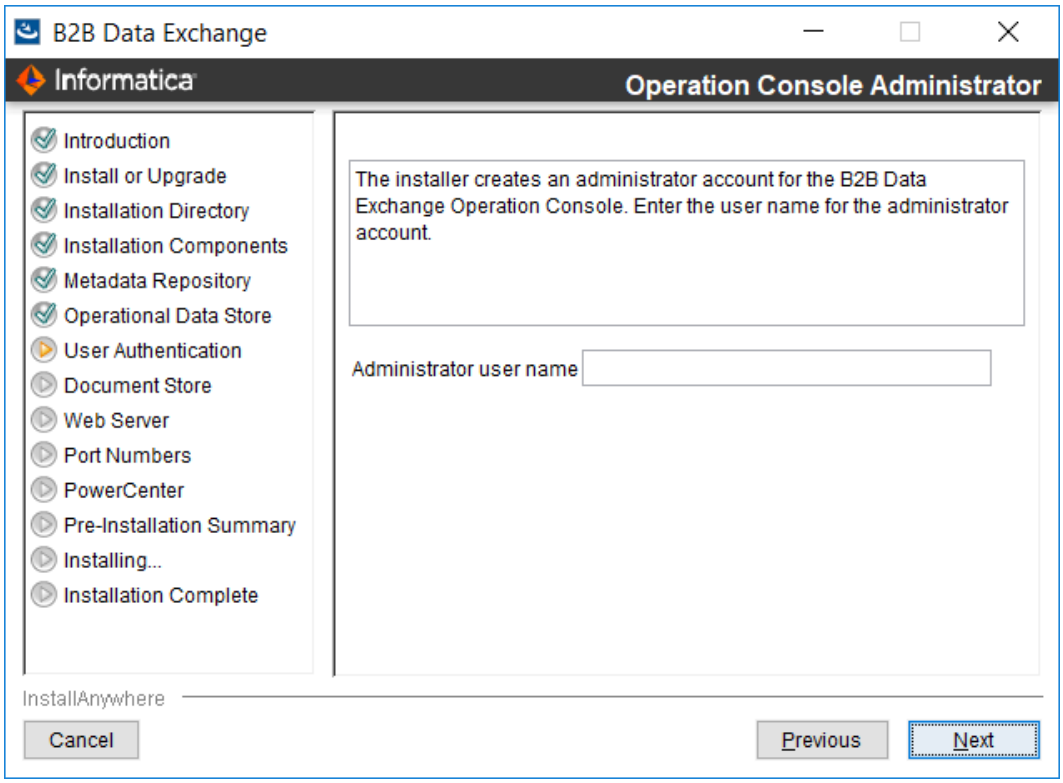
B2B Data Exchange stores the security group in the dx.authentication.groups system property in the following format:

```
<group name>@<security group>[;<groupname>@<security group>]
```

Configure Settings for B2B Data Exchange Native Authentication

If you select the **B2B Data Exchange native authentication** option on the **User Authentication** page, you need to enter the B2B Data Exchange administrator user name on the **Operation Console Administrator** page. B2B Data Exchange uses this value for the user name and password when you log in to the Operation Console.

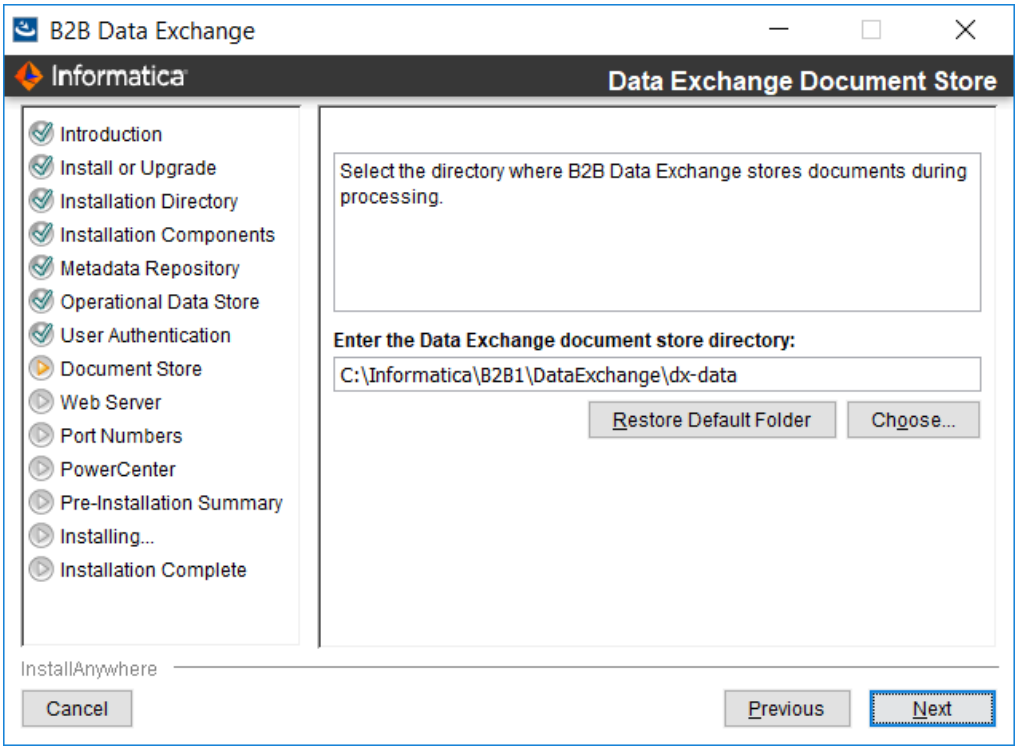
The following image shows the **Operation Console Administrator** page.



Step 6. Configure Document Store, Web Server, and Port Numbers

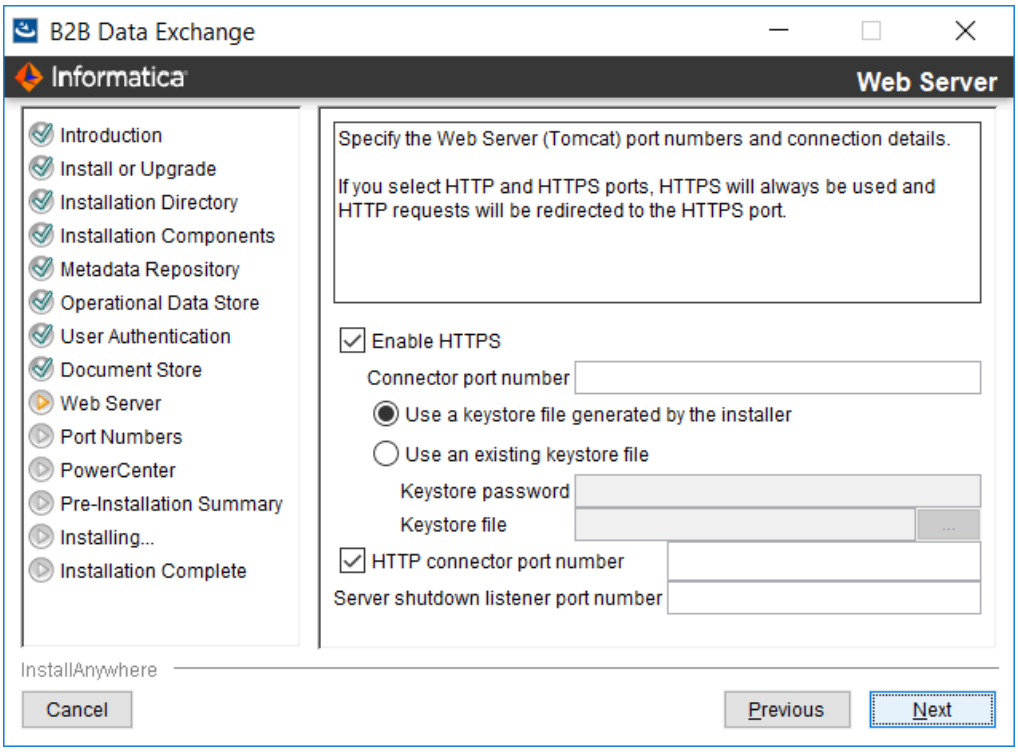
1. On the **Data Exchange Document Store** page, accept the default directory or enter the directory where you want to create the document store directory.

   B2B Data Exchange stores documents and files in the document store during processing. The document store directory must be accessible to B2B Data Exchange, PowerCenter services, and Data Transformation.



2. Click **Next**.

The **Web Server** page appears.



3. Enter values in the following fields:

Enable HTTPS

Instructs B2B Data Exchange to use secure network communication when you open the Operation Console in the browser. If you select HTTPS and HTTP, the Operation Console switches existing HTTP connections with HTTPS connections.

Connector port number

Port number for the Tomcat connector to use when you open the Operation Console with HTTPS. The default value is 18443.

Use a keystore file generated by the installer

Instructs the installer to generate a keystore file with an unregistered certificate. If you select this option, ignore the security warning that you receive from the browser the first time you open the Operation Console.

Use an existing keystore file

Instructs the installer to load an existing keystore file. Enter values in the following fields:

- Keystore password. Password for the keystore file.
- Keystore file. Path to the keystore file.

The keystore file must be in the Public Key Cryptography Standard (PKCS) #12 format.

HTTP connector port number

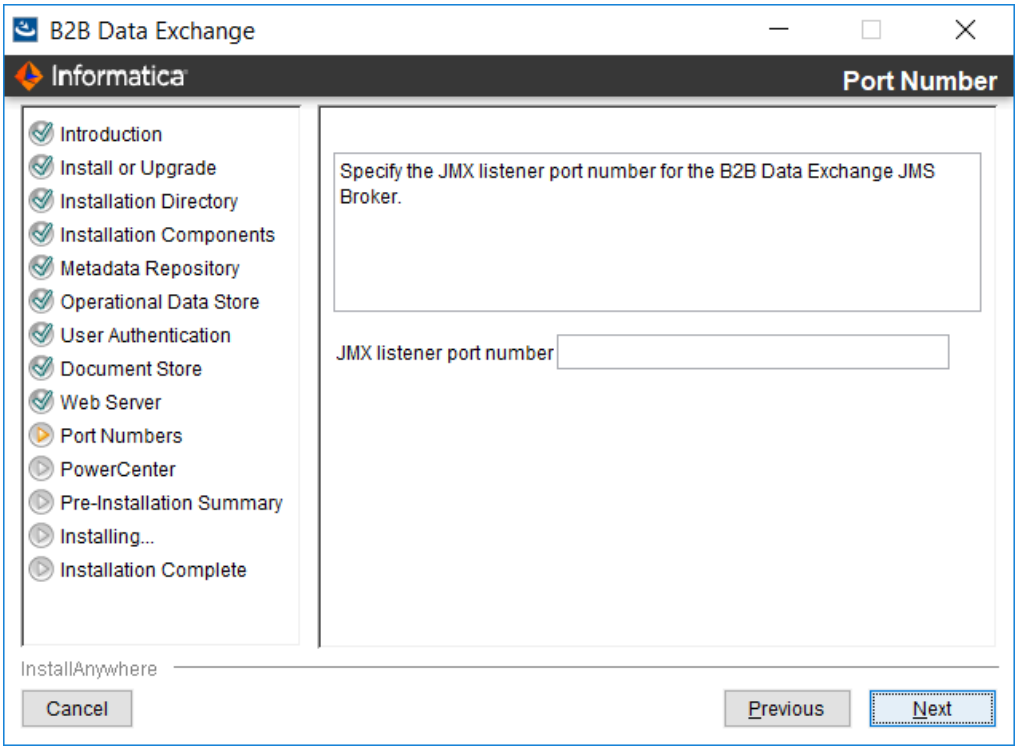
Port number for the HTTP connector. If you clear this field, your browser must connect to the B2B Data Exchange server with HTTPS when you log in to the Operation Console.
The default value is 18080.

Server shutdown listener port number

Port number for the listener that controls the Tomcat server shutdown. The default value is 18005.

4. Click **Next**.

   The **Port Numbers** page appears.

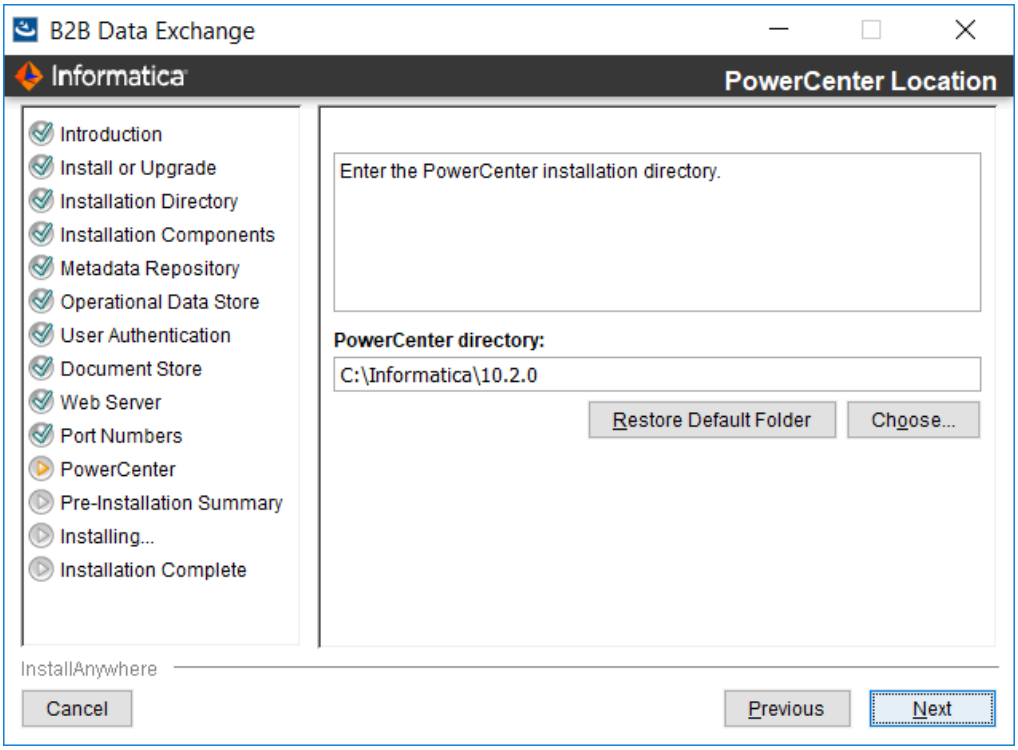


5. Enter the port number for the B2B Data Exchange JMS Broker JMX listener port or accept the default port, and then click **Next**.

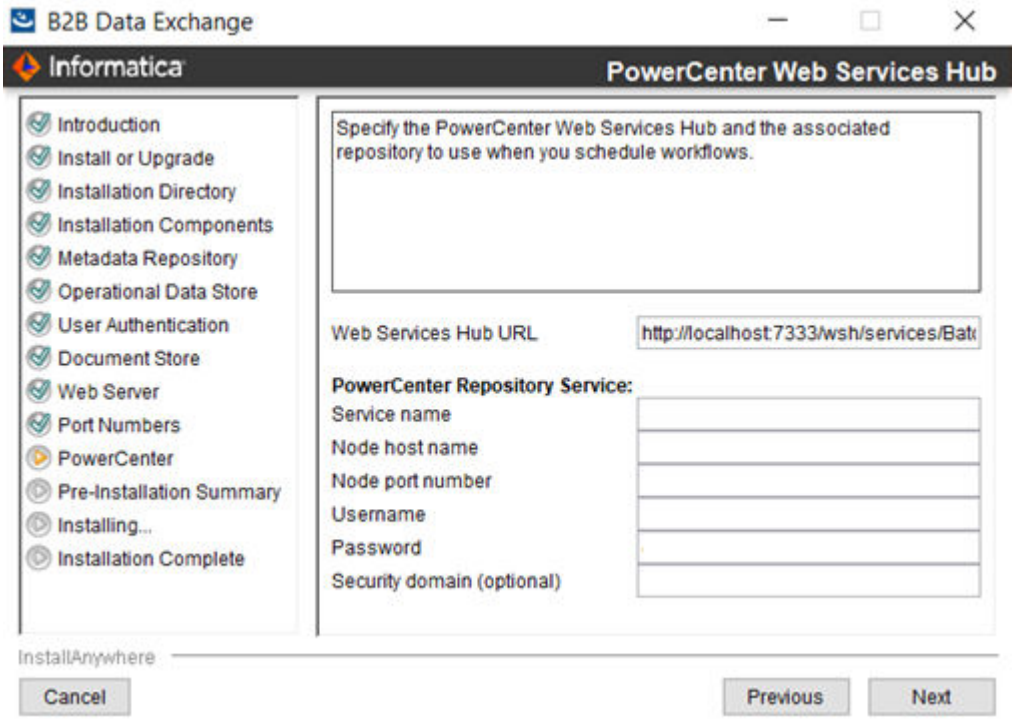
   If you selected to install the B2B Data Exchange server plug-in for PowerCenter or the B2B Data Exchange client plug-in for PowerCenter components, the **PowerCenter Location** page appears. If you did not select the PowerCenter server or client components, the **PowerCenter Web Services Hub** page appears.

Step 7. Configure PowerCenter Settings

1. If you selected to install the B2B Data Exchange server plug-in for PowerCenter or the B2B Data Exchange client plug-in for PowerCenter components, on the **PowerCenter Location** page, enter the directory where you installed PowerCenter or accept the default directory, and then click **Next**.



The **PowerCenter Web Services Hub** page appears.



2. On the **PowerCenter Web Services Hub** page, enter the PowerCenter web services details.

   Web Services Hub URL

   URL that the PowerCenter Web Services Hub uses when B2B Data Exchange transfers documents to PowerCenter for processing with batch workflows.

   Service name

   Name of the PowerCenter Repository Service.

   Node host name

   Host name of the node that runs the PowerCenter Repository Service.

   Node port number

   Port number of the node that runs the PowerCenter Repository Service.

   Username

   Name of the PowerCenter Repository Service user.

   Password

   Password for the PowerCenter Repository Service user. B2B Data Exchange stores the password as an encrypted string.

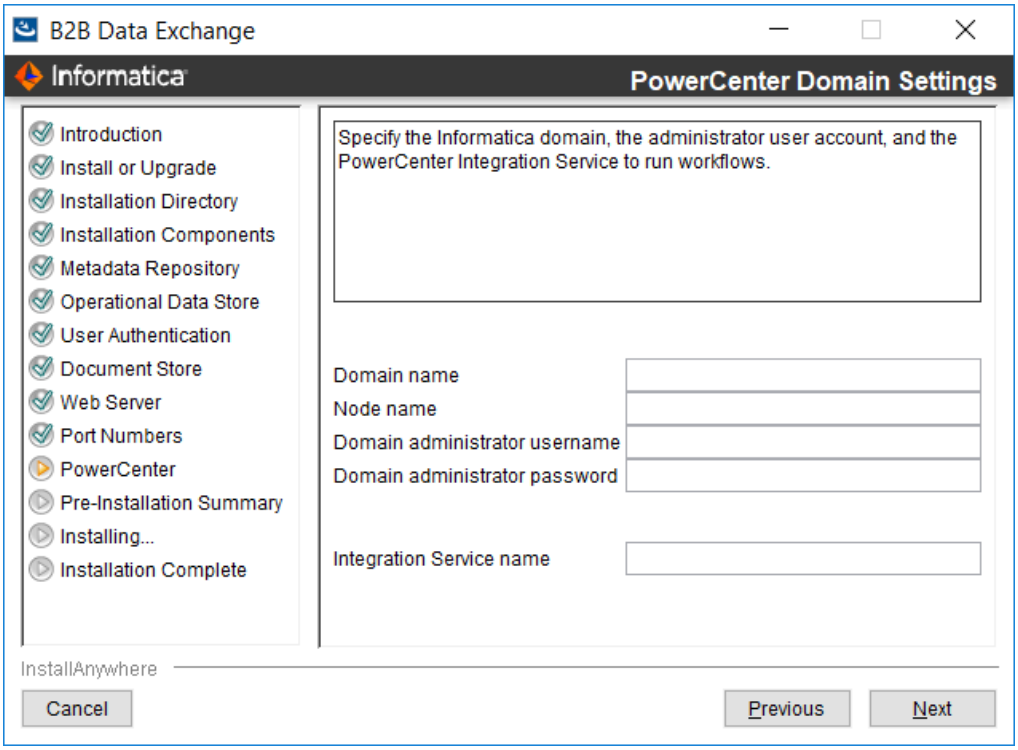
   Security domain

   Optional. Name of the Informatica security domain in which the PowerCenter Repository Service user is stored.
   Default is Native.

3. Click **Next**.

   If you selected to install the B2B Data Exchange server plug-in for PowerCenter component, the **PowerCenter Domain Settings** page appears.

If you did not select the PowerCenter server component, the **PowerCenter pmrep Command Line Utility Location** page appears. Go to step 6.



4. Enter values in the following fields:

Domain name

Name of the Informatica domain that contains the PowerCenter Integration Service that runs B2B Data Exchange workflows.

Node name

Node in the Informatica domain on which the PowerCenter Integration Service runs.

Domain administrator username

Name of the Informatica domain administrator.

Domain administrator password

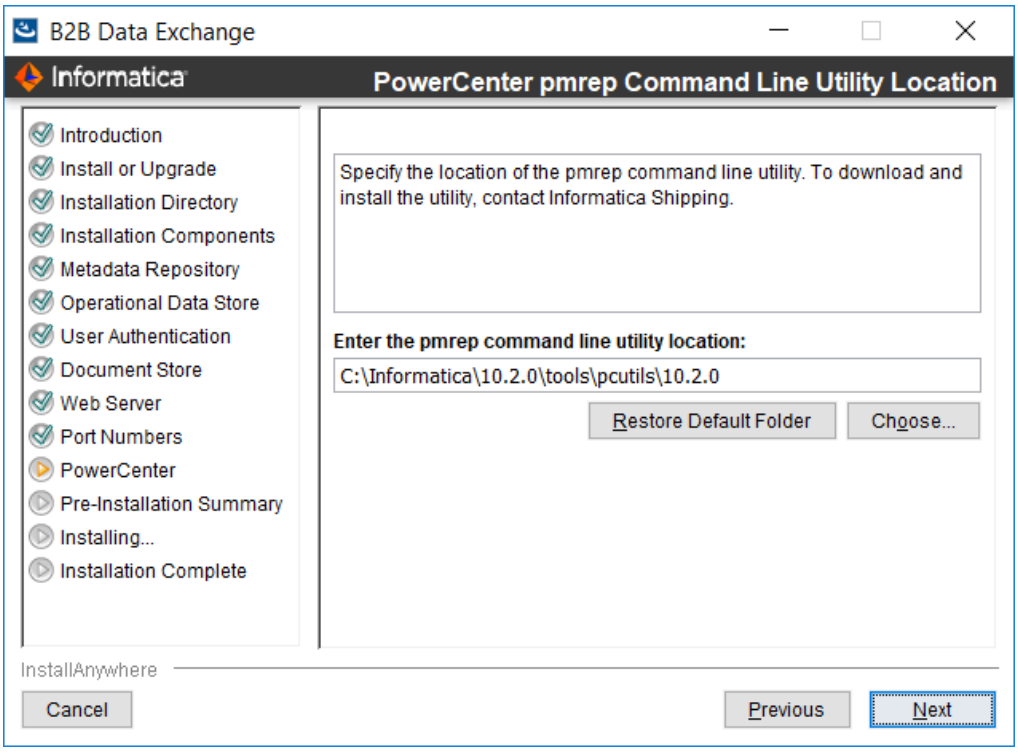
Password for the Informatica domain administrator. B2B Data Exchange stores the password as an encrypted string.

Integration Service name

The name of the PowerCenter Integration Service that B2B Data Exchange uses to run workflows.

5. Click **Next**.

The **PowerCenter pmrep Command Line Utility Location** page appears.



6. Specify the location of the pmrep command line utility.

   The location of the utility depends on whether or not you install B2B Data Exchange on the machine where the PowerCenter services are installed.

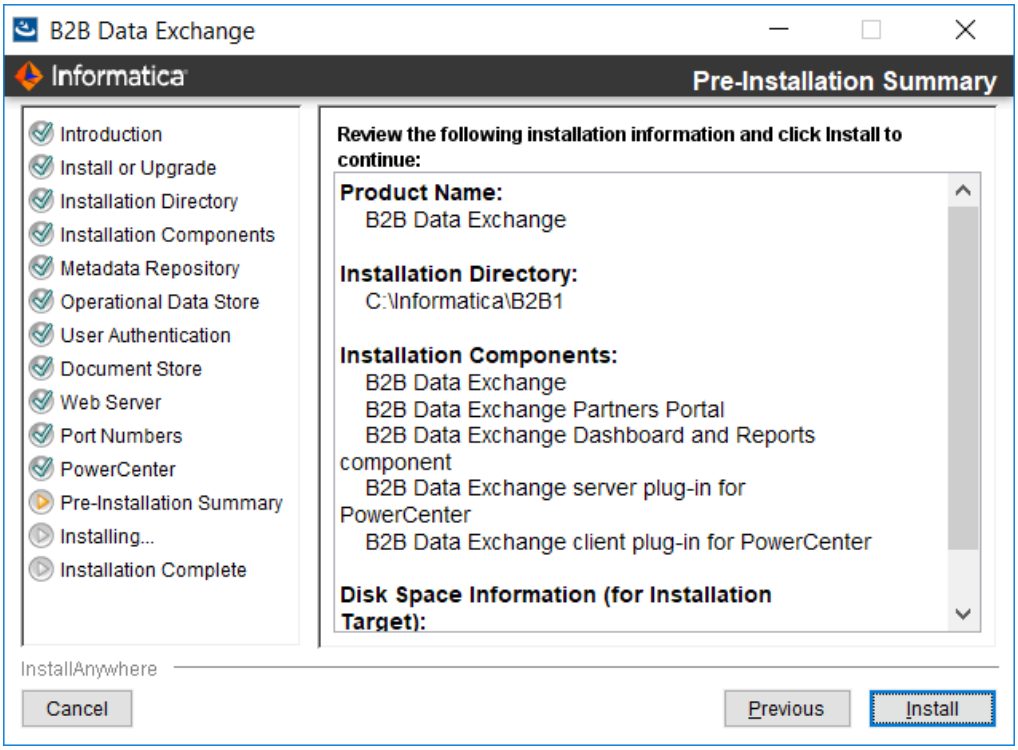
Environment	Location of the pmrep command line utility
B2B Data Exchange installed on the machine where the PowerCenter services are installed	`<PowerCenter_services_installation_folder>\<PowerCenter_version>\tools\pcutils\<PowerCenter_version>`
B2B Data Exchange and PowerCenter services installed on different machines	`<PowerCenter_client_installation_folder>\<PowerCenter_version>\clients\PowerCenterClient\client\bin`

7. Click **Next**.

   The **Pre-Installation Summary** page appears.

Step 8. Complete the Installation

1. On the **Pre-Installation Summary** page, verify that the installation information is correct, and then click **Install**.



   During the installation process, the installer displays progress information. When the installation process ends, the **Post-Installation Actions** page appears.

2. If you installed the B2B Data Exchange PowerCenter server plug-in, follow the wizard instructions to register the plug-in to the PowerCenter repository, and then click **Next**.

   The **Installation Complete** page appears.

3. Click **Done** to close the installer.

4. To view the log files that the installer generates, navigate to the following directory: `<DXInstallationDir>\logs`.

5. Perform the required post-installation tasks.

   For more information, see Chapter 5, “Post-Installation Tasks” on page 65.

   Note: Perform only the tasks that are relevant for your environment.

6. Optionally, perform additional configuration tasks. For more information, see Chapter 9, “Optional B2B Data Exchange Configuration” on page 115.

Installing B2B Data Exchange on a UNIX Operating System in Console Mode

Install B2B Data Exchange on UNIX operating systems in console mode. On Windows operating systems, install B2B Data Exchange in graphical mode.

Before you install, verify that your environment meets the minimum system requirements, perform the pre-installation tasks, and verify that the PowerCenter services are running.

During the installation, B2B Data Exchange saves log files in the home directory of the user, in the subdirectory named `DXLogs`. If the installation does not complete successfully, you can view the log files in this location.

Step 1. Run the Installer

1. Log in to the machine with the user account that you want to use to install B2B Data Exchange.

   To prevent permission errors, use the same account to install B2B Data Exchange and PowerCenter.
2. Close all other applications.
3. Run `Install.bin -i console` from the directory where you downloaded the installer.

   The **Introduction** section appears.
4. Read the instructions, and then press **Enter**.

   The **Install or Upgrade** section appears.
5. Enter **1** to install B2B Data Exchange, and then press **Enter**.

   The **Installation Directory** section appears.

Step 2. Define Installation Settings

1. In the **Installation Directory** section, enter the absolute path to the installation directory or accept the default directory, and then press **Enter**.

   The **Installation Components** section appears and displays a numbered list of the components to install.
2. Enter a comma-separated list of numbers for the components to install or accept the default components:

   1- B2B Data Exchange

   Installs the core B2B Data Exchange application.
   Selected by default.

   2- B2B Data Exchange Partners Portal

   Installs the B2B Data Exchange Partners Portal component. You must install B2B Data Exchange to install the Partners Portal component.
   Selected by default.

   3- B2B Data Exchange Dashboard and Reports

   Installs the B2B Data Exchange Dashboard and Reports component. You must install B2B Data Exchange to install the Dashboard and Reports component.
   Cleared by default.

Note:

- If you install the Dashboard and Reports component, you must import the operational data store event loader after you install B2B Data Exchange.
- If you install the Dashboard and Reports component, your B2B Data Exchange and operational data store repositories are installed on Microsoft SQL Servers, and you use PowerCenter version 10, you must configure the repository connections in PowerCenter Workflow Manager. For details, see "Configuring Repository Connections on PowerCenter Version 10" on page 126.
- If you do not install the Dashboard and Reports component, the Dashboard will not be available in the Partners Portal.

4- B2B Data Exchange Server Plug-in for PowerCenter

Installs the B2B Data Exchange PowerCenter server plug-in component. After the installation, register the plug-in to the PowerCenter repository.
Selected by default.

3. Press **Enter**.

   The **PowerCenter Version** section appears.

4. Select the PowerCenter version for which to install B2B Data Exchange or accept the default selection:

   1- PowerCenter version below 10.2.0

   Select this option for PowerCenter versions below 10.2.0.

   2 - PowerCenter version 10.2.0 and above

   Select this option for PowerCenter versions 10.2.0 and above.

5. Press **Enter**.

   The **Metadata Repository** section appears.

Step 3. Configure B2B Data Exchange Repository

1. In the **Metadata Repository** section, enter the number for the metadata repository database configuration option or accept the default option:

   1- Create a B2B Data Exchange repository

   Creates a repository in the database.

   2- Use an existing B2B Data Exchange repository

   Uses the tables and data in an existing repository.

2. Press **Enter**.

   The **Metadata Repository Connection** section appears.

3. Enter one of the following numericals depending on the database you plan to use as the B2B Data Exchange metadata repository database:

   - Enter `1` to use an Oracle database as the B2B Data Exchange metadata repository database.
   - Enter `2` to use Microsoft SQL Server database as the B2B Data Exchange metadata repository database.

4. Enter the number for the metadata repository database connection type or accept the default connection type:

1- Database URL

Location of the database. If you select this option, enter values in the following fields:

- **Database Host Name**. Host name of the machine where the database server is installed.
- **Database Port Number**. Port number for the database. The default port number for Oracle is 1521. The default port for Microsoft SQL Server 1433.
- **Database SID**. System identifier for the database.
- **Microsoft SQL Server database** . Database name. Name of the database instance.

2- Custom Connection String

Connection string to the database. If you select this option, enter values in one of the following fields:

- JDBC string. JDBC connection string to the metadata repository.
- ODBC string. ODBC connection string to the metadata repository. Applicable if you install the PowerCenter client plug-in. The installer cannot verify the validity of the ODBC string.

Note: If you use a named Microsoft SQL Server database instance, you cannot connect to the database instance using the **Database URL** option. Use the **Custom Connection String** option.

For example:

```
jdbc:informatica:sqlserver://MYSQLSERVERCOMPUTERHOSTNAME
\MYDBINSTANCENAME;DatabaseName=MYDATABASENAME;
```

5. Enter values in the following fields:

Database username

Name of the database user account.

Database user password

The password for the database account for the database. B2B Data Exchange stores the password as an encrypted string.

6. Press **Enter**.

If you selected to install the B2B Data Exchange Dashboard and Reports component, the **Operational Data Store** section appears. If you did not select to install the Dashboard and Reports component, go to "Step 5. Configure the Web Server and Port Numbers" on page 105.

Step 4. Set Up the Operational Data Store

1. In the **Operational Data Store** section, enter the number for the database configuration option for the operational data store or accept the default option:

1- Create an operational data store repository

Creates an operational data store repository in the database.

2- Use an existing operational data store repository

Uses the tables and data in an existing operational data store repository.

2. Enter the number for the database connection type for the operational data store or accept the default connection type:

1- Database URL

Location of the database. If you select this option, enter values in the following fields:

- **Database host name**. Host name of the machine where the database server is installed.
- **Database port number**. Port number for the database. The default port number for Oracle is 1521. The default port for Microsoft SQL Server is 1433.
- **Oracle database**. Database SID. System identifier for the database.
- **Microsoft SQL Server database** . Database name. Name of the database instance.

2- Custom Connection String

Connection string to the database. If you select this option, enter values in one of the following fields:

- **JDBC string.** JDBC connection string to the Operational Data Store.
- **ODBC string**. ODBC connection string to the Operational Data Store. If you install the PowerCenter client plug-in, the installer cannot verify the validity of the ODBC string.

Note: If you use a named Microsoft SQL Server database instance, you cannot connect to the database instance using the **Database URL** option. Use the **Custom Connection String** option.

For example:

```
jdbc:informatica:sqlserver://MYSQLSERVERCOMPUTERHOSTNAME
\MYDBINSTANCENAME;DatabaseName=MYDATABASENAME;
```

3. Enter values for the operational data store in the following fields:

Database username

Name of the database user account for the database.

Database user password

The password for the database account for the database. B2B Data Exchange stores the password as an encrypted string.

4. Press **Enter**.

The **User Authentication** section appears.

Step 5. Configure User Authentication

1. In the **User Authentication** section, choose the type of user authentication that you want to use.

Note: If you select an existing repository, the installer selects the existing authentication method.

- Choose Informatica domain authentication to manage user credentials in the Informatica domain and synchronize user information with B2B Data Exchange. Use Informatica domain authentication for production environments. For more information, see “Configure Settings for Informatica Domain Authentication” on page 52.

  Note: If your Informatica domain uses Kerberos authentication, choose the option **Informatica domain with Kerberos authentication**.
- Choose Informatica domain with Kerberos authentication if your Informatica domain uses Kerberos authentication. Use Informatica domain with Kerberos authentication for production environments. For more information, see “Configure Settings for Informatica Domain with Kerberos Authentication” on page 52.
- Choose **B2B Data Exchange native authentication** to manage user credentials locally in B2B Data Exchange. Use native authentication in development and staging environments. For more information, see “ Configure Settings for B2B Data Exchange Native Authentication ” on page 53.

2. Press **Enter**.

   The **Document Store** section appears.

Configure Settings for Informatica Domain Authentication

If you choose Informatica domain authentication, enter values in the following fields:

Gateway host

Host name of the Informatica security domain server. B2B Data Exchange stores the host name in the `pwc.domain.gateway` system property.

Gateway port

Port number for the Informatica security domain gateway. B2B Data Exchange stores the port number in the `pwc.domain.gateway` system property. Use the gateway HTTP port number to connect to the domain from the PowerCenter Client. You cannot use the HTTPS port number to connect to the domain.

Username

User name to access the Administrator tool. You must create the user in the Administrator tool and assign the **manage roles/groups/user** privilege to the user.

Password

Password of the Informatica security domain user.

Security domain

Name of the Informatica security domain where the user is defined.

Security group

Optional. Security group within the Informatica security domain where B2B Data Exchange users are defined in the following format:

```
<security group>@<domain>
```

If you leave the field empty, the Informatica security domain synchronizes only the B2B Data Exchange administrator user account.

B2B Data Exchange stores the security group in the dx.authentication.groups system property in the following format:

```
<group name>@<security group>[;<groupname>@<security group>]
```

Configure Settings for Informatica Domain with Kerberos Authentication

If you choose Informatica domain with Kerberos authentication, enter values in the following fields:

Kerberos configuration file

File that stores Keberos configuration information, usually named `krb5.conf`

The installation copies the file to the following location:

```
<DXInstallationDir>/shared/conf/security/krb5.conf
```

Operation Console SPN name

Service Principal Name (SPN) for the B2B Data Exchange Operation Console.

B2B Data Exchange stores the SPN in the `dx-security-config.properties` property file, in the dx.kerberos.console.service.principal.name property.

Operation Console keytab file

Location of the keytab file for the B2B Data Exchange Operation Console SPN.

The installation copies the file to the following location:

```
<DXInstallationDir>/shared/conf/security/HTTP_console.keytab
```

B2B Data Exchange stores the location of the keytab file in the `dx-security-config.properties` property file, in the dx.kerberos.console.keytab.file property.

If you change the property to point to a different file, you must enter the absolute path to the file using the following format:

```
file://<full_path>
```

System Administrator

B2B Data Exchange system administrator credentials.

Enter the credentials in the following format:

```
<username>@<SECURITY_DOMAIN>
```

Note: You must enter `<SECURITY_DOMAIN>` in uppercase letters.

Gateway host

PowerCenter domain gateway host.

Gateway port number

PowerCenter domain gateway port number.

Security group

Optional. Security group within the Informatica security domain where B2B Data Exchange users are defined in the following format:

```
<security group>@<domain>
```

If you leave the field empty, the Informatica security domain synchronizes only the B2B Data Exchange administrator user account.

B2B Data Exchange stores the security group in the dx.authentication.groups system property in the following format:

```
<group name>@<security group>[;<groupname>@<security group>]
```

Configure Settings for B2B Data Exchange Native Authentication

If you choose **B2B Data Exchange native authentication**, enter the B2B Data Exchange administrator user name. B2B Data Exchange uses this value for the user name and password when you log in to the Operation Console.

Step 6. Configure Document Store, Web Server, and Port Numbers

1. In the **Document Store** section, enter the directory where B2B Data Exchange stores documents and files during processing or accept the default directory, and then press `Enter`.

   The document store directory must be accessible to B2B Data Exchange, PowerCenter services, and Data Transformation.

2. Press **Enter**.

   The **Web Server** section appears.

3. Configure the Web Server connection.
   a. Enter the number for the network communication protocol or accept the default protocol:

      1- Enable HTTPS

      Instructs B2B Data Exchange to use secure network communication when you open the Operation Console in the browser.
      If you select HTTPS and HTTP, the Operation Console switches existing HTTP connections with HTTPS connections.

      2- Enable HTTP

      Instructs B2B Data Exchange to use regular HTTP network communication when you open the Operation Console in the browser.

   b. If you selected **Enable HTTPS**, enter values in the following fields:

      Connector port number

      Port number for the Tomcat connector to use when you open the Operation Console with HTTPS.
      The default value is 18443.

      Use a keystore file generated by the installer

      Instructs the installer to generate a keystore file with an unregistered certificate. If you select this option, ignore the security warning that you receive from the browser the first time you open the Operation Console.

      Use an existing keystore file

      Instructs the installer to load an existing keystore file. Enter values in the following fields:

      - Keystore password. Password for the keystore file.
      - Keystore file. Path to the keystore file.

      The keystore file must be in the Public Key Cryptography Standard (PKCS) #12 format.

   c. If you selected **Enable HTTP**, enter values in the following fields:

      HTTP connector port number

      Port number for the HTTP connector. If you clear this field, your browser must connect to the B2B Data Exchange server with HTTPS when you log in to the Operation Console.
      The default value is 18080.

      Server shutdown listener port number

      Port number for the listener that controls the Tomcat server shutdown.
      The default value is 18005.

4. Press **Enter**.

   The **Port Numbers** section appears.

5. Enter the port number for the B2B Data Exchange JMS Broker JMX listener port or accept the default port and then press **Enter**.

   If you selected to install the B2B Data Exchange PowerCenter server plug-in or the B2B Data Exchange PowerCenter Client plug-in components, the **PowerCenter Location** section appears. If you did not select the PowerCenter server or client components, the **PowerCenter Web Services Hub** section appears.

Step 7. Configure PowerCenter Settings

1. If you selected to install the B2B Data Exchange PowerCenter server plug-in or the B2B Data Exchange PowerCenter Client plug-in components, in the **PowerCenter Location** section, enter the directory where you installed PowerCenter or accept the default directory, and then press **Enter**.

   The **PowerCenter Web Services** section appears.
2. In the **PowerCenter Web Services** section, press **Enter** to accept the default URL or enter the URL that the PowerCenter Web Services Hub uses when B2B Data Exchange transfers documents to PowerCenter for processing with batch workflows and then press **Enter**.
3. Enter the name of the PowerCenter Repository Service, and then press **Enter**.
4. Enter values in the following fields:

   Node host name

   Host name of the node that runs the PowerCenter Repository Service.

   Node port number

   Port number of the node that runs the PowerCenter Repository Service.

   Username

   Name of the PowerCenter Repository Service user.

   Password

   Password for the PowerCenter Repository Service user. B2B Data Exchange stores the password as an encrypted string.

   Security domain

   Optional. Name of the Informatica security domain in which the PowerCenter Repository Service user is stored.
   Default is Native.
5. Press **Enter**.

   If you selected to install the B2B Data Exchange server plug-in for PowerCenter component, the **Informatica Domain** section appears. If you did not select the PowerCenter server component, the **PowerCenter pmrep Command Line Utility Location** section appears. Go to step 9.
6. Enter values in the following fields:

   Domain name

   Name of the Informatica domain that contains the PowerCenter Integration Service that runs B2B Data Exchange workflows.

   Node name

   Node in the Informatica domain on which the PowerCenter Integration Service runs.

   Domain administrator user name

   Name of the Informatica domain administrator.

   Domain administrator password

   Password for the Informatica domain administrator. B2B Data Exchange stores the password as an encrypted string.
7. Press **Enter**.
8. Enter the name of the PowerCenter Integration Service that B2B Data Exchange uses to run workflows, and then press **Enter**.

9. Enter the location of the pmrep command line utility and then press **Enter**. The location of the utility depends on whether or not you install B2B Data Exchange on the machine where the PowerCenter services are installed.

   Note: On Linux operating systems, pmrep must be executable.

Environment	Location of the pmrep command line utility
B2B Data Exchange installed on the machine where the PowerCenter services are installed	`<PowerCenter_services_installation_folder>/<PowerCenter_version>/tools/pcutils/<PowerCenter_version>`
B2B Data Exchange and PowerCenter services installed on different machines	`<PowerCenter_client_utility_directory>/PowerCenter/server/bin`

10. Press **Enter**.

    The **Pre-Installation Summary** section appears.

Step 8. Complete the Installation

1. In the **Pre-Installation Summary** section, verify that the installation information is correct, and then press **Enter**.

   During the installation process, the installer displays progress information.
2. If you installed the B2B Data Exchange PowerCenter server plug-in, follow the on-screen instructions to register the plug-in to the PowerCenter repository, and then press **Enter**.
3. To view the log files that the installer generates, navigate to the following directory:
   `<DXInstallationDir>\logs`
4. Perform the required post-installation tasks.

   For more information, see Chapter 5, “Post-Installation Tasks” on page 65.

   Note: Perform only the tasks that are relevant for your environment.
5. Optionally, perform additional configuration tasks. For more information, see Chapter 9, “Optional B2B Data Exchange Configuration” on page 115.

Installing B2B Data Exchange in a Silent Mode

To install B2B Data Exchange without user interaction, install in a silent mode. Use a properties file to specify the installation options. The installer reads the file to determine the installation options. You can use silent mode installation to install B2B Data Exchange on multiple machines on the network or to standardize the installation across machines.

Before you install, verify that your environment meets the minimum system requirements, perform the pre-installation tasks, and verify that the PowerCenter services are running.

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. Secure the passwords in the installation properties file.

Configuring the Installation Properties

The installation properties file includes the parameters that are required by the installer.

The following table describes parameters that you add in the installation properties file:

Parameter	Description
Specify whether to install or upgrade B2B Data Exchange.	
IS_INSTALL	To install B2B Data Exchange, set the parameter to 1.
IS_UPGRADE	To upgrade B2B Data Exchange, set the parameter to 1.
Configure PowerCenter version using the following parameters:	
PWC_VERSION	PowerCenter version you use.
PMREP_HOME_1	Location of the pmrep command line utility.
POWERCENTER_HOME_1	Directory where you installed PowerCenter.
Configure the installation directory using the following parameter:	
USER_INSTALL_DIR	Absolute path to the installation directory
Configure the components to install using the following parameters:	
DX_SERVER	To install the B2B Data Exchange application, set the parameter to 1.
DX_PARTNER_PORTAL	To install the B2B Data Exchange Partners Portal component, set the parameter to 1.
DX_DASHBOARD	To install the B2B Data Exchange Dashboard and Reports component, set the parameter to 1.
PC_SERVER_PLUGIN	To install the B2B Data Exchange plug-in for the PowerCenter services, set the parameter to 1.
PC_CLIENT_PLUGIN	To install the B2B Data Exchange plug-in for the PowerCenter client, set the parameter to 1.
MFT_COMPONENT	To install the Managed File Transfer component, set the parameter to 1.
WEBAPP_DASHBOARD_NAME_1	Name of the B2B Data Exchange Dashboard and Reports component.
WEBAPP_CONSOLE_NAME_1	Name of the B2B Data Exchange web console.
WEBAPP_PARTNER_PORTAL_NAME_1	Name of the B2B Data Exchange partners portal.
Configure the B2B Data Exchange repository using the following parameters:	

Parameter	Description
BLANK_USER	To create a new B2B Data Exchange repository, set the parameter to 1.
CONFIGURED_USER	To use an existing B2B Data Exchange repository, set the parameter to 1.
DB_TYPE_1	Type of database to use for the B2B Data Exchange metadata repository. Enter either of the following options: - Oracle - Microsoft SQL Server
DB_CONNECTION_STRING_1	To use a custom connection string, set the parameter to 1.
DB_HOST_1	Host name of the machine where the database server is installed.
DB_PORT_1	Port number for the database. The default port number for Oracle is 1521. The default port number for Microsoft SQL Server is 1433.
DB_SID_1	System identifier for the database if the database is Oracle. Enter a fully qualified Service Name or a fully qualified SID.
DB_CONNECTION_STRING_VALUE_1	The value of the connection string. Use one of the following connection strings: - JDBC connection string - ODBC connection string
DB_WINDOWS_AUTHENTICATION_1	To authenticate user names against the Microsoft Windows authentication mechanism, set the parameter to 1.
DB_USER_1	Name of the database user account for the database where you do not use Windows authentication.
DB_PASSWORD_1	Password for the database account for the database where you do not use Windows authentication. B2B Data Exchange stores the password as an encrypted string.
Configure the operational data store using the following parameters:	
ODS_DB_USE_NEW	To create an operational data store repository, set the parameter to 1.
ODS_DB_USE_EXISTING	To use an existing operational data store repository, set the parameter to 1.
ODS_DB_TYPE_1	Type of database to use for the operational data store. Enter one of the following options: - Oracle - Microsoft SQL Server
ODS_DB_CONNECTION_STRING_1	To use a custom connection string, set the parameter to 1.

Parameter	Description
ODS_DB_HOST_1	Host name of the machine where the database server is installed.
ODS_DB_PORT_1	Port number for the database. The default port number for an Oracle database is 1521. The default port number for a Microsoft SQL server is 1433.
ODS_DB_SID_1	System identifier for the database if you select Oracle as the database. Enter either a fully qualified Service Name or a fully qualified SID.
ODS_DB_JDBC_STRING_VALUE_1	The value of the connection string. You can enter values for either of following connection strings: - JDBC connection string - ODBC connection string
ODS_DB_WINDOWS_AUTHENTICATION_1	To authenticate user names against the Microsoft Windows authentication mechanism., set the parameter to 1.
ODS_DB_USER_1	Name of the database user account for the database where you do not use Windows authentication.
ODS_DB_PASSWORD_1	Password for the database account for the database where you do not use Windows authentication. B2B Data Exchange stores the password as an encrypted string.
Configure settings for Informatica Domain with Kerberos authentication using the following parameters:	
INTERNAL_AUTH	To use B2B Data Exchange native authentication, set the value to 1.
INTERNAL_AUTH_DEFAULT	To use the B2B Data Exchange native authentication as the default authentication, set the value to True.
ISF_AUTH	To use Informatica domain authentication, set the value to 1.
ISF_AUTH_DEFAULT=	To use the Informatica domain authentication as the default authentication, set the value to True.
KERBEROS_AUTH	To use Informatica domain with Kerberos authentication, set the value to 1.
KERBEROS_AUTH_DEFAULT	To use the Informatica domain with Kerberos authentication as the default authentication, set the value to True.
Configure settings for Informatica domain authentication using the following parameters:	
INFA_HOST_1	Host name of the Informatica security domain server.
INFA_PORT_1	Port number for the Informatica security domain gateway.
INFA_USERNAME_1	User name to access the Administrator tool.

Parameter	Description
INFA_PASSWORD_1	Password of the Informatica security domain user.
INFA_SECURITY_DOMAIN_1	Name of the Informatica security domain where the user is defined.
INFA_SECURITY_GROUP_1	Optional. Security group within the Informatica security domain where B2B Data Exchange users are defined in the following format: <security group>@<domain>
Configure B2B Data Exchange native authentication using the following parameter:	
CONSOLE_ADMIN_1	User name of the administrator account.
Configure the B2B Data Exchange document store using the following parameter:	
DATA_STORE_FOLDER_1	The directory where the B2B Data Exchange stores documents during processing.
Configure the Web Server using the following parameters:	
TOMCAT_ENABLE_HTTPS_1	To use the HTTPS secure network communication when you open the Operation Console in the browser, set the parameter to 1.
TOMCAT_HTTPS_PORT_1	The Port number for the Tomcat connector to use when you open the Operation Console with HTTPS. The default value is 18443.
TOMCAT_EXISTING_KEYSTORE_FILE_1	To use an existing keystore file, set the parameter to 1.
TOMCAT_KEYSTORE_PASSWORD_1	If you chose to use an existing keystore, enter the password for the keystore file.
TOMCAT_KEYSTORE_FILE_PATH_1	If you chose to use an existing keystore, enter the path to the keystore file.
TOMCAT_ENABLE_HTTP_1	To use the HTTP network communication when you open the Operation Console in the browser, set the parameter to 1.
TOMCAT_PORT_1	Port number for the HTTP connector.
TOMCAT_SERVER_LISTENER_PORT_1	Port number for the listener that controls the Tomcat server shutdown. The default value is 18005.
ACTIVEMQ_JMX_LISTENER_PORT_1	Port number for the B2B Data Exchange JMS Broker JMX listener port.
Configure the PowerCenter settings using the following parameters:	
POWERCENTER_HOME_1	PowerCenter installation directory.

Parameter	Description
PC_SCHEDULING_WORKFLOWS_1	To use the PowerCenter Web Services Hub when B2B Data Exchange transfers documents to PowerCenter for processing with batch workflows, set the parameter to 1.
PC_WEB_SERVICES_URL_1	URL that the PowerCenter Web Services Hub uses when B2B Data Exchange transfers documents to PowerCenter for processing with batch workflows.
PC_REPOSITORY_NAME_1	Name of the PowerCenter Repository Service.
PC_REPOSITORY_HOST_1	Host name of the node that runs the PowerCenter Repository Service.
PC_REPOSITORY_PORT_1	Port number of the node that runs the PowerCenter Repository Service.
PC_REPOSITORY_USER_1	Name of the PowerCenter Repository Service user.
PC_REPOSITORY_PASSWORD_1	Password for the PowerCenter Repository Service user. B2B Data Exchange stores the password as an encrypted string.
PC_REPOSITORY_SECURITY_DOMAIN_1	Optional. Name of the Informatica security domain in which the PowerCenter Repository Service user is stored. Default is Native.
PC_DOMAIN_NAME_1	Name of the Informatica domain that contains the PowerCenter Integration Service that runs B2B Data Exchange workflows.
PC_NODE_NAME_1	Node in the Informatica domain on which the PowerCenter Integration Service runs.
PC_ADMIN_USER_1	Name of the Informatica domain administrator.
PC_ADMIN_PASSWORD_1	Password for the Informatica domain administrator. B2B Data Exchange stores the password as an encrypted string.
PC_INTEGRATION_SERVICE_1	The name of the PowerCenter Integration Service that B2B Data Exchange uses to run workflows.
PMREP_HOME_1	The location of the pmrep command line utility.

Sample of the Installation Properties

Use the following sample to configure the installation properties file to install B2B Data Exchange in a silent mode:

```
#Install or Upgrade
#------------------
IS_INSTALL=1
IS_UPGRADE=0

#PowerCenter Version
#-------------------
PWC_VERSION=PWC_1020
```

```
PMREP_HOME_1=/data/akash/10.2.0/tools/pcutils/10.2.0
POWERCENTER_HOME_1=/data/akash/10.2.0

#Installation Directory
#----------------------
USER_INSTALL_DIR=/data/Diwakar/P_DX1023

#Installation Components
#-----------------------
DX_SERVER=1
DX_PARTNER_PORTAL=1
DX_DASHBOARD=1
PC_SERVER_PLUGIN=1
PC_CLIENT_PLUGIN=0
MFT_COMPONENT=0
WEBAPP_DASHBOARD_NAME_1=dx-dashboard
WEBAPP_CONSOLE_NAME_1=dx-console
WEBAPP_PARTNER_PORTAL_NAME_1=dx-portal
DIH_HADOOP_SERVICE=0
DIH_BIG_DATA_MANAGEMENT=0

#Metadata Repository
#-------------------
BLANK_USER=1
CONFIGURED_USER=0

#Metadata Repository Connection
#------------------------------
DB_TYPE_1=Oracle
DB_CONNECTION_STRING_1=0
DB_HOST_1=10.75.142.27
DB_PORT_1=1521
DB_SID_1=ORCL
DB_CONNECTION_STRING_VALUE_1=jdbc:informatica:oracle://10.75.142.27:1521;SID=ORCL;
DB_WINDOWS_AUTHENTICATION_1=0
DB_USER_1=C##BPK_DX1023_2
DB_PASSWORD_1=C##BPK_DX1023_2

#Operational Data Store
#----------------------
ODS_DB_USE_NEW=1
ODS_DB_USE_EXISTING=0

#Operational Data Store Database Connection
#------------------------------------------
ODS_DB_TYPE_1=Oracle
ODS_DB_CONNECTION_STRING_1=0
ODS_DB_HOST_1=10.75.142.27
ODS_DB_PORT_1=1521
ODS_DB_SID_1=orcl
ODS_DB_JDBC_STRING_VALUE_1=jdbc:informatica:oracle://10.75.142.27:1521;SID=orcl;
ODS_DB_WINDOWS_AUTHENTICATION_1=0
ODS_DB_USER_1=C##BPK_DX1023_2
ODS_DB_PASSWORD_1=C##BPK_DX1023_2

#User Authentication
#-------------------
INTERNAL_AUTH=1
INTERNAL_AUTH_DEFAULT=true
ISF_AUTH=0
ISF_AUTH_DEFAULT=false
KERBEROS_AUTH=0
KERBEROS_AUTH_DEFAULT=false

#Informatica Platform Authentication
#-----------------------------------
INFA_HOST_1=
INFA_PORT_1=
INFA_USERNAME_1=
INFA_PASSWORD_1=
INFA_SECURITY_DOMAIN_1=
```

```
INFA_SECURITY_GROUP_1=

#Operation Console Administrator
#-------------------------------
CONSOLE_ADMIN_1=Administrator

#Data Exchange Document Store
#----------------------------
DATA_STORE_FOLDER_1=/data/Diwakar/DX1023/DataExchange/dx-data

#Web Server
#----------
TOMCAT_ENABLE_HTTPS_1=1
TOMCAT_HTTPS_PORT_1=18443
TOMCAT_EXISTING_KEYSTORE_FILE_1=0
TOMCAT_KEYSTORE_PASSWORD_1=
TOMCAT_KEYSTORE_FILE_PATH_1=
TOMCAT_ENABLE_HTTP_1=1
TOMCAT_PORT_1=18080
TOMCAT_SERVER_LISTENER_PORT_1=18005

#Port Number
#-----------
ACTIVEMQ_JMX_LISTENER_PORT_1=18098

#PowerCenter Location
#--------------------
POWERCENTER_HOME_1=/data/akash/10.2.0

#PowerCenter Web Services Hub
#----------------------------
PC_SCHEDULING_WORKFLOWS_1=1
PC_WEB_SERVICES_URL_1=http://localhost:7333/wsh/services/BatchServices/DataIntegration
PC_REPOSITORY_NAME_1=PCRS
PC_REPOSITORY_HOST_1=localhost
PC_REPOSITORY_PORT_1=6005
PC_REPOSITORY_USER_1=Administrator
PC_REPOSITORY_PASSWORD_1=Administrator
PC_REPOSITORY_SECURITY_DOMAIN_1=

#PowerCenter Domain Settings
#---------------------------
PC_DOMAIN_NAME_1=Domain
PC_NODE_NAME_1=node01
PC_ADMIN_USER_1=Administrator
PC_ADMIN_PASSWORD_1=Administrator
PC_INTEGRATION_SERVICE_1=PCIS

#PowerCenter pmrep Command Line Utility Location
#-----------------------------------------------
PMREP_HOME_1=/data/akash/10.2.0/tools/pcutils/10.2.0
```

Running the Silent Installer

Before you run the installer in the silent mode, ensure that you configure the installer configuration file:

1. Configure the installer properties in a text file.

   Note:

   - For more information about parameters to configure in the installer properties file, refer to "Configuring the Installation Properties" on page 57.
   - For using a sample of the installer properties file, refer to "Sample of the Installation Properties" on page 61.

2. Run the following command in the command prompt to silent install B2B Data Exchange using the installer properties file:

- If you use the Windows operating system, run the following command:
  Install.exe -f <filename> -i silent, where filename is the name of the file that contains the installer properties.
- If you are using the UNIX operating system, run the following command: ./Install.bin -f <location>/installer.properties -i silent, where location is the location of the file that contains the installer properties. For example, /data/username/installers/1023/MFT/installer.properties.

The silent installer runs in the background.

The silent installation fails if you incorrectly configure the properties file or if the installation directory is not accessible. View the installation log files and correct the errors. Then run the silent installation again.

CHAPTER 5

Post-Installation Tasks

This chapter includes the following topics:

Post-Installation Tasks Overview

After you install B2B Data Exchange, perform the steps that are relevant for your environment.

1. Configure authentication for the B2B Data Exchange Operation Console.
2. If you installed the B2B Data Exchange server plug-in for PowerCenter, register the plug-in to the PowerCenter repository.
3. Configure PowerCenter to access B2B Data Exchange.
4. If you do not have the Informatica services installed on the same machine as B2B Data Exchange, configure B2B Data Exchange to connect to a remote Informatica domain.
5. If you want to use web services, set up the web services.
6. If you installed the B2B Data Exchange repositories on a Microsoft SQL Server and you selected to use Windows authentication, configure credentials for Windows authentication.
7. Configure the mail server for B2B Data Exchange monitoring notifications.
8. Set the environment variable `JRE_HOME` to `<DIH_HOME>/DataIntegrationHub/jdk1.8/jre`, if you installed B2B Data Exchange on SUSE Linux operating system.
9. Start the B2B Data Exchange services. For more information, see Chapter 8, “Starting and Stopping B2B Data Exchange” on page 113.
10. Log in to the B2B Data Exchange Operation Console.

11. Configure connections to the B2B Data Exchange repositories in the B2B Data Exchange Operation Console.
12. If you installed B2B Data Exchange repositories on Microsoft Azure SQL databases, configure connections to the Microsoft Azure SQL databases.
13. If you installed B2B Data Exchange with Informatica domain authentication or with Informatica domain with Kerberos authentication, synchronize B2B Data Exchange users in the B2B Data Exchange Operation Console.
14. If you installed the Dashboard and Reports component, activate the component.
15. If you installed the Partners Portal component, you can brand the portal with your organization logo.

Related Topics:

- "Overview of Starting and Stopping B2B Data Exchange" on page 113

Configure Authentication for the Operation Console

When you install B2B Data Exchange, you choose native authentication or Informatica domain authentication.

If you choose native authentication, use the administrator user name you entered in the Operation Console Administrator screen to log in to the Operation Console. If you choose Informatica domain authentication, use the user name and password you entered in the **Informatica Platform Authentication** screen to log in to the Operation Console.

If you use B2B Data Exchange native authentication with an authentication protocol that the Informatica domain authentication does not support, you can create a JAAS login module to enable authentication for users that log in to the Operation Console. You configure the connection between the Operation Console and the JAAS login module. The login module must support storing the user principal in the JAAS shared state.

Configure a JAAS Module for the Operation Console

If you use B2B Data Exchange native authentication, you can create a JAAS login module to connect to the authentication server before you configure authentication to the Operation Console.

For more information about the JAAS login module, browse to the following websites:

```
http://download.oracle.com/javase/6/docs/technotes/guides/security/jaas
/JAASRefGuide.html
http://download.oracle.com/javase/6/docs/technotes/guides/security/jaas
/JAASLMDevGuide.html
```

1. After you create the JAAS login module, copy the JAR file to the following directory:

   ```
   <DXInstallationDir>/DataExchange/tomcat/shared/lib
   ```

2. Go to the home directory of the user account that runs the instance of Apache Tomcat in B2B Data Exchange and locate the file named dx-console.login.config.

   On Windows 7, the default user home directory is `C:\Username`. On Windows XP the default user home directory is *C:\Documents and Settings\UserName*. On UNIX systems, the default user home directory is `/home/UserName`. If the file does not exist, create a text file with the name `dx-security.login.config` in the following directory: `<DXInstallationDir>/DataExchange/tomcat/shared/classes`

3. Add the following lines of code to the file and specify the class name of the JAAS module and any options required:

```
DX-SECURITY {
<Class_Name_of_Login_Module> REQUISITE;
};
```

4. Save the file.

Register the B2B Data Exchange Server Plug-in for PowerCenter

If you installed the B2B Data Exchange server plug-in for PowerCenter, register the plug-in to the PowerCenter repository where you create B2B Data Exchange workflows. If you do not register the plug-in, you cannot create B2B Data Exchange transformations in the PowerCenter Designer, and B2B Data Exchange cannot run PowerCenter workflows. Under these conditions, when B2B Data Exchange attempts to run a PowerCenter workflow and fails, B2B Data Exchange logs the following error in the PowerCenter workflow session log:
`[REP_12400 Repository Error ([REP_57140] Object does not exist).`

The PowerCenter Repository Service must be running in exclusive mode when you register the plug-in. After the registration, restart the PowerCenter Repository Service in normal mode.

1. Log in to the Administration tool.
2. In the Navigator, select the Repository Service for which you want to register the plug-in.
3. On the Properties tab, edit the General Properties section and set the operating mode to Exclusive.
4. Restart the Repository Service.
5. After the Repository Service restarts, click the Plug-ins tab.
6. Click the link to register a Repository Service plug-in.
7. On the Register Plug-in for <Repository Service> page, click the **Browse** button to find the plug-in file.

   Select the following file in the directory where you installed the B2B Data Exchange server plug-in for PowerCenter:

   `<DXInstallationDir>/powercenter/plugin`*`VERSION`*`/dxplugin.xml`

   Note: The B2B Data Exchange installer creates separate plug-in folders for each PowerCenter version. Make sure to select the plug-in folder for the PowerCenter version that you are using.
8. Enter the Repository Service administrator user name and password to log in to the repository.

   If the security group field appears, select the security group for the Repository Service administrator.
9. Click **OK**.

   The Repository Service registers the plug-in. Verify that the list of registered plug-ins for the Repository Service includes the B2B Data Exchange transformations.
10. On the Properties tab, edit the General Properties section and set the operating mode to Normal.
11. Restart the PowerCenter Integration Service.

Connect to a Remote Informatica Domain

If you do not have the Informatica services installed on the same machine as B2B Data Exchange, you can configure B2B Data Exchange to connect to a remote Informatica domain.

Verify that you can access the machine that hosts B2B Data Exchange from the machine hosting the Informatica services.

Perform the following tasks to connect to a remote Informatica domain:

- Modify the B2B Data Exchange configuration files to explicitly use the host name of the machine where B2B Data Exchange is installed.
- Configure the remote domain to access B2B Data Exchange.
- Update the Java security file to allow remote access to B2B Data Exchange.

Modify the B2B Data Exchange Host Name

Replace the default host name for the Operation Console with the actual name of the machine that hosts B2B Data Exchange.

Modify the host name information in the following files:

```
<DXInstallationDir>/conf/dx-configuration.properties
<DXInstallationDir>/DataExchange/tomcat/shared/classes/dx-configuration.properties
```

Back up the files before you update them.

1. Go to the following directory and locate the file named dx-configuration.properties:

   ```
   <DXInstallationDir>/conf/
   ```

2. Use a text editor to open the file.
3. Search for the following text:

   ```
   dx.rmi.host=localhost
   ```

4. Replace **localhost** with the host name of the machine that hosts B2B Data Exchange.

   ```
   dx.rmi.host=DXHostName
   ```

5. Save the dx-configuration.properties file.

   B2B Data Exchange maintains two copies of the dx-configuration.properties. The contents of the files must be identical.

6. Copy the updated dx-configuration.properties file to the following directory:

   ```
   <DXInstallationDir>/DataExchange/tomcat/shared/classes/
   ```

Configuring a PowerCenter Integration Service to Access B2B Data Exchange

During the B2B Data Exchange installation or upgrade, you define a PowerCenter Integration Service that B2B Data Exchange uses to run workflows. If required, you can configure a different PowerCenter Integration Service to access B2B Data Exchange.

In the Java classpath for the PowerCenter Integration Service, add the path to the B2B Data Exchange class files.

1. Log in to the Administrator tool and select the PowerCenter Integration Service that runs the workflows for B2B Data Exchange.

2. On the **Processes** tab, edit the Java SDK ClassPath property and add the location of the B2B Data Exchange Java classes at the beginning of the ClassPath property:

```
<DXInstallationDir>/powercenter/lib/dx-client-powercenter-10.2.3.jar;
<DXInstallationDir>/powercenter/lib/commons-logging-1.1.3.jar;
<DXInstallationDir>/powercenter/lib/log4j-1.2.17.jar;
<DXInstallationDir>/powercenter/lib/activemq-all-5.12.1.1.jar
```

Note: You can reference the libraries if the you can access the `<DXInstallationDir>` from PowerCenter, or you can copy the library files locally.

3. Add environment variables to the B2B Data Exchange console and server integration services.

Integration Service	Environment Variable
DX_CONSOLE_URL	`rmi://<HostName>:<dx.tpm.rmi.port>`
DX_SERVER_URL	`rmi://<HostName>:<dx.rmi.port>`

You can find the RMI port numbers for the console and server in the following location:

```
<DXInstallationDir>\conf\dx-configuration.properties
```

By default:

- `dx.tpm.rmi.port`: 18096
- `dx.rmi.port`: 18095

4. Save the changes.

Configure Remote Access to B2B Data Exchange

Update the Java security file in PowerCenter to enable remote access to B2B Data Exchange.

1. Go to the PowerCenter installation directory on the remote machine and locate the files named java.policy and javaws.policy in the following directory:

```
<PowerCenterInstallationDirectory>\java\jre\lib\security
```

2. Back up the files before you modify them.
3. Use a text editor to open the java.policy and the javaws.policy files.
4. Search for the following text:

```
permission java.security.AllPermission;
```

If you do not find the text, add it to the list of permissions. To add to the list of permissions, add the permission to the end of the grant command before the closing bracket:

```
permission java.security.AllPermission;
```

5. If you modify the java.policy or the javaws.policy files, save the files.

Set Up the B2B Data Exchange Web Services

If you want to use web services, import the web service workflows into PowerCenter.

If the PowerCenter services and the B2B Data Exchange server run on separate machines, verify that the settings for the B2B Data Exchange server are set correctly.

Importing the Web Services to PowerCenter

When you install B2B Data Exchange, the B2B Data Exchange web services workflows are installed in the `<DX_INSTALLATION_DIR>/powercenter/webservices` folder. You must import the B2B Data Exchange web service workflows into PowerCenter before you can access the web services.

To use the web services, the Informatica domain must contain the following services:

- PowerCenter Repository Service
- Web Services Hub
- PowerCenter Integration Service

1. Use the PowerCenter Repository Manager to import the following workflow files into the PowerCenter repository:
   - `wf_m_DX_WS_TPM.XML`. Contains the workflows for the DX_TPM_Partner, DX_TPM_Account, and DX_TPM_Profile web services.
   - `wf_m_DX_WS_Endpoint.XML`. Contains the workflow for the DX_Endpoint web service.
2. In the Web Services Hub console, verify that the B2B Data Exchange web services are correctly imported into PowerCenter. If the import process is successful, the list of valid services includes the B2B Data Exchange web services.
3. You can use the Try-It application in the Web Services Hub console to test the B2B Data Exchange web services. On the **XML Input** tab, enter the data into the SOAP message and click **Send**. To avoid authentication errors, do not use the **Form Input** page to test a B2B Data Exchange web service.

   After you verify that the web services are working, you can create a client application to send requests to the web services.

Verifying the Server Settings

If the PowerCenter services and the B2B Data Exchange server run on separate machines, verify that the settings for the B2B Data Exchange server and Operation Console are set correctly.

In the Informatica Administrator, select the PowerCenter Integration Service that runs B2B Data Exchange workflows. Verify the following environment variable settings:

Environment Variable	Value
DX_SERVER_URL	The RMI URL for B2B Data Exchange server. For example: `rmi://<DXServerHostname>:<RMIPort>/TSSARuntime` **Note:** <RMIPort> must match the *dx.rmi.port* parameter in the `dx-configuration.properties` file. The default port number is 18095.
DX_CONSOLE_URL	The RMI URL for the B2B Data Exchange Operation Console. For example: `rmi://<DXServerHostname>:<RMIPort>/PartnerManagementService` **Note:** <RMIPort> must match the *dx.tpm.rmi.port* parameter in the `dx-configuration.properties` file. The default port number is 18096.

Configure Credentials for Windows Authentication

If you installed any of the B2B Data Exchange repositories on a Microsoft SQL Server and you selected to use Windows authentication, configure the credentials that B2B Data Exchange uses to access the Microsoft SQL Server instance.

Before you start the configuration process, verify that all B2B Data Exchange Windows services are stopped and that the B2B Data Exchange Operation Console and the B2B Data Exchange server are not running.

1. Access the Windows **Services** window.
2. Double-click the service **Informatica B2B Data Exchange Server *version***.

   The B2B Data Exchange Server Properties window appears.
3. Select the **Log On** tab.
4. Select **This account**, click **Browse**, and then specify a user account in the **Select User** dialog box. When you are finished, click **OK**.
5. Type the password for the user account in **Password** and in **Confirm password**, and then click **OK.**
6. Repeat steps 2 through 5 for the service **Informatica B2B Data Exchange Console *version***.

Log in to the Operation Console

You log in to the Operation Console with the administrator user account that you defined during installation.

If you use Informatica platform authentication, verify that all user accounts and user passwords exist on the authentication server.

1. Make sure that the Operation Console service is running.
2. Access the Operation Console login page.
   - On Microsoft Windows or UNIX operating systems, open a browser window and enter the URL for the Operation Console in one of the following formats:

     ```
     HTTP: http://<HostName>:<HTTPPortNumber>/
     HTTPS: https://<HostName>:<HTTPSPortNumber>/
     ```
   - On Microsoft Windows operating systems, click the Desktop shortcut to open a new browser window to the Operation Console URL.
3. Enter your user name and password and click **Log In**.

Configure the Mail Server

When you set up an event monitor in the Operation Console, you can specify that the B2B Data Exchange server sends email notifications to users in the organization when the conditions of the monitor are met, such as when an error occurs. You must configure a mail server to send email notifications.

Note: To invite partners to use the Partners Portal, you must set up the mail server.

To configure a mail server, edit the following B2B Data Exchange system properties:

System Property	Edit
dx.smtp.server	Replace **localhost** with the host name of the mail server.
dx_email_from_field	Replace the sample email address **noreply@example.com** with the return address for the email notification.
dx.smtp.port	Replace the default port **25** with the port of the mail server.
dx.smtp.login	Enter the user name for the mail server.
dx.smtp.password	Enter the password for the mail server. B2B Data Exchange stores the password as an encrypted string.
dx.smtp.ssl	If you use ssl (SMTPS) replace the default value **false** with **true**.

Activate the Dashboard and Reports Component

If you installed the Dashboard and Reports component, perform the following tasks to activate the component:

- Register the license of the Dashboard and Reports component.
- Import the operational data store event loader to PowerCenter.

Register the Dashboard and Reports License

Register the license of the B2B Data Exchange Dashboard and Reports component.

1. Contact Informatica Global Customer Support to receive the Logi Info Dashboard license files.
2. Start the B2B Data Exchange services.
3. Move the file `_Settings.lgx` from the following location:

   ```
   <DXInstallationDir>\DataExchange\tomcat\webapps\dx-dashboard\_Definitions
   ```

   To the following location:

   ```
   <DXInstallationDir>\DataExchange\tomcat\shared\classes
   ```

   Rename the file to the following name:

   ```
   dx_dashboard_configuration.xml
   ```
4. Copy the Logi Info Dashboard license file `_Settings_encrypted.lgx` to the following location:

   ```
   <DXInstallationDir>\DataExchange\tomcat\webapps\dx-dashboard\_Definitions
   ```
5. Rename the file `_Settings_encrypted.lgx` to `_Settings.lgx`.
6. Restart the B2B Data Exchange services.

To customize and enhance the Dashboard, the B2B Data Exchange developer installs and registers Logi Info Studio. For more information and installation instructions, see the *B2B Data Exchange Developer Guide*.

If the IP addresses of the machine that hosts B2B Data Exchange change any time after the installation, you must update the IP addresses in the Logi Info Dashboard license file. For more information, see "Updating the Dashboard Configuration File" on page 124.

Import the Operational Data Store Event Loader Workflow to PowerCenter

Import the operational data store (ODS) event loader workflow to load event information from the B2B Data Exchange repository to the B2B Data Exchange ODS.

If you use an existing workflow with the name DX_ETL, rename the existing workflow in PowerCenter Repository Manager before you import the ODS event loader workflow, or import the workflow to a different folder.
Note: After you import the ODS event loader workflow, do not run the workflow manually. The workflow must start at the scheduled time. If you start the workflow manually it might fail to store aggregated events in the B2B Data Exchange ODS.

1. In the PowerCenter Workflow Manager, select **Connections** > **Relational**.
2. Add the **DX_REPO** connection for the B2B Data Exchange repository.
3. Add the **DX_ODS** connection for the B2B Data Exchange ODS.
4. In the PowerCenter Repository Manager, import the B2B Data Exchange ODS workflow file. The name of the workflow file depends on type of database on which the ODS is installed.

Database Type	Workflow Location and Name
Oracle	<DXInstallationDir>\powercenter\ETL\DX_ETL.xml
Microsoft SQL Server	<DXInstallationDir>\powercenter\ETL\DX_ETL_SQLSERVER.xml

5. In the PowerCenter Workflow Manager, connect to the PowerCenter repository.
6. If B2B Data Exchange was previously installed at your site, and you want to exclude old events from the dashboard reports, instruct the workflow to load only events that finished processing after a specific date and time. Click **Workflow** > **Edit** > **Variables** and change the value of the **$$WF_Last_Load_End_Time** variable.

   Note: Do not change the variable after the first time the workflow runs.
7. By default, the workflow runs every 15 minutes. You can schedule the workflow start time.
8. Right-click the PowerCenter Integration Service that you want to assign to the ODS event loader workflow and select **Assign to Workflows**.

   The **Assign Integration Service** dialog box appears.
9. Select the **DX_ETL** check box and then click **Assign**.

   PowerCenter assigns the Data Integration Service to the ODS event loader workflow.

Synchronize B2B Data Exchange Users

If you installed B2B Data Exchange with Informatica domain authentication or with Informatica domain with Kerberos authentication, synchronize B2B Data Exchange users in the B2B Data Exchange Operation Console.

1. In the Navigator, click **Administration** > **Users**.

   The **Users** page appears.
2. Click **Synchronize users** and follow the instructions on the screen.

3. For each user that is added to the **Users** page, assign the required privileges. For more information see the *B2B Data Exchange Administrator Guide*.

Customize the Partners Portal Logo

If you installed the Partners Portal component, you can brand the Partners Portal with the organization logo.

The Partners Portal requires two logo graphic files in .png format, a small logo and a large logo. The file for the small logo must be named `Organization_logo.png` and must be 144 pixels by 50 pixels. The file for the large logo must be named `Login_Organization_logo.png` and must be 170 pixels by 100 pixels. The logo graphics must be transparent.

1. Copy the `Login_Organization_logo.png` file to the following directory: `dx\tomcat\webapps\dx-portal\img\Login_Organization_logo.png`.

   This logo appears in the upper right corner of the Partners Portal login page.

2. Copy the `Organization_logo.png` file to the following directory: `dx\tomcat\webapps\dx-portal\img\Organization_logo.png`.

   This logo appears in the upper right corner of the Partners Portal tabs.

CHAPTER 6

Installing the Partners Portal on Non-B2B Data Exchange Nodes

This chapter includes the following topics:

Installing the Partners Portal on Non-B2B Data Exchange Nodes Overview

You can install the Partners Portal in your organization on a different node than the B2B Data Exchange node.

You can install the Partners Portal on Windows and UNIX operating systems. On Windows, run the B2B Data Exchange installer in graphical mode. On UNIX, run the B2B Data Exchange installer in console mode. When you run the installer, you must select only the **B2B Data Exchange Partners Portal** component.

Before you install, verify that your environment meets the installation requirements.

Verify the Minimum System Requirements

Verify that your system meets the minimum requirements.

The following table describes the minimum system requirements:

System	Requirement
Operating system	- Microsoft Windows - IBM AIX - Sun Solaris - Red Hat Linux - SUSE Linux
Processor	2 CPU cores

System	Requirement
RAM	2 GB for the B2B Data Exchange Partners Portal
Disk space	3 GB
Browser	- Microsoft Internet Explorer - Google Chrome

The following table describes the minimum system requirements to run the installer:

System	Requirement
Operating system	X Window server if you run the installer on a UNIX operating system in graphical mode.
RAM	512 MB
Disk space	1 GB

For more information about product requirements and supported platforms, see the Product Availability Matrix on the Informatica My Support Portal: https://mysupport.informatica.com/community/my-support/product-availability-matrices

Installation Process

The Partners Portal installation process consists of the following tasks:

1. Install the Partners Portal.
   Run the installer in graphical mode or in console mode to install the Partners Portal.
2. Optionally, configure the Partners Portal logo.

Installing the Partners Portal on Non-B2B Data Exchange Nodes Requirements

Before you install the Partners Portal, set up the node to run the installer. If you plan to brand the portal with your organization logo, follow the logo branding guidelines.

Partners Portal node

Follow these guidelines to set up the node where you plan to install the Partners Portal:

- B2B Data Exchange must be installed in the network.
- B2B Data Exchange and the Partners Portal must be deployed on the same operating system type.
- The Partners Portal requires file system level access to the B2B Data Exchange Document Store.
- Open HTTP or HTTPS ports from the external network to the node where you plan to install the Partners Portal. Configure the firewall to allow URLs that start with the suffix `/dx-portal` or `/dx-portal-help`.

Logo branding

Follow these guidelines if you plan to brand the Partners Portal with the organization logo:

- The Partners Portal requires two graphic files for a small logo and a large logo in .png format.
- The file for the small logo must be named `Organization_logo.png` and must be 144 pixels by 50 pixels.
- The file for the large logo must be named `Login_Organization_logo.png` and must be 170 pixels by 100 pixels.
- The logo graphics must be transparent.

Step 1. Install the Partners Portal

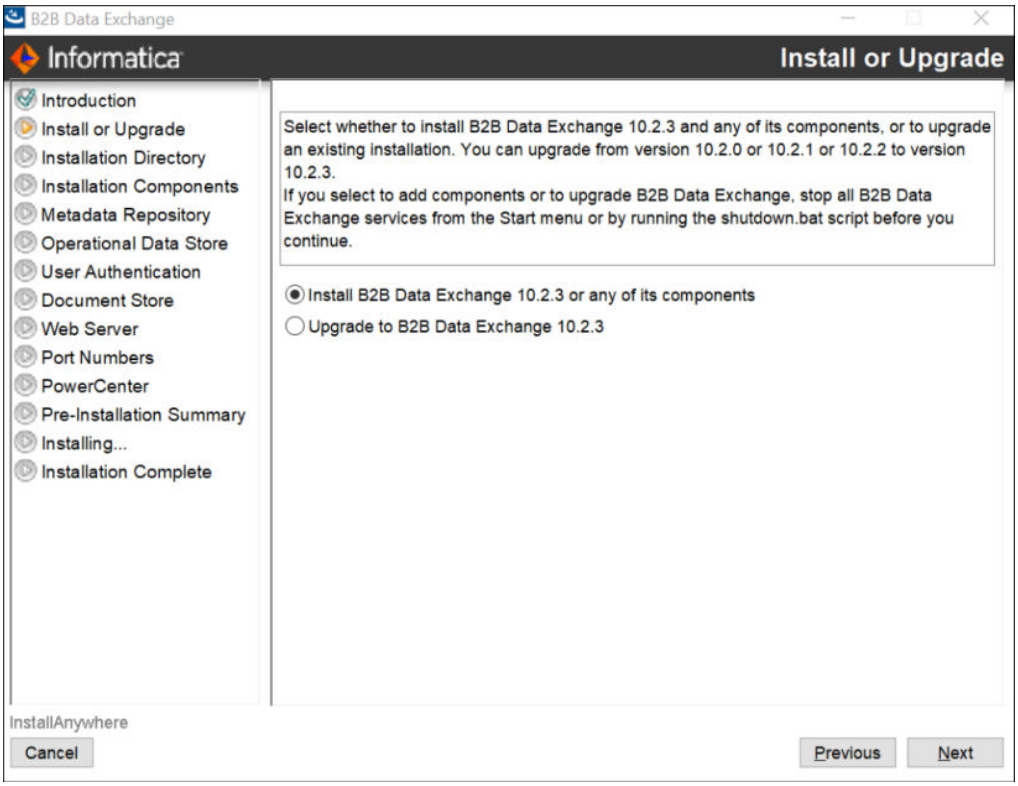
Based your operating system, install the Partners Portal in graphical mode or in console mode.

Installing the Partners Portal on Windows in Graphical Mode

1. Log in to the machine with the user account that you want to use to install the Partners Portal.
2. Close all other applications.
3. Run the `Install.exe` installer file from the directory where you downloaded the installer.

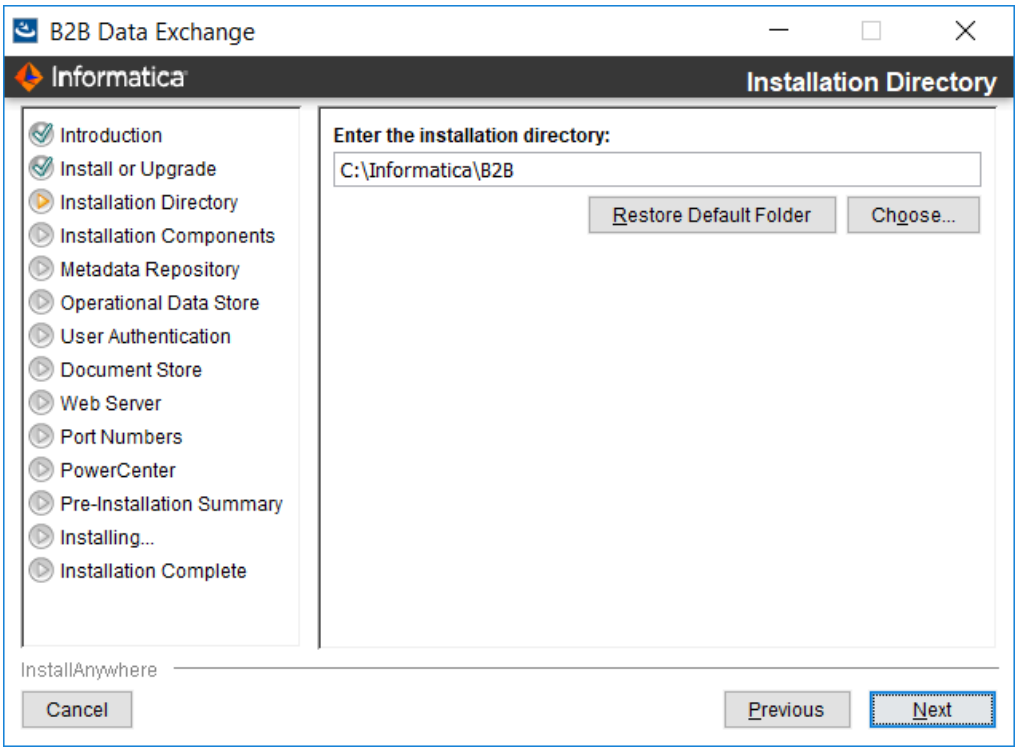
   The **Introduction** page appears.
4. Read the instructions, and then click **Next**.

The **Install or Upgrade** page appears.



5. Select the option to install B2B Data Exchange, and then click **Next**.

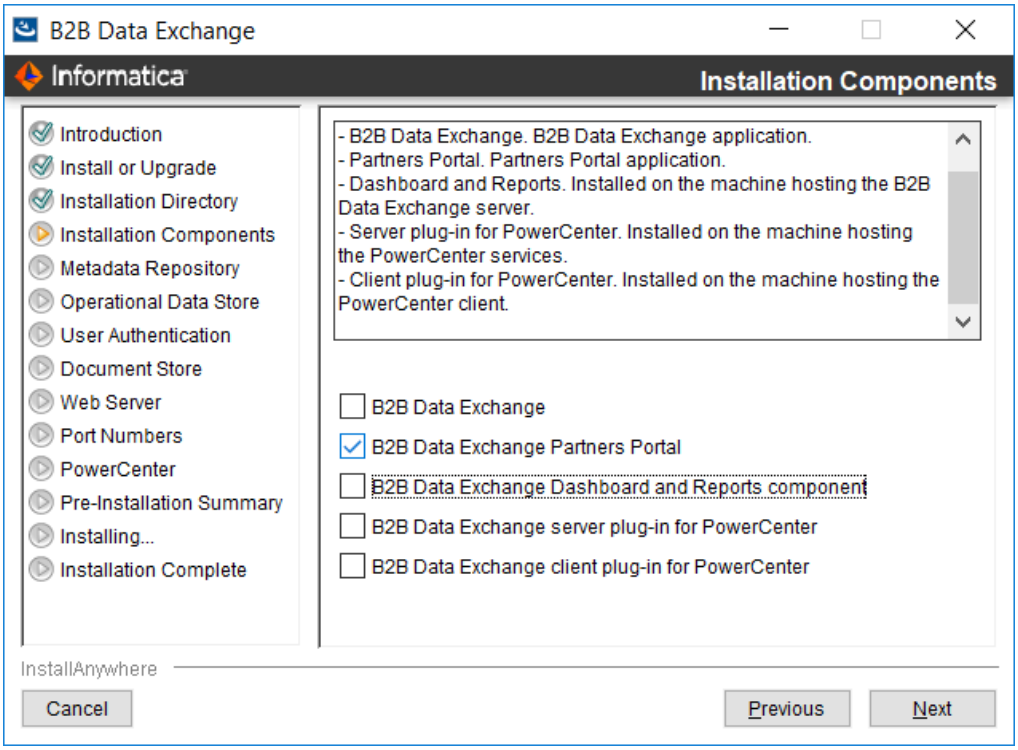
   The **Installation Directory** page appears.



6. Enter the absolute path to the installation directory or accept the default directory.

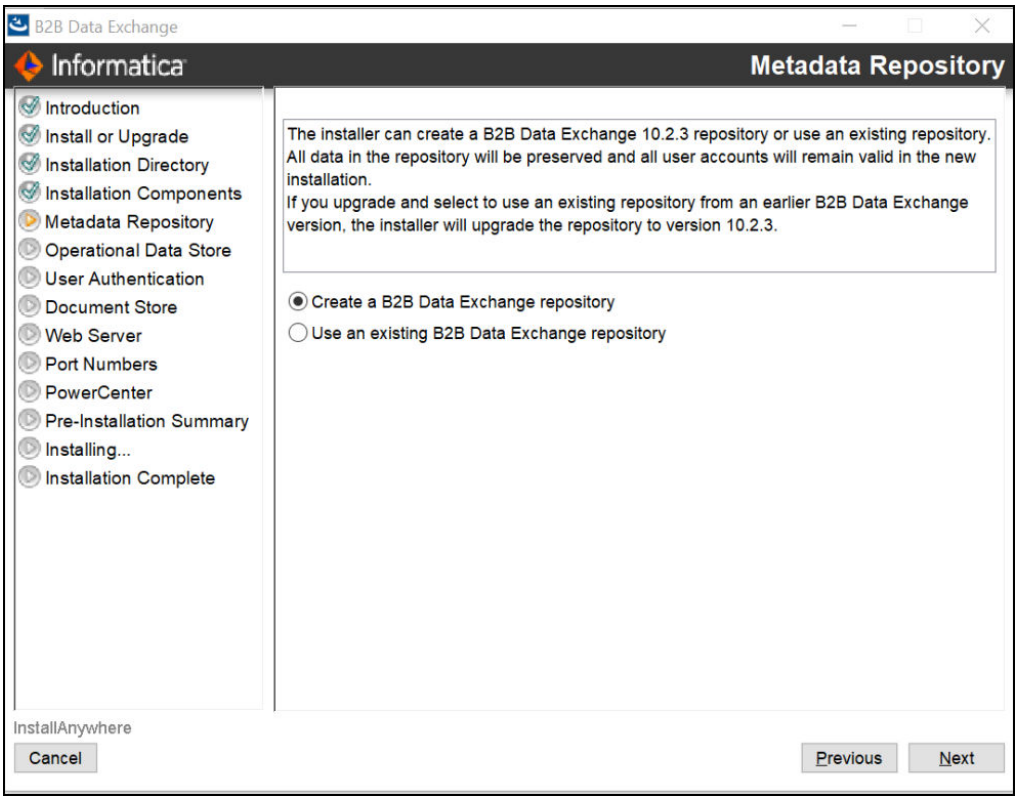
7. Click **Next**.

   The **Installation Components** page appears.



8. Select **B2B Data Exchange Partners Portal**, and then click **Next**.

The **Metadata Repository Connection** page appears.



Select to use an existing repository.

9. Enter values in the following fields:

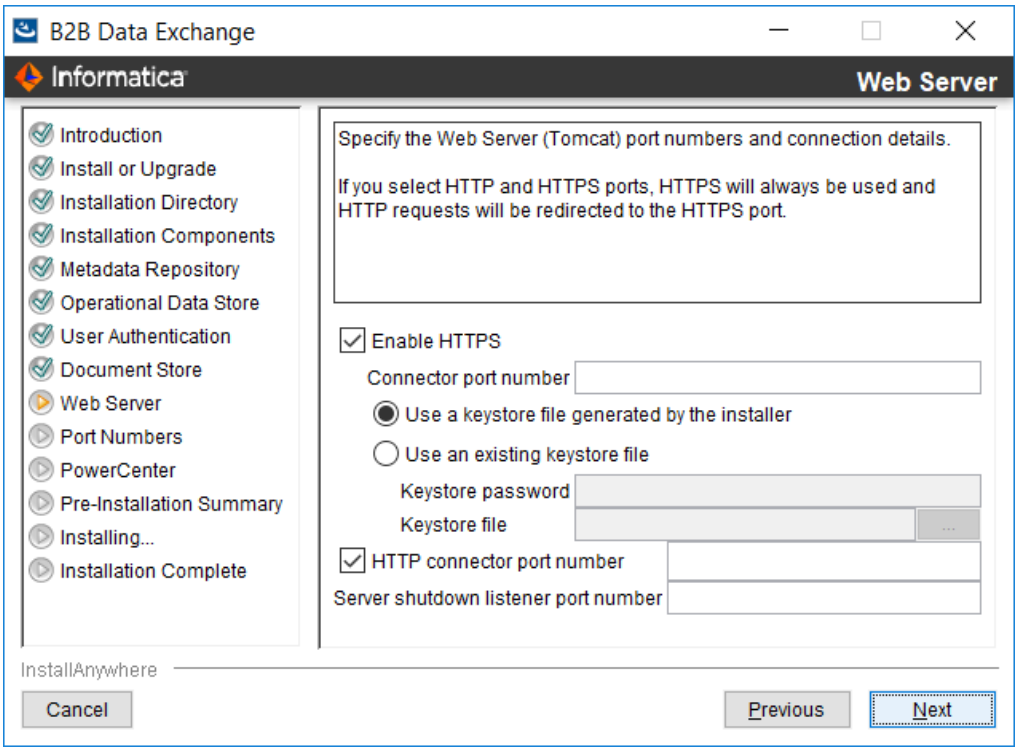
Field	Description
Database type	Type of database to use for the B2B Data Exchange metadata repository. You can choose one of the following options: - Oracle - Microsoft SQL Server
Database URL	Location of the database. If you select this option, enter the values in the following fields: - Database host name. Host name of the machine where the database server is installed. - Database port. Port number for the database. The default port number for Oracle is 1521. The default port number for Microsoft SQL Server is 1433. - Oracle database. Database SID. System identifier for the database. Enter either a fully qualified ServiceName or a fully qualified SID. **Note:** It is recommended that you enter a ServiceName in this field. - Microsoft SQL Server database. Database name.

Field	Description
Custom Connection String	Connection string to the database. If you select this option, enter values in one of the following fields: - JDBC string. JDBC connection string to the metadata repository. - ODBC string. ODBC connection string to the metadata repository. Available if you install the PowerCenter Client plug-in. The installer cannot verify the validity of the ODBC string. **Note:** If you use a named Microsoft SQL Server database instance, you must specify a custom connection string. You cannot connect to the database instance with a database URL. For example, `jdbc:informatica:sqlserver://MYSQLSERVERCOMPUTERHOSTNAME \MYDBINSTANCENAME;DatabaseName=MYDATABASENAME;`
Microsoft SQL Server database: Use Windows Authentication	Instructs B2B Data Exchange to authenticate user names against the Microsoft Windows authentication mechanism. Available when you select a Microsoft SQL Server database.
Oracle database or Microsoft SQL Server database where you do not use Windows authentication: Database username	Name of the database user account.
Oracle database or Microsoft SQL Server database where you do not use Windows authentication: Database user password	Password for the database account. B2B Data Exchange stores the password as an encrypted string.

Note: The values that you enter here must be identical to the values that you entered in this page during B2B Data Exchange installation.

10. Click **Next**.

The **Web Server** page appears.



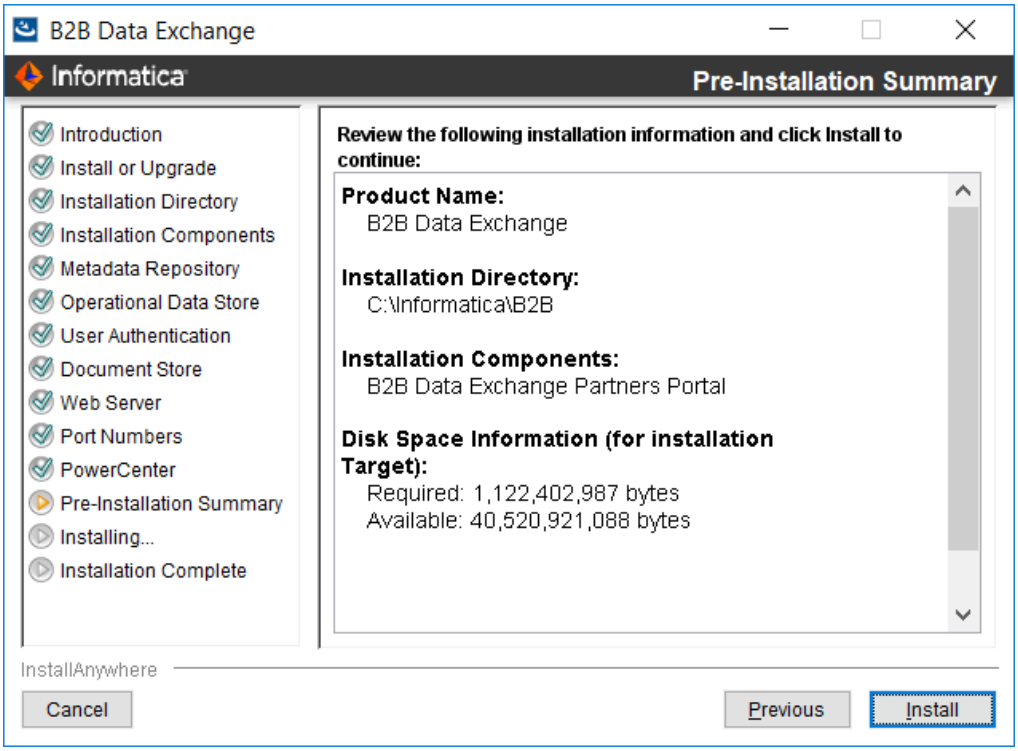
11. Enter values in the following fields:

Field	Description
Enable HTTPS	Instructs B2B Data Exchange to use secure network communication when you open the Operation Console in the browser. If you select HTTPS and HTTP, the Operation Console switches existing HTTP connections with HTTPS connections.
Connector port number	Port number for the Tomcat connector to use when you open the Partners Portal or Operation Console with HTTPS. The default value is 18443.
Use a keystore file generated by the installer	Instructs the installer to generate a keystore file with an unregistered certificate. If you select this option, ignore the security warning that you receive from the browser the first time you open the Operation Console.
Use an existing keystore file	Instructs the installer to load an existing keystore file. Enter values in the following fields: - Keystore password. Password for the keystore file. - Keystore file. Path to the keystore file. The keystore file must be in the Public Key Cryptography Standard (PKCS) #12 format.

Field	Description
HTTP connector port number	Port number for the HTTP connector. If you clear this field, your browser must connect to the B2B Data Exchange server with HTTPS when you log in to the Operation Console. The default value is 18080.
Server shutdown listener port number	Port number for the listener that controls the Tomcat server shutdown. The default value is 18005.

12. Click **Next**.

    The **Pre-Installation Summary** page appears.



13. Verify that the installation information is correct, and then click **Install**.

    During the installation process, the installer displays progress information. When the installation process ends, the **Installation Complete** page appears.

14. Click **Done** to close the installer.

15. To view the log files that the installer generates, navigate to the following directory:
    `<DXInstallationDir>\logs`.

Installing the Partners Portal on UNIX in Console Mode

1. Log in to the machine with the user account that you want to use to install the Partners Portal.
2. Close all other applications.
3. Run the `Install.bin -i console` command.

   The **Introduction** section appears.

4. Read the installation instructions, and then press **Enter**.

The **Install or Upgrade** section appears.

5. Select **1- Install B2B Data Exchange or any of its components**, and then press **Enter**.

   The **PowerCenter Version** section appears.

6. Select the PowerCenter version for which you want to install B2B Data Exchange, and then press **Enter**.

   The **Installation Directory** section appears.

7. Enter the absolute path to the installation directory or accept the default directory, and then press **Enter**.

   The **Installation Components** section appears and displays a numbered list of the components to install.

8. Select **2- B2B Data Exchange Partners Portal**, and then press **Enter**.

   The **Metadata Repository Connection** section appears.

9. Enter the number for the B2B Data Exchange metadata repository database type or accept the default database type:

Option	Description
1- Oracle	Oracle database.
2- Microsoft SQL Server	Microsoft SQL Server database.

10. Enter the number for the metadata repository database connection type or accept the default connection type.

Option	Description
1- Database URL	Location of the database. If you select this option, enter values in the following fields: - Database host name. Host name of the machine where the database server is installed. - Database port number. Port number for the database. The default port number for Oracle is 1521. The default port for Microsoft SQL Server is 1433. - Oracle database. Database SID. System identifier for the database. - Microsoft SQL Server database. Database name. Name of the database instance.
2- Custom Connection String	Connection string to the database. If you select this option, enter values in one of the following fields: - JDBC string. JDBC connection string to the metadata repository. - If you install the PowerCenter client plug-in: ODBC string. ODBC connection string to the metadata repository. The installer cannot verify the validity of the ODBC string. **Note:** If you use a named Microsoft SQL Server database instance, you must specify a custom connection string. You cannot connect to the database instance with a database URL. For example, `jdbc:informatica:sqlserver://MYSQLSERVERCOMPUTERHOSTNAME\MYDBINSTANCENAME;DatabaseName=MYDATABASENAME;`

   Note: The values that you enter here must be identical to the values that you entered in this section during B2B Data Exchange installation.

11. Press **Enter**.

    The **Web Server** section appears.

12. Configure the Web Server connection.
    a. Enter the number for the network communication protocol or accept the default protocol:

Option	Description
1- Enable HTTPS	Instructs B2B Data Exchange to use secure network communication when you open the Operation Console in the browser. If you select HTTPS and HTTP, the Operation Console switches existing HTTP connections with HTTPS connections.
2- Enable HTTP	Instructs B2B Data Exchange to use regular HTTP network communication when you open the Operation Console in the browser.

    b. If you selected **Enable HTTPS**, enter values in the following fields:

Field	Description
Connector port number	Port number for the Tomcat connector to use when you open the Operation Console with HTTPS. The default value is 18443.
Use a keystore file generated by the installer	Instructs the installer to generate a keystore file with an unregistered certificate. If you select this option, ignore the security warning that you receive from the browser the first time you open the Operation Console.
Use an existing keystore file	Instructs the installer to load an existing keystore file. Enter values in the following fields: - Keystore password. Password for the keystore file. - Keystore file. Path to the keystore file. The keystore file must be in the Public Key Cryptography Standard (PKCS) #12 format.

    c. If you selected **Enable HTTP**, enter values in the following fields:

Field	Description
HTTP connector port number	Port number for the HTTP connector. If you clear this field, your browser must connect to the B2B Data Exchange server with HTTPS when you log in to the Operation Console. The default value is 18080.
Server shutdown listener port number	Port number for the listener that controls the Tomcat server shutdown. The default value is 18005.

13. Click **Next**.

    The **Pre-Installation Summary** section appears.

14. Verify that the installation information is correct, and then press **Enter**.

    During the installation process, the installer displays progress information.

15. To view the log files that the installer generates, navigate to the following directory:
    `<DXInstallationDir>\logs`

Step 2. Configure the Partners Portal Logo

1. Copy the `Login_Organization_logo.png` file to the following directory: `dx\tomcat\webapps\dx-portal\img\`.

   This logo appears in the upper right corner of the Partners Portal login page.
2. Copy the `Organization_logo.png` file to the following directory: `dx\tomcat\webapps\dx-portal\img\`.

   This logo appears in the upper right corner of the Partners Portal tabs.

Step 3. Set the Dashboard Properties

When you install the Partners Portal with a stand-alone installation, set the Dashboard properties to ensure that you can view all the Dashboard charts in the Partners Portal.

1. Log in to the machine where you installed the Partners Portal.
2. Edit the following properties in the `dx-configuration.properties` file in the directory `\DX Installation directory\DataExchange\conf\`:

System Property	Description
dx.dashboard.jdbc.username	User name for the operational data store database.
dx.dashboard.jdbc.password	Password for the operational data store in an encrypted string database. If you change the password you must encrypt the string with the password encryption utility and use the encrypted string.
dx.dashboard.jdbc.url	Location of operational data store. The location must be different from the B2B Data Exchange repository.

3. Edit the same properties in the `dx-configuration.properties` file in the directory `\DX Installation directory\DataExchange\tomcat\shared\classes\`.

CHAPTER 7

Upgrading B2B Data Exchange

This chapter includes the following topics:

Upgrading B2B Data Exchange Overview

You can upgrade the following versions of B2B Data Exchange directly to the latest version:

- B2B Data Exchange 10.2.2 HF1
- B2B Data Exchange 10.2.2
- B2B Data Exchange 10.2

When you upgrade B2B Data Exchange, the installer backs up the files of the previous version of B2B Data Exchange and installs the new version. If the document store is found under the B2B Data Exchange Installation folder, you must move the document store to its original location after the upgrade process completes and before you start the DX service. You can create a new repository for the new version or you can use the existing repository. If you use the repository from the previous version, the installer upgrades the repository to the latest version. When you upgrade the B2B Data Exchange repository, you cannot change the database server type and server location.

Before you start the upgrade process, perform the procedures that are described in "Before You Upgrade" on page 88. Then run the B2B Data Exchange installer.

To perform a silent upgrade of the B2B Data Exchange, refer to "Installing B2B Data Exchange in a Silent Mode" on page 56.

After the upgrade, perform the procedures that are described in "After You Upgrade" on page 108.

For more information about the B2B Data Exchange configuration that you can perform after you upgrade, see Chapter 4, "B2B Data Exchange Installation" on page 25.

Note: During the upgrade you cannot change the user authentication method that B2B Data Exchange uses. To change the user authentication method you must first upgrade the system and then switch to the required authentication method. For information about switching between authentication methods see the *B2B Data Exchange Administrator Guide*.

Before You Upgrade

To prepare for the upgrade, perform the following tasks:

1. Verify that you have the user names and passwords for the required database accounts.
2. Stop all B2B Data Exchange services. The B2B Data Exchange upgrade modifies the B2B Data Exchange files. The installer cannot proceed if the files are in use.
3. Stop all PowerCenter workflows that process B2B Data Exchange documents. In PowerCenter, stop all workflows that process B2B Data Exchange documents. Do not start the workflows again until the upgrade is complete.
4. Back up the B2B Data Exchange repository to be upgraded. Use the database server backup utility to back up the repository. This ensures that you can recover from any errors that you encounter during the upgrade.
5. Back up the existing B2B Data Exchange installation folder. Perform this action to help ensure that you can recover from any errors encountered during the upgrade, and that, after the upgrade, you can reapply modifications that were made to the configuration in previous versions.
6. If the PowerCenter services are not installed on the same machine where B2B Data Exchange is installed and you have upgraded the pmrep command line utility after you installed the previous version of B2B Data Exchange, clean up all CNX files from the `Tmp` folder on your root directory.
7. If the Partners Portal was not installed on your system in previous versions and you want to install the portal when you upgrade to the new version, open ports to the portal in your firewall.

Opening Ports to the Partners Portal

If you want to install the Partners Portal, enable access to the portal in the firewall by opening the HTTP or HTTPS ports from the external network to the Portal server.

Configure the firewall to allow URLs that start with the suffix `/dx-portal` and `/dx-portal-help` only.

To ensure that outside access to the Partners Portal is securely performed, assign the external hostname URL for the portal to the **dx.portal.url** system property. For more information about configuring system properties in the B2B Data Exchange Operation Console, see the *B2B Data Exchange Administror Guide*.

Upgrading B2B Data Exchange on a Windows Operating System

Upgrade B2B Data Exchange on Windows operating systems in graphical mode. On UNIX operating systems, upgrade B2B Data Exchange in console mode.

Before you install, verify that your environment meets the minimum system requirements, perform the pre-installation tasks, and verify that the PowerCenter services are running.

Note: During the upgrade, B2B Data Exchange saves log files in the home directory of the user in the subdirectory named `DXLogs`. If the upgrade does not complete successfully, you can view the log files in this location.

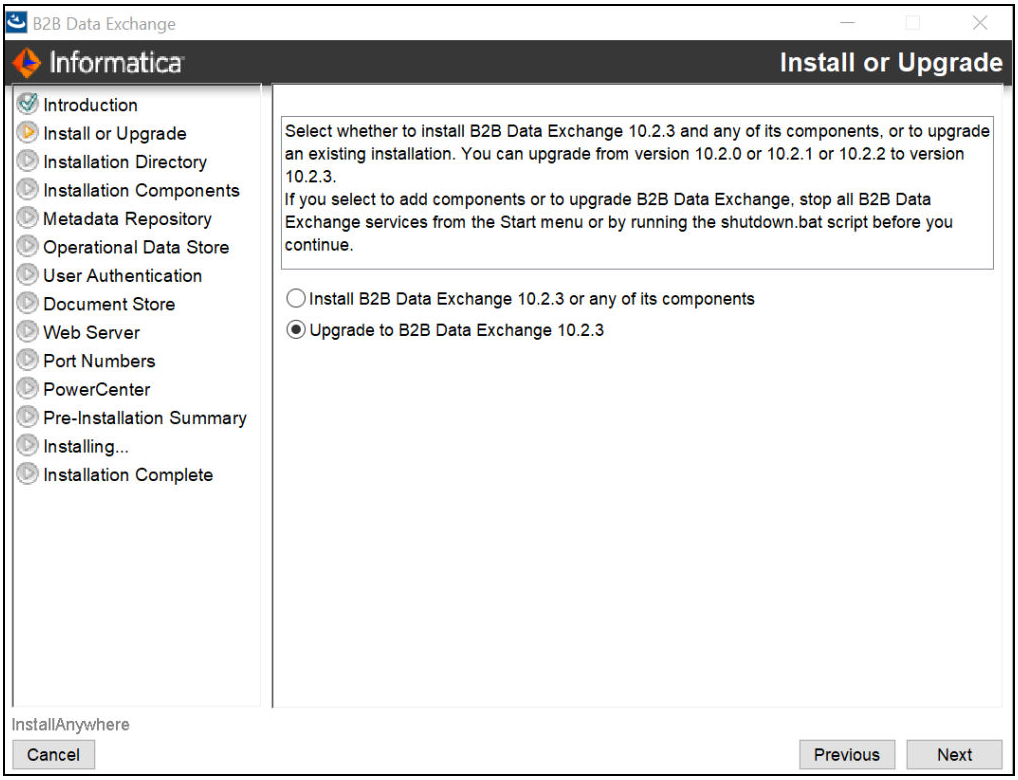
Step 1. Run the Installer

1. Log in to the machine with the user account that you want to use to install B2B Data Exchange.

   To prevent permission errors, use the same account to install B2B Data Exchange and PowerCenter.
2. Close all other applications.
3. Run `Install.exe` from the directory where you downloaded the installer.

   The **Introduction** page appears.
4. Read the instructions, and then click **Next**.

   The **Install or Upgrade** page appears.

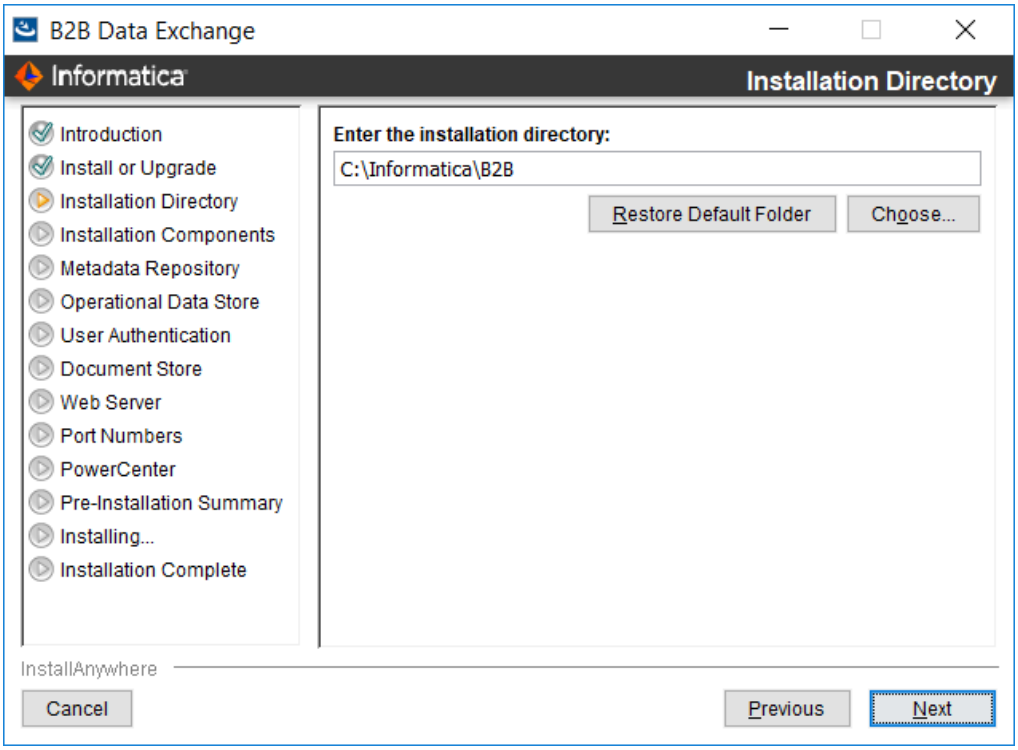


5. Select the option to upgrade B2B Data Exchange, and then click **Next**.

   The **Installation Directory** page appears.

Step 2. Define Installation Settings

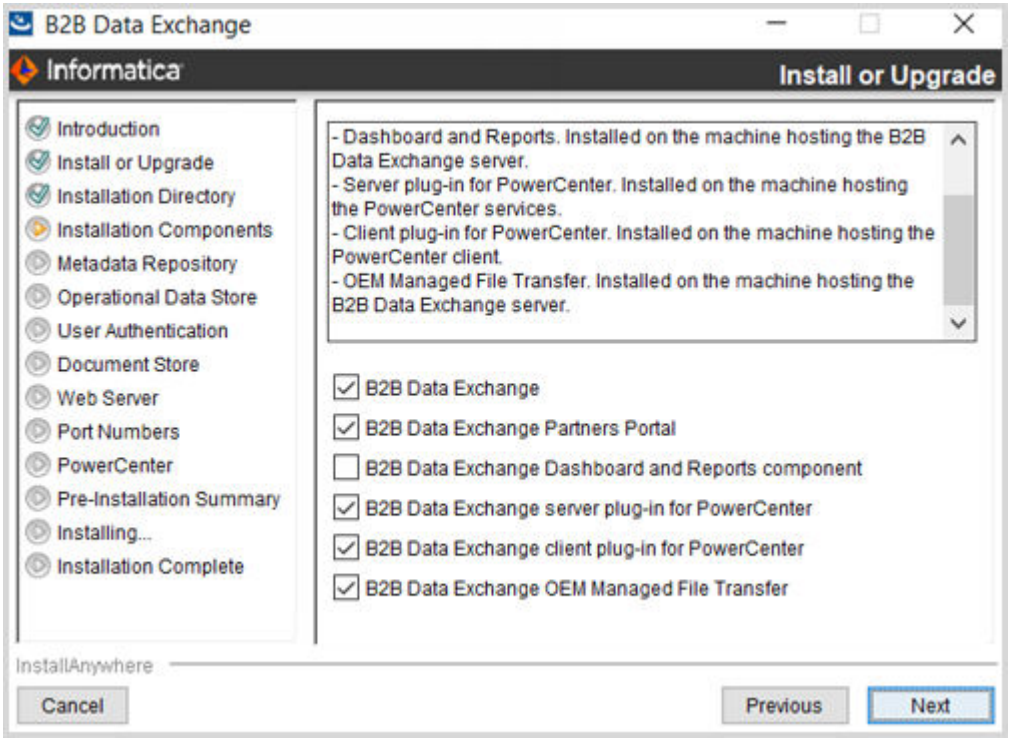
1. On the **Installation Directory** page, enter the absolute path to the installation directory or accept the default directory.



Note: You must select the same installation directory where you installed the previous B2B Data Exchange version.

2. Click **Next**.

The **Installation Components** page appears.



3. Select the components to install:

B2B Data Exchange

Installs the core B2B Data Exchange application.
Selected by default.

B2B Data Exchange Partners Portal

Installs the B2B Data Exchange Partners Portal component. You must install B2B Data Exchange to install the Partners Portal component.
Selected by default.

B2B Data Exchange Dashboard and Reports

Installs the B2B Data Exchange Dashboard and Reports component. You must install B2B Data Exchange to install the Dashboard and Reports component.
Cleared by default.

Note:

- If you install the Dashboard and Reports component, you must import the operational data store event loader after you install B2B Data Exchange.
- If you install the Dashboard and Reports component, your B2B Data Exchange and operational data store repositories are installed on Microsoft SQL Servers, and you use PowerCenter version 10, you must configure the repository connections in PowerCenter Workflow Manager. For details, see "Configuring Repository Connections on PowerCenter Version 10" on page 126.
- If you do not install the Dashboard and Reports component, the Dashboard will not be available in the Partners Portal.

B2B Data Exchange PowerCenter server plug-in

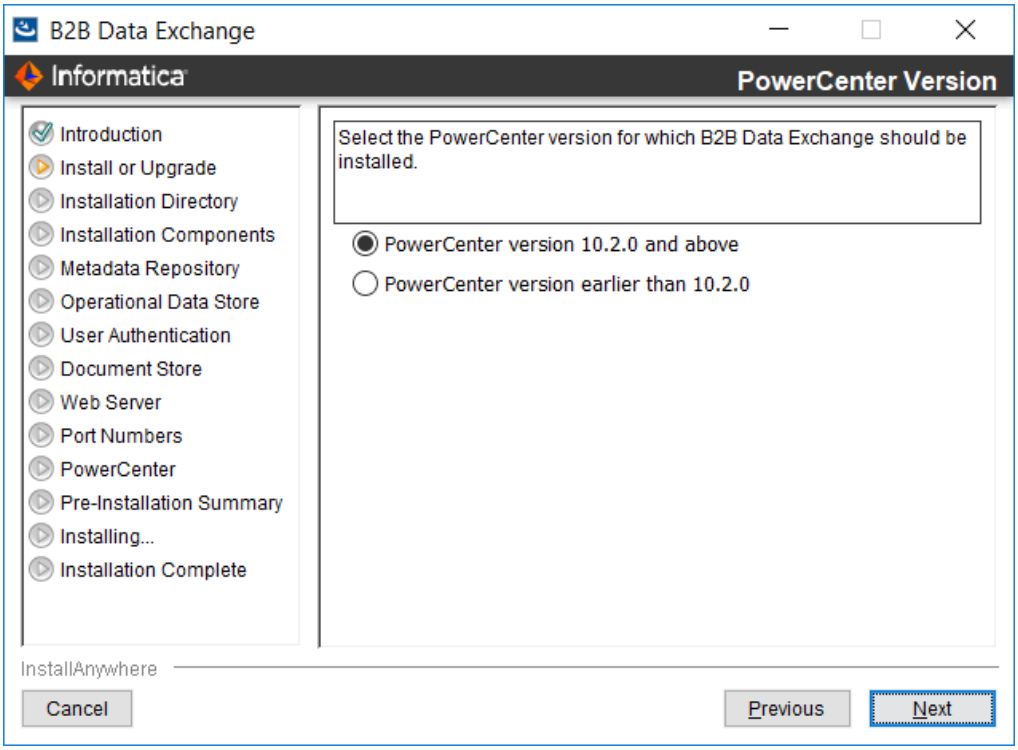
Installs the B2B Data Exchange plug-in for the PowerCenter services. After the installation, you register the plug-in to the PowerCenter repository.
Selected by default.

B2B Data Exchange PowerCenter client plug-in

Installs the B2B Data Exchange plug-in for the PowerCenter Client. Install this component on every machine that runs the PowerCenter Client.
Selected by default.

4. Click **Next**.

   The **PowerCenter Version** page appears.



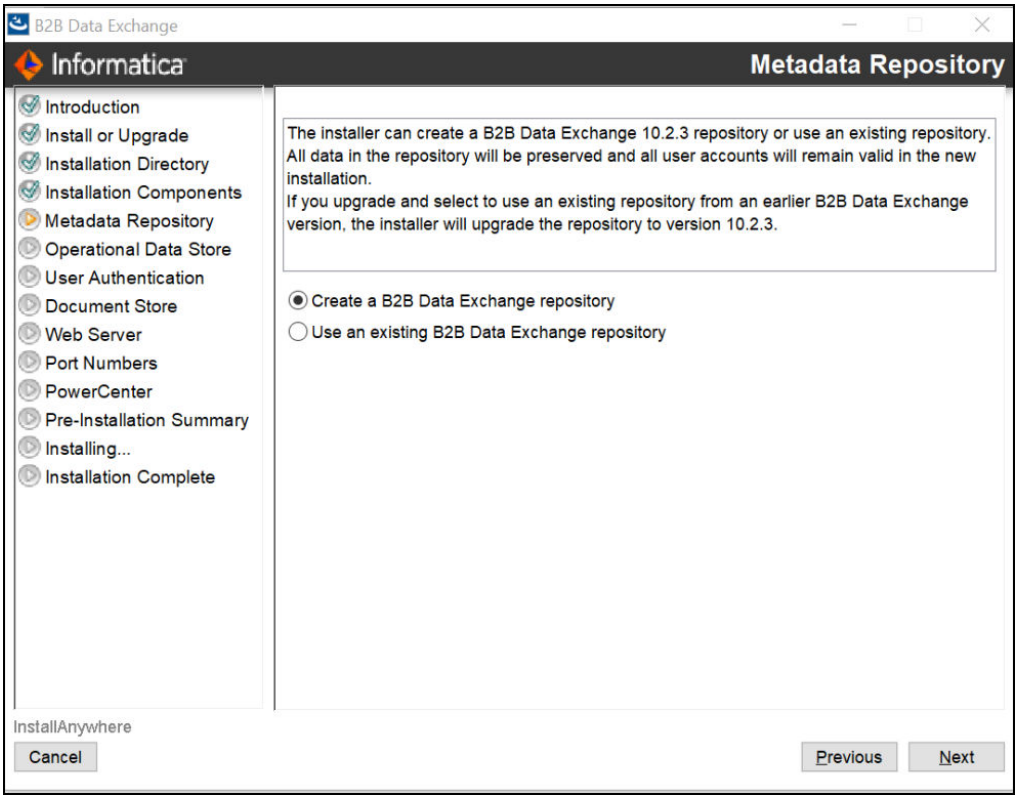
5. Select the PowerCenter version for which to install B2B Data Exchange and then click **Next**.

   The **Metadata Repository** page appears.

Step 3. Configure B2B Data Exchange Repository

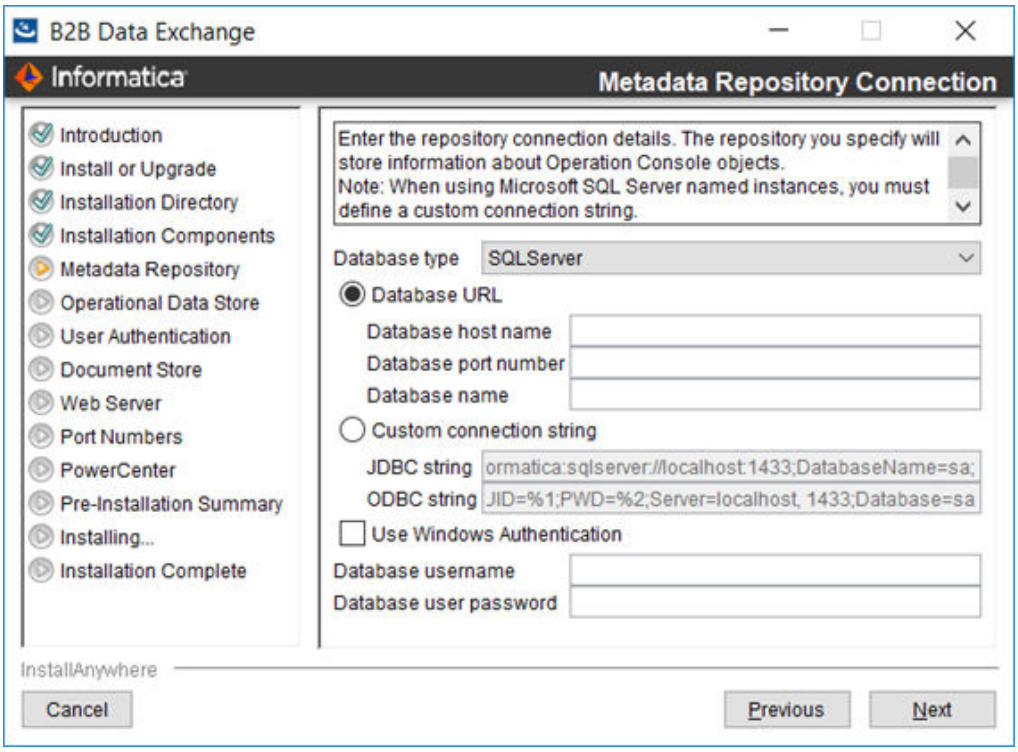
1. On the **Metadata Repository** page, select one of the following options:
   - **Create a B2B Data Exchange repository**. Creates a repository in the database.

- **Use an existing B2B Data Exchange repository**. Uses the tables and data in an existing B2B Data Exchange repository and upgrades the repository.



2. Click **Next**.

The **Metadata Repository Connection** page appears.



3. Enter values in the following fields:

Database type

Type of database to use for the B2B Data Exchange metadata repository. You can choose one of the following options:

- Oracle
- Microsoft SQL Server

Database URL

Location of the database.
If you select this option, enter the values in the following fields:

- **Database host name**. Host name of the machine where the database server is installed.
- **Database port**. Port number for the database. The default port number for Oracle is 1521. The default port number for Microsoft SQL Server is 1433.
- **Database SID**. System identifier for the database if the database is Oracle. Enter either a fully qualified ServiceName or a fully qualified SID.

  Note: It is recommended that you enter a ServiceName in this field.
- **Microsoft SQL Server database** . Database name.

Custom Connection String

Connection string to the database.
If you select this option, enter values in one of the following fields:

- **JDBC string**. JDBC connection string to the metadata repository.

- **ODBC string**. ODBC connection string to the metadata repository. Available if you install the PowerCenter Client plug-in. The installer cannot verify the validity of the ODBC string.

Use Windows Authentication

Instructs B2B Data Exchange to authenticate user names against the Microsoft Windows authentication mechanism. Available when you select a Microsoft SQL Server database.

Database username

Name of the database user account for the database where you do not use Windows authentication.

Database user password

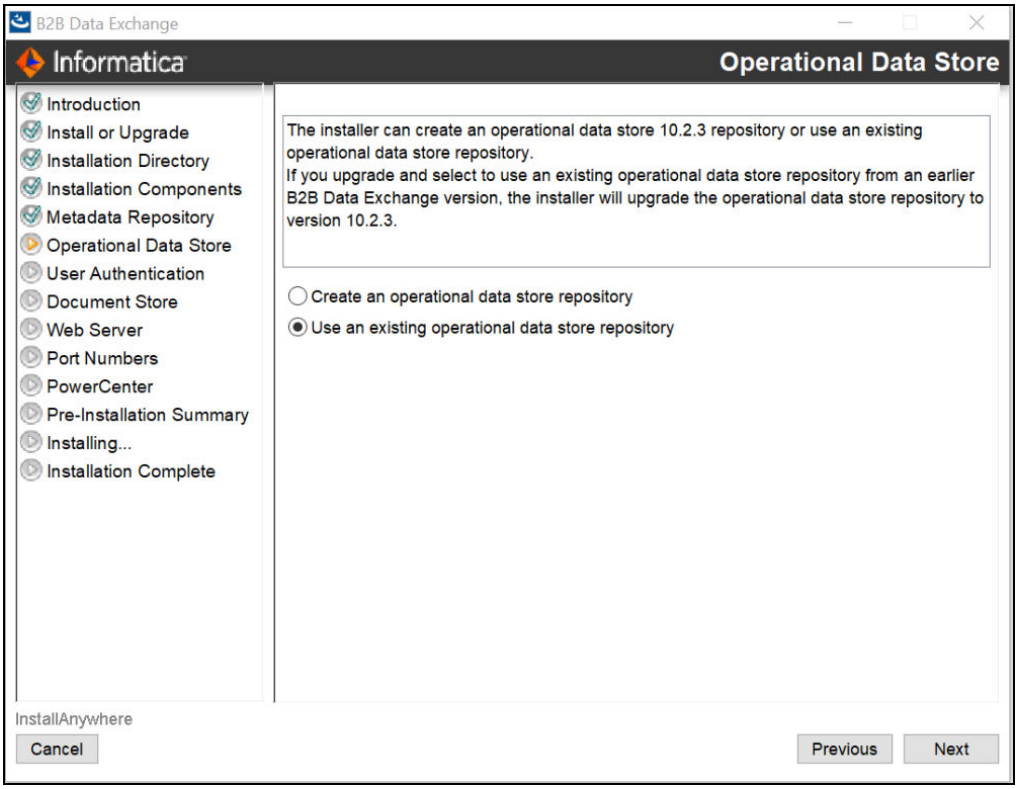
Password for the database account for the database where you do not use Windows authentication. B2B Data Exchange stores the password as an encrypted string.

4. Click **Next**.

If you selected the **B2B Data Exchange Dashboard and Reports** component, the **Operational Data Store** page appears. If you did not select the Dashboard and Reports component, go to "Step 5. Configure Web Server and Port Numbers" on page 97.

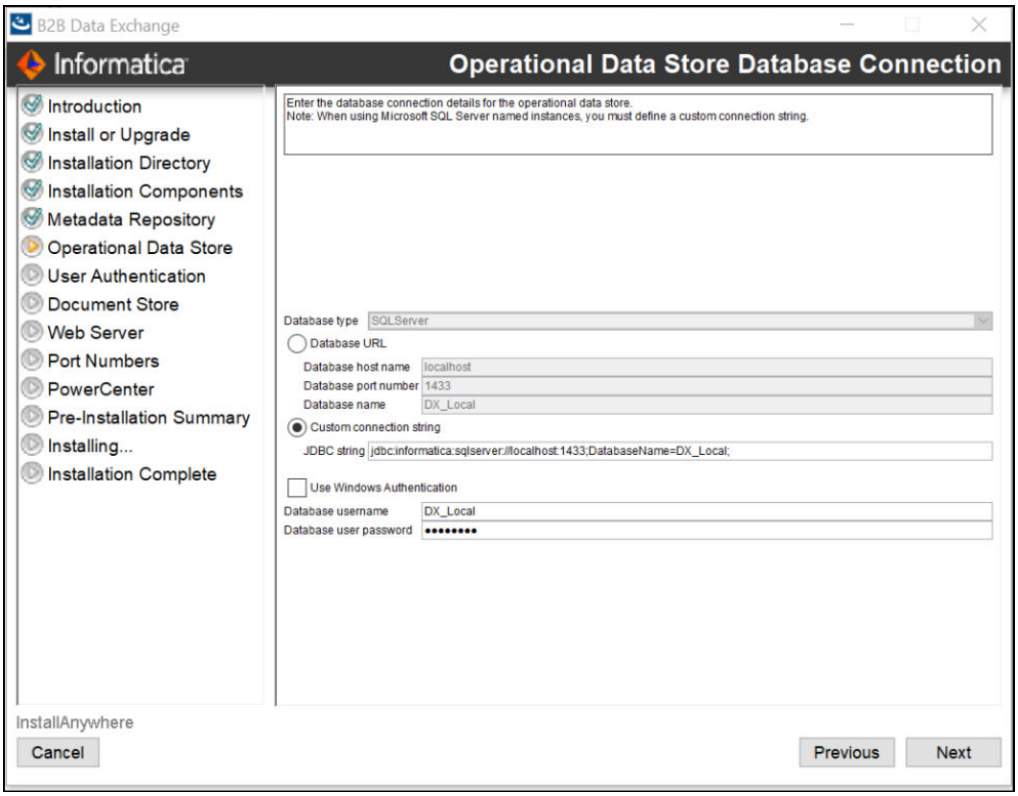
Step 4. Set Up the Operational Data Store

1. On the **Operational Data Store** page, select one of the following options:
   - **Create an operational data store repository**. Creates an operational data store repository in the database.
   - **Use an existing operational data store repository**. Uses the tables and data in an existing operational data store repository.



2. Click **Next**.

The **Operational Data Store Database Connection** page appears.



3. Enter values in the following fields:

Database URL

Location of the database. If you select this option, enter the values in the following fields:

- **Database host name**. Host name of the machine where the database server is installed.
- **Database port number**. Port number for the database. The default port number for an Oracle database is 1521. The default port number for a Microsoft SQL server is 1433.
- **Database SID**. System identifier for the database if you select Oracle as the database. Enter either a fully qualified ServiceName or a fully qualified SID.

  Note: It is recommended that you enter a ServiceName in this field.
- **Microsoft SQL Server database** . Database name.

Custom Connection String

Connection string to the database. If you select this option, enter values in one of the following fields:

- **JDBC string**. JDBC connection string to the Operational Data Store.
- **ODBC string**. ODBC connection string to the Operational Data Store. Available if you install the PowerCenter Client plug-in. The installer cannot verify the validity of the ODBC string.

Note: If you use a named Microsoft SQL Server database instance, you cannot connect to the database instance using the **Database URL** option. Use the **Custom Connection String** option.

For example:

```
jdbc:informatica:sqlserver://MYSQLSERVERCOMPUTERHOSTNAME
\MYDBINSTANCENAME;DatabaseName=MYDATABASENAME;
```

Use Windows Authentication

Instructs B2B Data Exchange to authenticate user names against the Microsoft Windows authentication mechanism. Available when you select a Microsoft SQL Server database.

Database username

Name of the operational data store user account for the database where you do not use Windows authentication.

Database user password

Password for the operational data store account for the database where you do not use Windows authentication. B2B Data Exchange stores the password as an encrypted string.

4. Click **Next**.

   The **Web Server** page appears.

Step 5. Configure Web Server and Port Numbers

1. On the **Web Server** page enter values in the following fields:

   Enable HTTPS

   Instructs B2B Data Exchange to use secure network communication when you open the Operation Console in the browser. If you select HTTPS and HTTP, the Operation Console switches existing HTTP connections with HTTPS connections.

   Connector port number

   Port number for the Tomcat connector to use when you open the Operation Console with HTTPS. The default value is 18443.

   Use a keystore file generated by the installer

   Instructs the installer to generate a keystore file with an unregistered certificate. If you select this option, ignore the security warning that you receive from the browser the first time you open the Operation Console.

   Use an existing keystore file

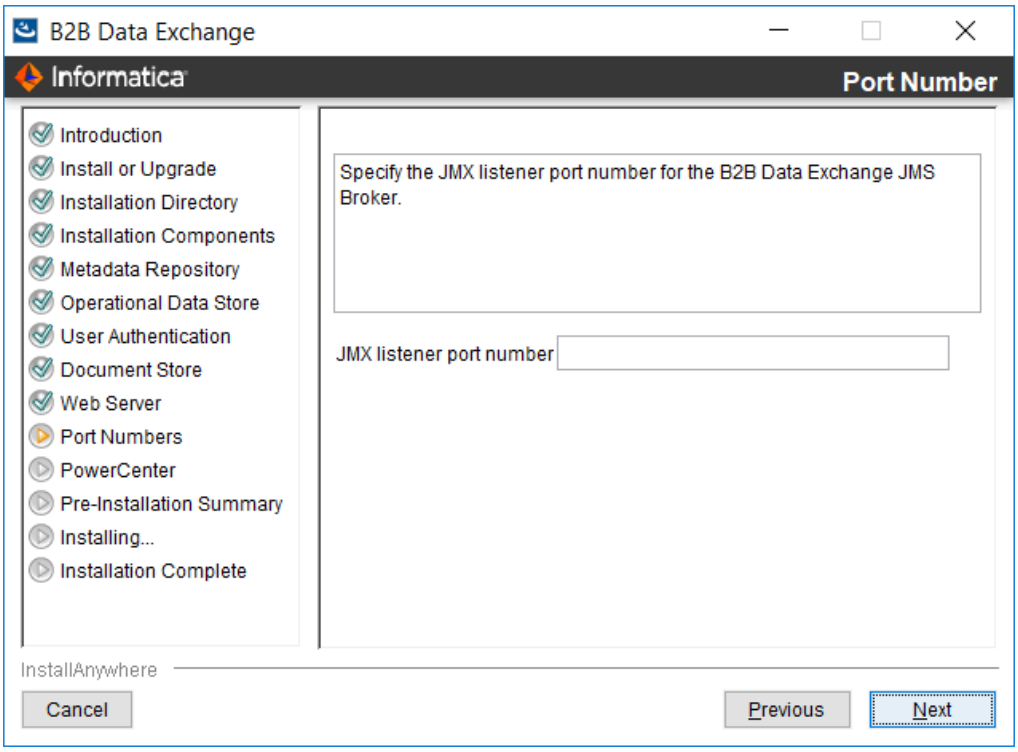
   Instructs the installer to load an existing keystore file. Enter values in the following fields:

   - Keystore password. Password for the keystore file.
   - Keystore file. Path to the keystore file.

   The keystore file must be in the Public Key Cryptography Standard (PKCS) #12 format.

2. Click **Next**.

The **Port Numbers** page appears.



3. Enter the port number for the B2B Data Exchange JMS Broker JMX listener port or accept the default port, and then click **Next**.

   If you selected to install the B2B Data Exchange server plug-in for PowerCenter or the B2B Data Exchange client plug-in for PowerCenter components, the **PowerCenter Location** page appears. If you did not select the PowerCenter server or client components, the **PowerCenter Web Services Hub** page appears.

Step 6. Configure PowerCenter Settings

1. On the **PowerCenter Web Services Hub** page, enter the PowerCenter web services details.

   Web Services Hub URL

   URL that the PowerCenter Web Services Hub uses when B2B Data Exchange transfers documents to PowerCenter for processing with batch workflows.

   Service name

   Name of the PowerCenter Repository Service.

   Node host name

   Host name of the node that runs the PowerCenter Repository Service.

   Node port number

   Port number of the node that runs the PowerCenter Repository Service.

   Username

   Name of the PowerCenter Repository Service user.

   Password

   Password for the PowerCenter Repository Service user. B2B Data Exchange stores the password as an encrypted string.

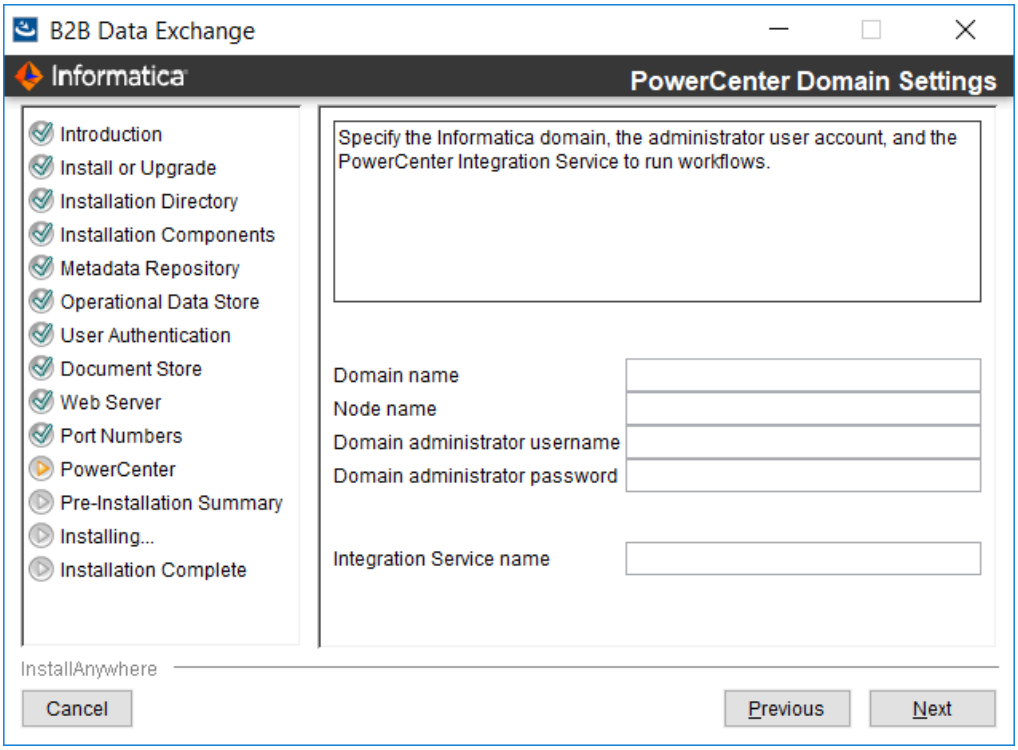
   Security domain

   Optional. Name of the Informatica security domain in which the PowerCenter Repository Service user is stored.
   Default is Native.

2. Click **Next**.

   If you selected to install the B2B Data Exchange server plug-in for PowerCenter component, the **Informatica Domain** page appears.

If you did not select the PowerCenter server component, the **Pre-Installation Summary** page appears. Go to "Step 7. Complete the Installation" on page 101.



3. Enter values in the following fields:

Domain name

Name of the Informatica domain that contains the PowerCenter Integration Service that runs B2B Data Exchange workflows.

Node name

Node in the Informatica domain on which the PowerCenter Integration Service runs.

Domain administrator username

Name of the Informatica domain administrator.

Domain administrator password

Password for the Informatica domain administrator. B2B Data Exchange stores the password as an encrypted string.

Integration Service name

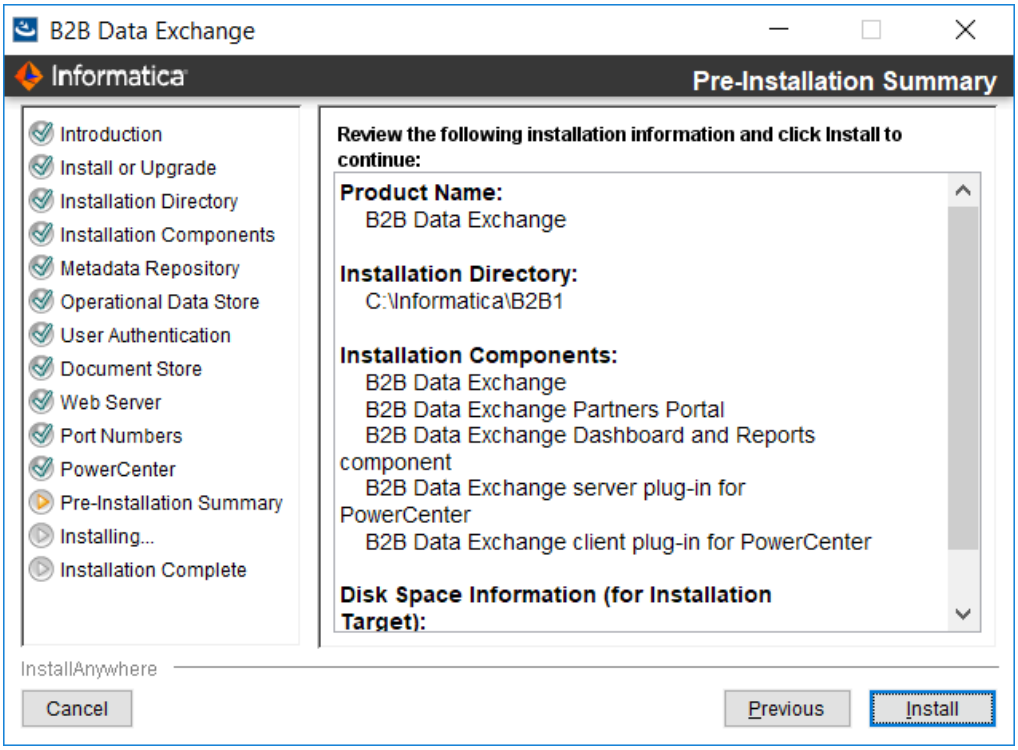
The name of the PowerCenter Integration Service that B2B Data Exchange uses to run workflows.

4. Click **Next**.

The **Pre-Installation Summary** page appears.

Step 7. Complete the Installation

1. On the **Pre-Installation Summary** page, verify that the installation information is correct, and then click **Install**.



   During the installation process, the installer displays progress information. When the installation process ends, the **Post-Installation Actions** page appears.

2. If you installed the B2B Data Exchange PowerCenter server plug-in, follow the wizard instructions to register the plug-in to the PowerCenter repository, and then click **Next**.

   The **Installation Complete** page appears.

3. Click **Done** to close the installer.

4. To view the log files that the installer generates, navigate to the following directory: `<DXInstallationDir>\logs`.

5. Perform the required post-installation tasks.

   For more information, see Chapter 5, “Post-Installation Tasks” on page 65.

   Note: Perform only the tasks that are relevant for your environment.

6. Optionally, perform additional configuration tasks. For more information, see Chapter 9, “Optional B2B Data Exchange Configuration” on page 115.

Upgrading B2B Data Exchange on a UNIX Operating System

Upgrade B2B Data Exchange on UNIX operating systems in console mode. On Windows operating systems, upgrade B2B Data Exchange in graphical mode.

Before you install, verify that your environment meets the minimum system requirements, perform the pre-installation tasks, and verify that the PowerCenter services are running.

Note: During the upgrade, B2B Data Exchange saves log files in the home directory of the user, in the subdirectory named `DXLogs`. If the upgrade does not complete successfully, you can view the log files in this location.

Step 1. Run the Installer

1. Log in to the machine with the user account that you want to use to install B2B Data Exchange.

   To prevent permission errors, use the same account to install B2B Data Exchange and PowerCenter.
2. Close all other applications.
3. Run `Install.bin -i console` from the directory where you downloaded the installer.

   The **Introduction** section appears.
4. Read the instructions, and then press **Enter**.

   The **Install or Upgrade** section appears.
5. Enter **2** to upgrade B2B Data Exchange, and then press **Enter**.

   The **Installation Directory** section appears.

Step 2. Define Installation Settings

1. In the **Installation Directory** section, enter the absolute path to the installation directory or accept the default directory, and then press **Enter**.

   The **Installation Components** section appears and displays a numbered list of the components to install.
2. Enter a comma-separated list of numbers for the components to install or accept the default components:

   1- B2B Data Exchange

   Installs the core B2B Data Exchange application.
   Selected by default.

   2- B2B Data Exchange Partners Portal

   Installs the B2B Data Exchange Partners Portal component. You must install B2B Data Exchange to install the Partners Portal component.
   Selected by default.

   3- B2B Data Exchange Dashboard and Reports

   Installs the B2B Data Exchange Dashboard and Reports component. You must install B2B Data Exchange to install the Dashboard and Reports component.
   Cleared by default.

4- B2B Data Exchange Server Plug-in for PowerCenter

Installs the B2B Data Exchange PowerCenter server plug-in component. After the installation, register the plug-in to the PowerCenter repository.
Selected by default.

5- B2B Data Exchange OEM Managed File Transfer

Adds the OEM Managed File Transfer component to B2B Data Exchange. You must install B2B Data Exchange to install the OEM Managed File Transfer component.
Selected by default.

3. Press **Enter**.

   The **PowerCenter Version** section appears.

4. Select the PowerCenter version for which to install B2B Data Exchange or accept the default selection:

   1- PowerCenter version below 10.2.0

   Select this option for PowerCenter versions below 10.2.0.

   2 - PowerCenter version 10.2.0 and above

   Select this option for PowerCenter versions 10.2.0 and above.

5. Press **Enter**.

   The **Metadata Repository** section appears.

Step 3. Configure B2B Data Exchange Repository

1. In the **Metadata Repository** section, enter the number for the metadata repository database configuration option or accept the default option:

   1- Create a B2B Data Exchange repository

   Creates a repository in the database.

   2- Use an existing B2B Data Exchange repository

   Uses the tables and data in an existing repository.

2. Press **Enter**.

   The **Metadata Repository Connection** section appears.

3. Enter one of the following numericals depending on the database you plan to use as the B2B Data Exchange metadata repository database:

   - Enter `1` to use an Oracle database as the B2B Data Exchange metadata repository database.
   - Enter `2` to use Microsoft SQL Server database as the B2B Data Exchange metadata repository database.

4. Enter the number for the metadata repository database connection type or accept the default connection type:

   1- Database URL

   Location of the database. If you select this option, enter values in the following fields:

   - **Database Host Name**. Host name of the machine where the database server is installed.
   - **Database Port Number**. Port number for the database. The default port number for Oracle is 1521. The default port for Microsoft SQL Server 1433.
   - **Database SID**. System identifier for the database.

- **Microsoft SQL Server database** . Database name. Name of the database instance.

2- Custom Connection String

Connection string to the database. If you select this option, enter values in one of the following fields:

- JDBC string. JDBC connection string to the metadata repository.
- ODBC string. ODBC connection string to the metadata repository. Applicable if you install the PowerCenter client plug-in. The installer cannot verify the validity of the ODBC string.

Note: If you use a named Microsoft SQL Server database instance, you cannot connect to the database instance using the **Database URL** option. Use the **Custom Connection String** option.

For example:

```
jdbc:informatica:sqlserver://MYSQLSERVERCOMPUTERHOSTNAME
\MYDBINSTANCENAME;DatabaseName=MYDATABASENAME;
```

5. Enter values in the following fields:

Database username

Name of the database user account.

Database user password

The password for the database account for the database. B2B Data Exchange stores the password as an encrypted string.

6. Press **Enter**.

If you selected to install the B2B Data Exchange Dashboard and Reports component, the **Operational Data Store** section appears. If you did not select to install the Dashboard and Reports component, go to "Step 5. Configure the Web Server and Port Numbers" on page 105.

Step 4. Set Up the Operational Data Store

1. In the **Operational Data Store** section, enter the number for the database configuration option for the operational data store or accept the default option:

1- Create an operational data store repository

Creates an operational data store repository in the database.

2- Use an existing operational data store repository

Uses the tables and data in an existing operational data store repository.

2. Enter the number for the database connection type for the operational data store or accept the default connection type:

1- Database URL

Location of the database. If you select this option, enter values in the following fields:

- **Database host name**. Host name of the machine where the database server is installed.
- **Database port number**. Port number for the database. The default port number for Oracle is 1521. The default port for Microsoft SQL Server is 1433.
- **Oracle database**. Database SID. System identifier for the database.
- **Microsoft SQL Server database** . Database name. Name of the database instance.

2- Custom Connection String

Connection string to the database. If you select this option, enter values in one of the following fields:

- **JDBC string.** JDBC connection string to the Operational Data Store.
- **ODBC string**. ODBC connection string to the Operational Data Store. If you install the PowerCenter client plug-in, the installer cannot verify the validity of the ODBC string.

Note: If you use a named Microsoft SQL Server database instance, you cannot connect to the database instance using the **Database URL** option. Use the **Custom Connection String** option.

For example:

```
jdbc:informatica:sqlserver://MYSQLSERVERCOMPUTERHOSTNAME
\MYDBINSTANCENAME;DatabaseName=MYDATABASENAME;
```

3. Enter values for the operational data store in the following fields:

Database username

Name of the database user account for the database.

Database user password

The password for the database account for the database. B2B Data Exchange stores the password as an encrypted string.

4. Press **Enter**.

The **Web Server** section appears.

Step 5. Configure the Web Server and Port Numbers

1. Configure the Web Server connection.
   a. Enter the number for the network communication protocol or accept the default protocol:

1- Enable HTTPS

Instructs B2B Data Exchange to use secure network communication when you open the Operation Console in the browser.
If you select HTTPS and HTTP, the Operation Console switches existing HTTP connections with HTTPS connections.

2- Enable HTTP

Instructs B2B Data Exchange to use regular HTTP network communication when you open the Operation Console in the browser.

   b. If you selected **Enable HTTPS**, enter values in the following fields:

Connector port number

Port number for the Tomcat connector to use when you open the Operation Console with HTTPS.
The default value is 18443.

Use a keystore file generated by the installer

Instructs the installer to generate a keystore file with an unregistered certificate. If you select this option, ignore the security warning that you receive from the browser the first time you open the Operation Console.

Use an existing keystore file

Instructs the installer to load an existing keystore file. Enter values in the following fields:

- Keystore password. Password for the keystore file.
- Keystore file. Path to the keystore file.

The keystore file must be in the Public Key Cryptography Standard (PKCS) #12 format.

c. If you selected **Enable HTTP**, enter values in the following fields:

HTTP connector port number

Port number for the HTTP connector. If you clear this field, your browser must connect to the B2B Data Exchange server with HTTPS when you log in to the Operation Console.
The default value is 18080.

Server shutdown listener port number

Port number for the listener that controls the Tomcat server shutdown.
The default value is 18005.

2. Press **Enter**.

   The **Port Numbers** section appears.

3. Enter the port number for the B2B Data Exchange JMS Broker JMX listener port or accept the default port and then press **Enter**.

   If you selected to install the B2B Data Exchange PowerCenter server plug-in or the B2B Data Exchange PowerCenter Client plug-in components, the **PowerCenter Location** section appears. If you did not select the PowerCenter server or client components, the **PowerCenter Web Services Hub** section appears.

Step 6. Configure PowerCenter Settings

1. If you selected to install the B2B Data Exchange PowerCenter server plug-in or the B2B Data Exchange PowerCenter Client plug-in components, in the **PowerCenter Location** section, enter the directory where you installed PowerCenter or accept the default directory, and then press **Enter**.

   The **PowerCenter Web Services** section appears.

2. In the **PowerCenter Web Services** section, press **Enter** to accept the default URL or enter the URL that the PowerCenter Web Services Hub uses when B2B Data Exchange transfers documents to PowerCenter for processing with batch workflows and then press **Enter**.
3. Enter the name of the PowerCenter Repository Service, and then press **Enter**.
4. Enter values in the following fields:

Node host name

Host name of the node that runs the PowerCenter Repository Service.

Node port number

Port number of the node that runs the PowerCenter Repository Service.

Username

Name of the PowerCenter Repository Service user.

Password

Password for the PowerCenter Repository Service user. B2B Data Exchange stores the password as an encrypted string.

Security domain

Optional. Name of the Informatica security domain in which the PowerCenter Repository Service user is stored.
Default is Native.

5. Press **Enter**.

   If you selected to install the B2B Data Exchange server plug-in for PowerCenter component, the **Informatica Domain** section appears. If you did not select the PowerCenter server component, the **Pre-Installation Summary** section appears. Go to Step 8. Complete the Installation.

6. Enter values in the following fields:

   Domain name

   Name of the Informatica domain that contains the PowerCenter Integration Service that runs B2B Data Exchange workflows.

   Node name

   Node in the Informatica domain on which the PowerCenter Integration Service runs.

   Domain administrator user name

   Name of the Informatica domain administrator.

   Domain administrator password

   Password for the Informatica domain administrator. B2B Data Exchange stores the password as an encrypted string.

7. Press **Enter**.
8. Enter the name of the PowerCenter Integration Service that B2B Data Exchange uses to run workflows, and then press **Enter**.
9. Press **Enter**.

   The **Pre-Installation Summary** section appears.

Step 7. Complete the Installation

1. In the **Pre-Installation Summary** section, verify that the installation information is correct, and then press **Enter**.

   During the installation process, the installer displays progress information.

2. If you installed the B2B Data Exchange PowerCenter server plug-in, follow the on-screen instructions to register the plug-in to the PowerCenter repository, and then press **Enter**.
3. To view the log files that the installer generates, navigate to the following directory:
   `<DXInstallationDir>\logs`
4. Perform the required post-installation tasks.

   For more information, see Chapter 5, “Post-Installation Tasks” on page 65.

   Note: Perform only the tasks that are relevant for your environment.

5. Optionally, perform additional configuration tasks. For more information, see Chapter 9, “Optional B2B Data Exchange Configuration” on page 115.

After You Upgrade

After you upgrade, update the B2B Data Exchange configuration files to work with the upgraded instance of B2B Data Exchange.

To update the configuration files and complete the upgrade process, perform the following steps:

1. Reapply modifications that were made to B2B Data Exchange configuration files in previous versions.
2. If you installed the Dashboard and Reports component, register the license of the Dashboard and Reports component.
3. If you installed the Dashboard and Reports component, import the operational data store (ODS) loader workflow.
4. To unregister the existing PowerCenter server plug-in, click the Plug-ins tab after the Repository Service restarts. Click the unregister icon (next to the existing plug-in) to unregister the plug-in.
5. Use the PowerCenter Administration Console to register the plug-in in the PowerCenter repository.
6. Restart PowerCenter workflows.
7. Start the B2B Data Exchange Server.
8. If any of the B2B Data Exchange repositories are installed on a Microsoft SQL Server and use Windows authentication, configure credentials for Windows authentication.
9. Clear the browser cache on each of the client machines.
10. If you upgrade the Partners Portal component, to provide existing portal users with Partners Portal privileges, create portal user groups and then assign each portal user to a portal user group.

    Note: If you do not assign a portal user to a portal user group, the portal user can only view the Dashboard in the Partners Portal.
11. If you installed the Partners Portal component, you can brand the Partners Portal with the organization logo.

    Note: If you used your logo in the previous version, you must perform this task after the upgrade in order to re-brand the portal.

Note: The B2B Data Exchange installer does not delete the previous version of B2B Data Exchange. The installer renames the folder with the suffix `_Backupn.n.n` where n.n.n is the version number that you upgraded. To ensure that you update the configuration files correctly, see the configuration files in the directory of the previous version of B2B Data Exchange.

Related Topics:

- "Importing the Web Services to PowerCenter" on page 70

Reapplying Configuration Modifications

Reapply modifications that were made to B2B Data Exchange configuration files in previous versions.

To perform this procedure, you must have backed up the B2B Data Exchange installation folder.

1. Open the following file from the location where you backed up the B2B Data Exchange installation folder:

   ```
   <BackupDir>/conf/dx-configuration.properties
   ```
2. On the machine where B2B Data Exchange is installed, open the server and console copies of the `dx-configuration.properties` files in a text editor from the following locations:

   ```
   <DXInstallationDir>\DataExchange\tomcat\shared\classes\
   <DXInstallationDir>\conf\
   ```

3. Copy any relevant configuration changes from the file that you backed up to both the `dx-configuration.properties` files.
4. Save the `dx-configuration.properties` files.

Registering the Dashboard and Reports License

Register the license of the B2B Data Exchange Dashboard and Reports component.

1. Start the B2B Data Exchange services.
2. Move the file `_Settings.lgx` from the following location:

   `<DXInstallationDir>\DataExchange\tomcat\webapps\dx-dashboard\_Definitions`

   To the following location:

   `<DXInstallationDir>\DataExchange\tomcat\shared\classes`

   Rename the file to the following name:

   `dx_dashboard_configuration.xml`
3. Reapply modifications that were made to the file `dx_dashboard_configuration.xml` in previous versions.
4. Copy the Logi Info Dashboard license file `_Settings_encrypted.lgx` to the following location:

   `<DXInstallationDir>\DataExchange\tomcat\webapps\dx-dashboard\_Definitions`
5. Rename the file `_Settings_encrypted.lgx` to `_Settings.lgx`.
6. Restart the B2B Data Exchange services.

Replacing the Operational Data Store Loader Workflow

If you installed the Dashboard and Reports component for the first time, import the operational data store (ODS) loader workflow. If the Dashboard and Reports component was installed in the previous version of B2B Data Exchange and you are upgrading to the current version from a version earlier than 9.6.2, replace the existing workflow.

Note: If the Dashboard and Reports component was installed in the previous version of B2B Data Exchange, you must have unscheduled the B2B Data Exchange ODS loader workflow before you upgraded B2B Data Exchange to the current version. For more information, see GUID-8BD86874-0566-47F6-99C8-16427FA8E887.

1. In PowerCenter Repository Manager, run the **Import Wizard**.
2. Select the B2B Data Exchange ODS loader workflow file. The name of the workflow file depends on the type of database on which the ODS is installed:

Database Type	Workflow Location and Name
Oracle	`<DXInstallationDir>\powercenter\ETL\DX_ETL.xml`
Microsoft SQL Server	`<DXInstallationDir>\powercenter\ETL\DX_ETL_SQLSERVER.xml`

3. If the Dashboard and Reports component was installed in the previous version of B2B Data Exchange and you are upgrading to the current version from version 9.6.1, select the PowerCenter repository folder that contains the B2B Data Exchange ODS loader workflow from the previous version as the import folder target.
4. If the Dashboard and Reports component was installed in the previous version of B2B Data Exchange, in the **Conflict Resolution Wizard**, select **Replace**.

In the **Apply this resolution to** list, select **All Conflicts**. Click **Next**.

5. In the Global Copy Options area select the options **Retain Sequence Generator, Normalizer, or XML key current values** and **Retain Persistent Mapping Variable Values**.
6. Follow the instructions in the **Import Wizard** to complete the import of the workflow.

Configure Credentials for Windows Authentication

If you installed any of the B2B Data Exchange repositories on a Microsoft SQL Server and you selected to use Windows authentication, configure the credentials that B2B Data Exchange uses to access the Microsoft SQL Server instance.

Before you start the configuration process, verify that all B2B Data Exchange Windows services are stopped and that the B2B Data Exchange Operation Console and the B2B Data Exchange server are not running.

1. Access the Windows **Services** window.
2. Double-click the service **Informatica B2B Data Exchange Server *version***.

   The B2B Data Exchange Server Properties window appears.
3. Select the **Log On** tab.
4. Select **This account**, click **Browse**, and then specify a user account in the **Select User** dialog box. When you are finished, click **OK**.
5. Type the password for the user account in **Password** and in **Confirm password**, and then click **OK.**
6. Repeat steps 2 through 5 for the service **Informatica B2B Data Exchange Console *version***.

Restart the B2B Data Exchange Services

Restart the B2B Data Exchange Server and other services. For more information, see Chapter 8, “Starting and Stopping B2B Data Exchange” on page 113.

Creating a Portal User Group

When you upgrade the Partners Portal component, create portal user groups in the Operation Console.

Note: If you do not assign a portal user group to a portal user, the portal user can only view the Dashboard in the Partners Portal.

1. In the Navigator, click **Administration** > **Portal User Groups**.

   The **Portal User Groups** page appears.
2. To create a portal user group, click **New User Group**.
3. To assign privileges to a portal user group, in the Privileges tab select the privileges to assign.
   - To assign the portal user role, select **Portal User Role**.
   - To view the Dashboard in the Partners Portal, click **View Dashboard**. Alternatively, to assign all Dashboard privileges, click **Dashboard**.
   - To view the Event List in the Partners Portal, click **View Event List**. Alternatively, to assign all Event List privileges, click **Event List**.
   - You can set the following message profile privileges in the Partners Portal:

     - To view message profiles, click **View Message Profiles**

- To edit message profiles, click **Edit Message Profiles**.
- Alternatively, to assign all privileges, click **Message Profile**.

a. To assign the portal user role, select **Portal User Role**.

Note: You cannot save the portal user group without assigning the portal user role.

b. To view the Dashboard in the Partners Portal, click **View Dashboard**. Alternatively, to assign all Dashboard privileges, click **Dashboard**.

c. To view the Event List in the Partners Portal, click **View Event List**. Alternatively, to assign all Event List privileges, click **Event List**.

d. You can set the following message profile privileges in the Partners Portal:
- To view message profiles, click **View Message Profiles**
- To edit message profiles, click **Edit Message Profiles**.
- Alternatively, to assign all privileges, click **Message Profile**.

e. You can set the following endpoint privileges in the Partners Portal:
- To view endpoints, click **View Endpoints**.
- To edit the password for organization hosted FTP or FTPs endpoints, click **Change Password**.
- Alternatively, to assign all privileges, click **Endpoint**.

f. You can set the following file exchange privileges in the Partners Portal:
- To view file exchanges, click **View File Exchange**.
- To download files from the portal, click **Download Files**.
- To upload files to the portal, click **Upload Files**.
- To delete files on the portal, click **Delete Files**.
- Alternatively, to assign all privileges, click **File Exchange**.

4. Click **Save**.

Assigning a Portal User to a Portal User Group

When you upgrade the Partners Portal component, after you create portal user groups, assign portal users to portal user groups.

1. In the **Navigator**, click **Partner Management** > **Portal Users**.
2. To add the portal user to a user group, in the **User Groups** tab, select a user group from the **Available User Groups** panel and transfer the group to the **Selected User Groups** panel.

   When you assign the portal user to a user group, the portal user obtains all the privileges associated with the user group. You can select more than one user group. If you do not assign a user group, the portal user can only view the Dashboard in the Partners Portal.
3. To save the changes, click **Save**.

Customize the Partners Portal Logo

If you installed the Partners Portal component, you can brand the Partners Portal with the organization logo.

The Partners Portal requires two logo graphic files in .png format, a small logo and a large logo. The file for the small logo must be named `Organization_logo.png` and must be 144 pixels by 50 pixels. The file for the large logo must be named `Login_Organization_logo.png` and must be 170 pixels by 100 pixels. The logo graphics must be transparent.

1. Copy the `Login_Organization_logo.png` file to the following directory: `dx\tomcat\webapps\dx-portal\img\Login_Organization_logo.png`.

   This logo appears in the upper right corner of the Partners Portal login page.

2. Copy the `Organization_logo.png` file to the following directory: `dx\tomcat\webapps\dx-portal\img\Organization_logo.png`.

   This logo appears in the upper right corner of the Partners Portal tabs.

Configure Data Archive

If you are upgrading to the current version, you must configure Data Archive.

1. Close B2B Data Exchange. Do not run any archive jobs related to B2B Data Exchange.
2. Update the dx.archive.jdbc.url, dx.archive.jdbc.username, and dx.archive.jdbc.password properties with the values for the URL, the user name, and the password that you use to access the history database. Update these properties in the `dx-configuration.properties` file located in the directory `<DXInstallationDir>/conf/`. Also update these properties in the `dx-configuration.properties` file located in the directory `<DXInstallationDir>/tomcat/shared/classes/`.
3. Start B2B Data Exchange.

CHAPTER 8

Starting and Stopping B2B Data Exchange

This chapter includes the following topics:

Overview of Starting and Stopping B2B Data Exchange

Stop or start the B2B Data Exchange services.

For example, start the services after you install B2B Data Exchange, or stop the services before you upgrade B2B Data Exchange.

Starting and Stopping B2B Data Exchange on Windows

Start and stop the B2B Data Exchange services from the Start menu or run the startup and shutdown scripts.

The installer creates shortcuts in the Start menu to start and stop all B2B Data Exchange services.

Starting and Stopping B2B Data Exchange from the Start Menu

On Windows operating systems, you can use the Start menu to start and stop all B2B Data Exchange services. You cannot start or stop a single service from the Start menu.

1. In the Start menu, click **Informatica > B2B Data Exchange**.
2. Choose one of the following options:
   - Start Services. Starts all B2B Data Exchange services.

- Stop Services. Stops all B2B Data Exchange services.
- Operation Console. Opens the Operation Console in a Web browser.

Starting and Stopping B2B Data Exchange with Batch Scripts

On Windows operating systems, you can run scripts to start and stop one or more B2B Data Exchange services.

1. Navigate to the following directory:

   ```
   <DXInstallationDir>\bin
   ```

2. Choose the script to run.
   - startup.bat. Starts all B2B Data Exchange services.
   - shutdown.bat. Stops all B2B Data Exchange services.
   - Start each of these services separately in the listed order:
     - activemq.bat. Starts the B2B Data Exchange JMS Broker.
     - mft.bat. Starts the B2B Managed File Transfer service.
     - dxconsole.bat. Starts the Operation Console.
     - dxserver.bat. Starts the B2B Data Exchange server.

Starting and Stopping B2B Data Exchange on Linux

Run the scripts to start or stop the B2B Data Exchange services. The installer creates shell scripts that you can use to start or stop all the B2B Data Exchange services or to start each service separately. You cannot stop each service separately.

1. Navigate to the following directory:

   ```
   <DXInstallationDir>/bin
   ```

2. Choose the script to run.
   - startup.sh. Starts all B2B Data Exchange services.
   - shutdown.sh. Stops all B2B Data Exchange services.
   - Start each of these services separately in the listed order:
     - activemq.sh. Starts the B2B Data Exchange JMS Broker.
     - mft-server.sh. Starts the Informatica Managed File Transfer service.
     - mft.sh. If you upgraded B2B Data Exchange and installed the Managed File Transfer, this command starts the Managed File Transfer service.
     - dxconsole.sh. Starts the Operation Console.
     - dxserver.sh. Starts the B2B Data Exchange server.

CHAPTER 9

Optional B2B Data Exchange Configuration

This chapter includes the following topics:

Optional B2B Data Exchange Configuration Overview

Optional configuration includes tasks that you might want to perform after you install or upgrade B2B Data Exchange, or at a later date.

- The B2B Data Exchange components send information through ports. You can change the default port numbers based on the requirements of your network environment.
- When different components process information or encounter errors, log files contain information that you can use to analyze and troubleshoot the installed components. You can change the location of the log files or define custom logs.
- To increase performance and reliability, you can change the maximum memory allocation for the B2B Data Exchange JMS Broker service, the embedded B2B Data Exchange server broker, or the embedded B2B Data Exchange console broker.

- If you change the database user credentials for the B2B Data Exchange repository or for the operational data store, you must update the B2B Data Exchange configuration files. If you are running the Dashboard and Reports component, you must also update the relevant PowerCenter connections.
- If you use the Dashboard and Reports component, and the IP addresses of the machine that hosts B2B Data Exchange change any time after the installation, you must update the IP addresses in the dashboard configuration file.
- For the B2B Data Exchange Dashboard and Reports component, you can specify a user name, password, and location for the operational data store user account.
- During the B2B Data Exchange installation or upgrade, you define a PowerCenter Integration Service that B2B Data Exchange uses to run workflows. If required, you can configure a different PowerCenter Integration Service to access B2B Data Exchange.
- If you use the Dashboard and Reports component, your B2B Data Exchange and operational data store repositories are installed on Microsoft SQL Servers, and you use PowerCenter version 10, configure the repository connections in PowerCenter Workflow Manager.
- If you want to change JMS broker communication settings, configure attributes to modify control of the JMS broker.
- To use the Active MQ Web Console to troubleshoot JMS broker communications, access the Active MQ Web Console, then use the predefined username and password.
- If you installed the Informatica Managed File Transfer component, perform the following procedures:
  - Configure the relevant B2B Data Exchange system properties and restart B2B Data Exchange before you try to access Informatica Managed File Transfer from the Operations Console.
  - You must enable SSO with Informatica Managed File Transfer before you try to access Informatica Managed File Transfer from the Operations Console. To enable SSO, copy the keystore from the Informatica Managed File Transfer server and the install an SSO key on the B2B Data Exchange server.
  - Share the B2B Data Exchange download directory and the Informatica Managed File Transfer Web User directories with both B2B Data Exchange and Informatica Managed File Transfer Web.
  - If you create a custom project in Informatica Managed File Transfer, ensure that you include specific variables to pass information from B2B Data Exchange system properties.
- Before you create endpoints that run Informatica Intelligent Cloud Services tasks, ensure that you have an active account and license, and are assigned the appropriate user roles.

Modifying Port Numbers

You can modify the port numbers that B2B Data Exchange uses to send and receive information.

You can modify the numbers of the following ports:

- B2B Data Exchange server startup and shutdown port
- B2B Data Exchange server RMI port
- JNDI provider port

Modifying the B2B Data Exchange Server Startup and Shutdown Port Number

On Windows operating systems, edit the Java Service Wrapper file to configure the B2B Data Exchange server to use a different port. On UNIX and Windows operating systems, run the dxserver command line utility with the different port number.

When you start the B2B Data Exchange server with a different port number, you must use the same port number when you ping or shut down the B2B Data Exchange server.

1. On Windows operating systems, edit the Java Service Wrapper file.
   a. On the machine where B2B Data Exchange is installed, open the wrapper.conf file in a text editor from the following directory:
      `<DXInstallationDir>/conf`
   b. Search for the following text:
      `wrapper.app.parameter.2=start`
   c. Add the following line below the text:
      `wrapper.app.parameter.3=<PortNumber>`
   d. Replace the <PortNumber> value with the port number that you want to use.
   e. Save the wrapper.conf file.
2. On Windows and UNIX operating systems, run the following command to restart the B2B Data Exchange:
   - Windows: `dxserver.bat start <PortNumber>`
   - UNIX: `dxserver.sh start <PortNumber>`

Modifying the B2B Data Exchange Server RMI Port Number

Replace the RMI port number in the dx-configuration.properties files and in the PowerCenter Integration Service.

1. On the machine where B2B Data Exchange is installed, open the server and console copies of the dx-configuration.properties files in a text editor from the following locations:
   `<DXInstallationDir>/conf/`
2. Enter the port number in the following property:
   `dx.rmi.port=`
3. Save the dx-configuration.properties files.
4. In the Administrator tool, select the PowerCenter Integration Service that runs B2B Data Exchange transformations.
5. On the Processes tab of the PowerCenter Integration Service, add or edit the DX_SERVER_URL environment variable and set the URL of the B2B Data Exchange server in the following format:
   `rmi://<HostName>:<PortNumber>`
6. Save the changes and restart the B2B Data Exchange services.

After you change the RMI port number, make sure you use it when you run the command line utilities. For example, to use the port number when you import, export, or archive B2B Data Exchange repository objects, run the command line utilities with the following options:

- Import: `importexport -c import -f <ExportFile> -s <SpecificationFile> -u <UserID> --server <"HostName:PortNumber">`

- Export: `importexport -c export -f <ExportFile> -s <SpecificationFile> -u <UserID> --server <"HostName:PortNumber">`
- Archive: `archive -s <SpecificationFile> -u <UserID> --server <"HostName:PortNumber">`

Note: You may encounter B2B Data Exchange performance and stability issues when using the basic archive command line utility in B2B Data Exchange. It is recommended to use the Data Archive utility for archiving high volumes of event data in production.

Modifying the JNDI Provider Port Number

PowerCenter uses the JNDI provider to find the JMS queues that B2B Data Exchange uses to send and receive messages. When you change the JNDI port number, change it in the B2B Data Exchange workflow connection objects in PowerCenter and in the dx.endpoint.jms.provider.url B2B Data Exchange system property. If you use JMS endpoints, also change the port number in the activemq.xml file and in the JMS endpoint properties.

1. In the Workflow Manager, update the port number in the JNDI Provider URL attribute of the JNDI connection object for all B2B Data Exchange workflows.
2. In the Operation Console, click **Administration** > **System Properties**.

   The **System Properties** page appears.
3. In the dx.endpoint.jms.provider.url, change the port number in the property value.

   The following example shows the property value with the default port number:

   ```
   failover:tcp://localhost:18616
   ```
4. In the Operation Console, click **Partner Management** > **Endpoints**.

   The **Endpoints** page appears.
5. In each JMS Send or JMS Receive endpoint, change the port number in the value of the Provider URL property.
6. On the machine where B2B Data Exchange is installed, open the activemq.xml file in a text editor from the following directory:

   ```
   <DXInstallationDir>\message-broker\conf\
   ```
7. In the <transportConnectors> element, change the port number for the URL attribute of the openwire connector.

   The following example shows the URL with the default port number:

   ```
   <transportConnector name="openwire" uri="tcp://localhost:18616" />
   ```
8. Save the activemq.xml file.

Logs

The B2B Data Exchange log files include information that you can use to analyze activity and troubleshoot.

You can configure the following logs:

- Debug logs
- RMI server logs
- Database debug logs

- Import logs

To send log messages to a different log file destination, you can create an SNMP appender to redirect the logs to a custom destination.

Default Log Files

B2B Data Exchange creates log files that record diagnostic information regarding system and user operations. The installer also creates log files that record installation selections and configuration.

You can configure log settings in the log4j.xml file located in the B2B Data Exchange configuration directory.

The following log files are available:

Server

The dxserver.log file is located in the following directory:

```
<DXInstallationDir>/logs
```

You can change the log mode to debug to generate more messages while you troubleshoot server issues.

Operation Console

The log files are located in the following directory:

Managed File Transfer

The log files are located in the following directory:

```
<DXInstallationDir>\ManagedFileTransfer\logs
```

The following logs include Managed File Transfer server error information:

- System XML log file (`VLTrader.xml`)
- System debug file (`VLTrader.dbg`)

JMS Broker

The log files are located in the following directory:

```
<DXInstallationDir>\message-broker\data\
```

The log4j.properties configuration file are located in the following directory:

```
<DXInstallationDir>\message-broker\
```

Installer

The log files are located in the following directory:

```
<DXInstallationDir>/logs
```

Customizing the Destination for Log Messages

By default, the log4j logging utility sends log messages to files. You can configure the log4j utility to send log messages to a destination that is different from the default log files with the Simple Network Management Protocol (SNMP). The installer installs the file that the log4j utility requires to work with SNMP.

Complete the following tasks to change the destination:

1. Add an SNMP appender to the log4j properties file and set the logging level. Change the sample SNMP appender in the log4j.xml file to the appender that you want to use. You can add multiple appenders to the log4j.xml file that send different types of log messages to different SNMP outputs.

2. Configure an SNMP manager to listen for messages. For information about configuring the SNMP manager to handle log4j messages, see the documentation for your SNMP network management software.

For general information about the log4j utility, see the Apache Web site:
http://logging.apache.org/log4j/1.2/manual.html

SNMP Appender Parameters

The parameters of the SNMP appender in the log4j.xml file define the output destination and settings for log messages.

The following table describes the SNMP parameters that you can define for B2B Data Exchange:

Parameter	Description
ManagementHost	IP address of the monitoring system host. Default is **127.0.0.1**
ManagementHostTrapListenPort	Port number of the monitoring system host. Default is **162**
LocalIPAddress	IP address of local SNMP embedded agent. You do not normally need to modify this value. Default is **127.0.0.1**
LocalTrapSendPort	Port number of the local SNMP embedded agent. Default is **161**
CommunityString	Name of the SNMP community. Default is **public**
GenericTrapType	Type of the trap. Set one of the following values: - 0=cold start - 1=warm start - 2=link down - 3=link up - 4=authentication failure - 5=egp neighbor loss - 6=enterprise specific Default is **6=enterprise specific**
ApplicationTrapOID	Identifier of the application object that sends the trap messages. You can set the value of this parameter to the name of the application object in B2B Data Exchange. Default is **1.3.6.1.2.1.2.0.0.0.0**
EnterpriseOID	Identifier of the organization object sending the trap message. You can set this parameter to any value that identifies the message in B2B Data Exchange. Default is **1.3.6.1.2.1.2.0**
ForwardStackTraceWithTrap	Determines whether to include the stack trace in the log message. Default is **False**

Parameter	Description
Threshold	Level of details to report. Set one of the following values: - FATAL - ERROR - WARN - INFO - DEBUG Threshold values that are lower than INFO or WARN might cause heavy network traffic. For fewer notifications, set the threshold value to FATAL. For a larger number of notifications, set the threshold value to WARN.
SysUpTime	Amount of time that the application is running. Set the value to 0 to calculate the system up time when a message is sent. Default is **0**

Adding an SNMP Appender to the log4j.xml File

Add an SNMP appender to the B2B Data Exchange server or Operation Console copies of the log4j.xml file to customize the output destination for log messages.

1. Back up the log4j.xml file that you want to edit from one of the following locations:
   - B2B Data Exchange server: `<DXInstallationDir>/conf`
   - Operation Console: `<DXInstallationDir>/DataExchange/tomcat/shared/classes`
2. Open the file in a text editor and search for the following text:

   ```
   SNMP_TRAP is a sample appender
   ```
3. To edit the sample appender with the actual values of your appender, remove the comment indicators from the SNMP_TRAP appender and edit the appender parameters and values based on your requirements.

   Note: You can also add an appender below the sample appender instead of editing the sample appender.
4. To set the formatting of the log messages, edit the layout element.

   The following example shows the layout element of the sample appender:

   ```
   <layout class="org.apache.log4j.PatternLayout">
      <param name="ConversionPattern" value="%d{ISO8601} %-5p [%c] {%t} %m%n"/>
   </layout>
   ```

   For information about the layout pattern options, see the description on the Apache Website: http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/PatternLayout.html
5. To activate the appender, search for the following text:

   ```
   <root>
   ```
6. Add the appender name to the appender list.

   The following example shows the appender list after you add the appender name:

   ```
   <root>
      <priority value="INFO"/>
      <appender-ref ref="BROKER-LOG"/>
      <appender-ref ref="CONSOLE"/>
      <appender-ref ref="SNMP_TRAP"/>
   </root>
   ```
7. Save the log4j.xml file.

After you add the SNMP appender, configure your SNMP manager to listen for the log messages.

Changing the Maximum Java Heap Size

You can change the maximum memory allocation for the B2B Data Exchange JMS Broker service, the embedded B2B Data Exchange server broker, or the embedded B2B Data Exchange console broker.

B2B Data Exchange JMS Broker

To change the maximum Java heap size of the B2B Data Exchange JMS Broker, open one of the following files:

Operating System	File Location
Microsoft Windows	<DXInstallationDir>\bin\setenv.bat
UNIX	<DXInstallationDir>/bin/setenv.sh

Change the maximum heap size in MB in the ACTIVEMQ_OPTS property. The default maximum heap size is 512 MB.

Embedded B2B Data Exchange server broker

To change the maximum Java heap size of the embedded B2B Data Exchange server broker, open one of the following files:

Operating System	File Location
Microsoft Windows	<DXInstallationDir>\bin\setenv.bat
UNIX	<DXInstallationDir>/bin/setenv.sh

Change the maximum heap size in MB in the DX_SERVER_OPTS property. The default maximum heap size is 1024 MB.

Embedded B2B Data Exchange client broker

To change the maximum Java heap size of the B2B Data Exchange client, open one of the following files:

Operating System	File Location
Microsoft Windows	<DXInstallationDir>\bin\setenv.bat
UNIX	<DXInstallationDir>/bin/setenv.sh

Change the maximum heap size in MB in the CATALINA_OPTS property. The default minimum heap size is 128 MB and the default maximum heap size is 2048 MB.

B2B Data Exchange JMS Broker service

To change the maximum Java heap size of the B2B Data Exchange JMS Broker service on Microsoft Windows operating systems, open the following file:

```
<DXInstallationDir>\message-broker\bin\win32\wrapper.conf
```

Change the maximum Java heap size in MB in the wrapper.java.maxmemory property. The default maximum heap size is 512 MB.

B2B Data Exchange server service

To change the maximum Java heap size of the B2B Data Exchange server service on Microsoft Windows operating systems, open the following file:

```
<DXInstallationDir>\conf\wrapper.conf
```

Change the maximum heap size in MB in the wrapper.java.maxmemory property. The default maximum heap size is 1024 MB.

B2B Data Exchange client service

To change the maximum Java heap size of the B2B Data Exchange client service on Microsoft Windows operating systems, run the following command:

```
<DXInstallationDir>\DataExchange\tomcat\bin\tomcat7.exe //US//InfaDXOpConsole<version> --
JvmMx <max_heap_size>
```

Enter the maximum heap size in MB with integers and without letters. The default maximum heap size is 2048 MB.

Changing the Credentials for a Database User Account

When you install B2B Data Exchange, you specify a user name and a user password for the user account of the B2B Data Exchange repository database. If you are running the Dashboard and Reports component, you also specify a user name and a user password for the operational data store user account.

Perform the following steps if you change the credentials for a database user account after you install B2B Data Exchange. Perform only the steps that are relevant to the changes that you are making. If you are not running the Dashboard and Reports component, skip the steps that are only relevant to this component.

1. Stop the B2B Data Exchange services and close the Operation Console.
2. Verify that the PowerCenter Integration Service is not running any B2B Data Exchange workflows.
3. If you are running the Dashboard and Reports component, and you are changing credentials for the B2B Data Exchange repository or for the operational data store user account, use the PowerCenter Workflow Manager to update the credentials in the following connections:
   - For the B2B Data Exchange repository, update the DX_REPO connection.
   - For the operational data store, update the DX_ODS connection.
4. If you are changing a password, perform the following steps:
   a. Run the password encryption utility and enter the new password in the following syntax:
      - On Windows operating systems: `<DXInstallationDir>\dx-tools\dxpasswd.bat -p <NewPassword>`
      - On UNIX operating systems: `<DXInstallationDir>/dx-tools/dxpasswd.sh -p <NewPassword>`

      The password encryption utility encrypts the password and displays an encrypted string. For example, `--><encrypted_string><--`.
   b. Copy the encrypted string without the `--><--` indicators to the clipboard.

5. Open both copies of the `dx-configuration.properties` file from the following locations in a text editor:

   ```
   <DXInstallationDir>/DataExchange/tomcat/shared/classes/
   <DXInstallationDir>/conf/
   ```

6. In both copies of the `dx-configuration.properties` file, perform the following steps:
   a. Search for the text that is relevant to the changes that you are making:
      - B2B Data Exchange repository:

        ```
        dx.jdbc.username=<CurrentUsername>
        dx.jdbc.password=<CurrentPassword>
        ```

      - Operational data store:

        ```
        dx.dashboard.jdbc.username=<CurrentUsername>
        dx.dashboard.jdbc.password=<CurrentPassword>
        ```

   b. Replace the relevant value with the new value. If you are replacing a password, enter the encrypted string.
   c. Save and close the files.

   Note: The content in both copies of the `dx-configuration.properties` file must be identical.
7. Start the B2B Data Exchange Operation Console.
8. If you are changing the credentials for the operational data store user account, perform the following steps:
   a. In the Navigator click **Administration** > **System Properties**.
   b. Change the values of the `dx.dashboard.jdbc.username` and the `dx.dashboard.jdbc.password` properties to the new values. For the password, enter the encrypted string.
9. Verify that the PowerCenter Integration Service is running.
10. Start the B2B Data Exchange Server service.
11. If you are running the Dashboard and Reports component, perform the following steps to schedule the B2B Data Exchange operational data store loader workflow:
    a. In PowerCenter Workflow Manager, expand the folder where the operational data store loader workflow is located and then right-click **DX_ETL**.
    b. Select **Schedule** from the menu and wait until PowerCenter Workflow Manager schedules and runs the workflow.

Updating the Dashboard Configuration File

If you use the Dashboard and Reports component, and the IP addresses of the machine that hosts B2B Data Exchange change any time after the installation, you must update the IP addresses in the dashboard configuration file.

1. Open the dashboard configuration file from the following location:

   ```
   <DXInstallationDir>\DataExchange\tomcat\shared\classes\dx_dashboard_configuration.xml
   ```

2. In the Security section, in the `AuthenticationClientAddresses` attribute, update the IP addresses of all the Network Interface Cards that provide access to the machine that hosts B2B Data Exchange, including both IPv4 and IPv6 addresses. For example:

   ```
   <Security AuthenticationSource="SecureKey" SecurityEnabled="True"
   AuthenticationClientAddresses="127.0.0.1,0:0:0:0:0:0:0:1,10.36.8.34,fe80:0:0:0:c1f:
   ```

```
167a:bc3c:8307%11,10.36.112.186,fe80:0:0:0:5c9a:af6e:
87b9:3c08%12,fe80:0:0:0:7c26:627:71d2:4784%14,fe80:0:0:0:0:5efe:a24:822%16,fe80:0:0:0
:0:5efe:a24:70ba%16,fe80:0:0:0:0:5efe:c0a8:7701%17,192.168.119.1,fe80:0:0:0:45cf:
7bcf:f673:4392%18,192.168.162.1,fe80:0:0:0:3516:cd0c:
6f8:df39%19,fe80:0:0:0:0:5efe:c0a8:a201%20" RestartSession="False"
CacheRights="Session" LogonFailPage="https://HBW180084:18443/dx-console/logout.jsp">
```

3. Restart the B2B Data Exchange services.

Configuring a PowerCenter Integration Service to Access B2B Data Exchange

During the B2B Data Exchange installation or upgrade, you define a PowerCenter Integration Service that B2B Data Exchange uses to run workflows. If required, you can configure a different PowerCenter Integration Service to access B2B Data Exchange.

In the Java classpath for the PowerCenter Integration Service, add the path to the B2B Data Exchange class files.

1. Log in to the Administrator tool and select the PowerCenter Integration Service that runs the workflows for B2B Data Exchange.
2. On the **Processes** tab, edit the Java SDK ClassPath property and add the location of the B2B Data Exchange Java classes at the beginning of the ClassPath property:

   ```
   <DXInstallationDir>/powercenter/lib/dx-client-powercenter-10.2.3.jar;
   <DXInstallationDir>/powercenter/lib/commons-logging-1.1.3.jar;
   <DXInstallationDir>/powercenter/lib/log4j-1.2.17.jar;
   <DXInstallationDir>/powercenter/lib/activemq-all-5.12.1.1.jar
   ```

   Note: You can reference the libraries if the you can access the `<DXInstallationDir>` from PowerCenter, or you can copy the library files locally.
3. Add environment variables to the B2B Data Exchange console and server integration services.

Integration Service	Environment Variable
DX_CONSOLE_URL	`rmi://<HostName>:<dx.tpm.rmi.port>`
DX_SERVER_URL	`rmi://<HostName>:<dx.rmi.port>`

   You can find the RMI port numbers for the console and server in the following location:

   ```
   <DXInstallationDir>\conf\dx-configuration.properties
   ```

   By default:

   - `dx.tpm.rmi.port`: 18096
   - `dx.rmi.port`: 18095
4. Save the changes.

Configuring Repository Connections on PowerCenter Version 10

If you use the Dashboard and Reports component, your B2B Data Exchange and operational data store repositories are installed on Microsoft SQL Servers, and you use PowerCenter version 10, configure the repository connections in PowerCenter Workflow Manager.

1. In the Workflow Manager, access the DX_REPO database connection and open the **Connection Object Definition** dialog box.
2. Perform the following actions and then click **OK**:
   a. Select **Use DNS**.
   b. In the **Connect String** text box enter the connection name. The name is defined in the ODBC Data Source Administrator interface, in ODBC SQL Server Wire Protocol Setup, in the **Data Source Name** field.
3. Repeat steps 1 and 2 for the DX_ODS connection.

Configuring the B2B Data Exchange JMS Broker

To configure the JMS communications broker, modify attributes and elements in the `activemq.xml` file. The file is located in the following folder: `<DXInstallationDir>\message-broker\conf\`

Modify the **memoryLimit** attribute to determine the maximum memory allocation for message transfer. You can increase the memory limit if you expect a large number of queues and messages or higher message volume. You can modify the memory limit for the following elements:

- policyEntry topic
- policyEntry queue

The default value is 20 MB.

To troubleshoot message communication issues, you can instruct the JMS Broker to open the administrator console when you start the B2B Data Exchange services.

The **jetty.xml** import element appears with the following syntax:

```
<!--
<import resource="jetty.xml"/>
-->
```

To access the administrator console, remove the comment indicators around the element and restart the B2B Data Exchange services.

If you use a JMS source, ensure that the PowerCenter workflow source property **Transacted Mode** is set to **Yes**.

1. Select to edit the workflow.
2. In the Mapping tab, select the source. In the Attributes section, change the value of the property **Transacted Mode** to **Yes**.

Activating the ActiveMQ Web Console

The ActiveMQ Web Console is a troubleshooting tool that can be used to debug JMS broker communication issues for B2B Data Exchange.

By default, the ActiveMQ Web Console is disabled. To enable the web console, in the `activemq.xml` file located in the directory `<DXInstallationDir>\message-broker\conf\`, un-comment the following section:

```
<import resource="jetty.xml"/>
```

After you activate the ActiveMQ Web Console, use the following user name and password to access the ActiveMQ Web Console:

Access Setting	Value
user name	admin
password	admin

Configure System Properties to Enable Informatica Managed File Transfer Access

If you install the Informatica Managed File Transfer component, to ensure that B2B Data Exchange can access Managed File Transfer, define the following system properties with the Operations Console:

System Property	Description
infamft.api.username	Name of a user from a user account with privileges to run Informatica Managed File Transfer projects. The credential is used to execute Informatica Managed File Transfer projects.
infamft.api.password	Password of the user defined for the **infamft.api.username** property. The credential is used to execute Informatica Managed File Transfer projects.
infamft.console.url	URL address for Informatica Managed File Transfer.

After you edit the system properties, restart B2B Data Exchange.

Installing a Single Sign On Key

Single Sign On (SSO) uses a symmetric key that applications share. After you install Informatica Managed File Transfer, you create a master key with the Informatica Managed File Transfer `mft-keytool` utility. Specify the keygen, keystore, and key passphrases. Next, use the master key to enable SSO with B2B Data

Exchange. After you enable SSO, you can launch Managed File Transfer from the B2B Data Exchange Operation console.

To create an SSO key for Informatica Managed File Transfer, see the *Informatica Managed File Transfer Installation Guide*. After you create the SSO key for Informatica Managed File Transfer, perform the following steps:

Note: In order to launch Managed File Transfer from the B2B Data Exchange Operation console you must enable Informatica domain authentication for both Managed File Transfer and B2B Data Exchange

1. Copy the generated Informatica Managed File Transfer keystore file `keystore.jceks` from the directory `<MFT_INSTALL_DIR>\mft\config\security` on the Informatica Managed File Transfer server to the B2B Data Exchange server.
2. To isntall an SSO key, run the `install-ssokey.bat` tool in Windows or the `install-ssokey.sh` tool in Linux based systems on the B2B Data Exchange server. Run a command with the following syntax:

   ```
   -c installMftSSOKey -f <keyStoreFileName> -kp <keyPassOption> -ksp <keyStorePassOption>
   ```

   -c installMftSSOKey

   Required. Installs the SSO key.

   -kp <Key Passphrase>

   Required. Specify a passphrase from 7 to 255 characters that will access the SSO encryption key. The passphrase is the same one that you specified when you created the key on the Informatica Managed File Transfer server.

   -ksp <Keystore Passphrase>

   Required. Specify a keystore passphrase from 7 to 255 characters that will access the SSO keystore. The passphrase is the same one that you specified when you created the keystore on the Informatica Managed File Transfer server.

   -f <Keystore File Name>

   Required. Specify the path to the keystore file that you copied from the Informatica Managed File Transfer server.
3. Stop the B2B Data Exchange services and close the Operation Console, and then restart the services. For more information, see "Starting and Stopping B2B Data Exchange on Linux" on page 114
4. For multiple B2B Data Exchange servers in high availability mode, follow the same procedure to install the key separately on each node.

Sharing Informatica Managed File Transfer Directories with B2B Data Exchange

Use Informatica Managed File Transfer to configure client and server machines that serve as B2B Data Exchange endpoints. If you install the Managed File Transfer component, to ensure that endpoints function correctly, share the relevant Managed File Transfer directories with B2B Data Exchange.

Before using an MFT Remote Receive or MFT Hosted Receive endpoint that runs a project, you must share the Informatica Managed File Transfer download directory. Share the Managed File Transfer directory specified in the B2B Data Exchange system property named `infamft.download.location` with B2B Data Exchange.

Before using an MFT Hosted Receive or MFT Hosted Send endpoint, share the Managed File Transfer directory `<MFT installation>\server\userdata\webdocs` with B2B Data Exchange.

Adding Variables to Custom Informatica Managed File Transfer Projects

You can use pre-configured Informatica Managed File Transfer projects to define communication protocols and file management processes for B2B Data Exchange MFT endpoints. If you choose to create a custom project, ensure that you include the following variables.

For an MFT Hosted Receive endpoint that runs a custom project, the source directory is specified with a variable starting with `InputFile`. For example, you could include the variable `${InputFile_DXData}` in the custom project to pass the source directory path to B2B Data Exchange.

For an MFT Hosted Send endpoint that runs a custom project, the destination file is specified with the variable `${OutputFile_DXData}` in the project.

Informatica Intelligent Cloud Services Configuration

Before you can use Data Integration to create and run tasks, ensure that you have an active Informatica Intelligent Cloud Services account, have defined user roles through the Administrator, and have a relevant Informatica Intelligent Cloud Services license.

You must have the following user roles assigned to your Informatica Intelligent Cloud Services account to create and run Data Integration tasks with B2B Data Exchange:

- Data Integration Task Executor
- Data Review
- Data Viewer
- Deployer
- Designer
- Monitor
- Operator
- Service Consumer

Ensure that the Secure Agent is installed on the same host machine as B2B Data Exchange.

CHAPTER 10

Migrating OEM Managed File Transfer Endpoint

This chapter includes the following topics:

Migrating OEM Managed File Transfer Endpoint Overview

When you upgrade B2B Data Exchange and install Informatica Managed File Transfer, you can use the Informatica migration tool to migrate OEM Managed File Transfer endpoint configuration for numerous endpoints to Informatica Managed File Transfer. You can use the migration tool to create Informatica Managed File Transfer endpoints in B2B Data Exchange for both hosted and remote servers. With the migration tool you can migrate OEM endpoint configuration for FTP, FTPS, HTTP, HTTPS, and AS2 endpoints.

Alternatively, you can manually migrate OEM migration configuration data. To do so, you create Informatica Managed File Transfer endpoints in B2B Data Exchange and configure endpoints in accordance with OEM Managed file Transfer Endpoint settings. If you have only one or a few endpoints, you might choose to manually migrate the configuration data.

Migration with the Migration Tool

You can use the Informatica migration tool to migrate OEM Managed File Transfer endpoint configuration data to Informatica Managed File Transfer endpoints in B2B Data Exchange.

You can select to migrate endpoints for a specific partner, a list of partners, or all partners. Run the migration tool through the command line interface. The migration process creates endpoints that are associated with specific partners.

For each partner that you specify, the migration tool fetches associated OEM endpoints and their configuration data and creates Informatica Managed File Transfer objects. The migration tool creates Informatica Managed File Transfer resources, connections, and web users in B2B Data Exchange and Informatica Managed File Transfer.

An OEM host and mailbox corresponds to a resource in Informatica Managed File Transfer. When the migration tool migrates a host and mailbox combination, the migration tool creates a corresponding resource in Informatica Managed File Transfer. The migration tool migrates mailbox passwords automatically.

For an OEM endpoint that is connected to a server hosted in a partner environment, the migration tool creates an MFT Remote Receive endpoint and an MFT Remote Send endpoint. For an OEM endpoint where the partner connects to the organization server, the migration tool creates an MFT Hosted Receive endpoint and an MFT Hosted Send endpoint.

The Send endpoint is assigned the same name as the original OEM endpoint. The Receive endpoint is provided a name with the format `<prefix>_<original OEM endpoint name>`, where the prefix can be customized in the migration configuration file. The OEM endpoint that has been migrated is renamed in the format `OEM_MFT_<original OEM endpoint name>`. If the migrated OEM outbound endpoint was the default endpoint for an account, the account is updated and the generated send endpoint is designated the default outbound endpoint.

All the common fields for the OEM Managed File Transfer endpoint and the Informatica Managed File Transfer endpoint are copied to the created endpoint without change, for example, read patterns, schedules, and backup options.

An OEM mailbox contains a set of actions that are performed for files to be sent or received. Each OEM Managed File Transfer host and mailbox has a set of properties which can be used to customize file transfer. For example, a native command can be run to post a file transfer (inbound or outbound) by setting the corresponding host property. For Informatica Managed File Transfer endpoints, the endpoints are associated with projects instead that perform actions for files to be sent or received.

The generated Informatica Managed File Transfer endpoints are provided template projects. To support the OEM scenarios, the template projects have corresponding variables that are defined using the values from the OEM Managed File Transfer host and mailbox. Host and mailbox properties are mapped to the corresponding Informatica Managed File Transfer project variables and populated during endpoint migration.

Before You Begin

Before you migrate endpoints with the migration tool, ensure that you have installed the following versions:

- B2B Data Exchange version 10.2.1.
- Informatica Managed File Transfer version 10.2.1.

Ensure that you upgrade B2B Data Exchange and install Informatica Managed File Transfer on the same machine where OEM Managed File Transfer is installed. Do not uninstall OEM Managed File Transfer before you perform the upgrade. The migration tool `mftMigrationTool` is automatically installed during the upgrade procedure in the directory `<B2B Data Exchange Installation>/DataExchange/dx-tools`.

Ensure that the following services are running:

- DX-Console
- DX-Server
- OEM Managed File Transfer service
- Informatica Managed File Transfer server

Before you run the migration tool, configure the migration configuration file named `migration.conf` located in the directory `<B2B Data Exchange Installation>\dx-tools\mftMigration`. For more information, see "Migration Configuration File Parameters" on page 132.

Migration Configuration File Parameters

Before you run the migration tool, configure the migration configuration file named `migration.conf`, located in the directory `<B2B Data Exchange Installation>\dx-tools\mftMigration`.

The following table describes the parameters that you can configure in the migration configuration file:

Parameter	Description
oemmft.install.home	Installation directory of OEM Managed File Transfer.
migration.transportType	Specify the transport type specification of the resources and endpoints to be migrated. The following options are available: - ftp - ftps - sftp - http - https - as2 - all For example, if you specify `ftp` then FTP resources and endpoints are migrated. Specify `-all` to migrate all transport types.

Parameter	Description
migration.partnerName	Specify one or more partners whose resources and endpoints are to be migrated. For more than one partner, provide names of partners separated by commas. To migrate resources and endpoints for all partners, specify `-all`.
mapping.file.location	Specify the directory for the mapping files that the migration tool uses. Default: `<B2B Data Exchange Installation>\dx-tools\mftMigration \<transport type>` Each transport type has a subdirectory with the specific mapping files for the protocol. There is a separate subdirectory that contains the single hosted project mapping file. For hosted endpoints, the same project is shared across all transport types.
infamft.endpoint.prefix	Specify a prefix for the endpoints for inbound connections that the migration process creates. Default: `INFA_MFT_`
infamft.webuser.password	Specify a default password that the migration process assigns to all migrated web users. The password must align with the password policy that you create for Informatica Managed File Transfer.
migrate.nonDx.mailboxes	Specify if to migrate OEM Managed File Transfer mailboxes that are not associated with B2B Data Exchange. The following options are available: - true. Migrate non-B2B Data Exchange mailboxes. - false. Do not migrate non-B2B Data Exchange mailboxes.
migrate.sshftp.as.sftp.task	Specify if the endpoints created for SSH FTP should be of SSH FTP type or SCP type. The OEM MFT endpoints of SSH FTP type can be associated with three different types of Informatica Managed File Transfer tasks - an SFTP Task, an SCP Task and an Execute SSH Command Task. The template projects that the migration process uses include just one type of task to transfer files. The template projects do not support the Execute SSH Command Task. The template project can use either an SFTP task or SCP task, in accordance to the value of this parameter. The following options are available: - true. Use the SFTP task in the migration process. - false. Use the SCP task in the migration process.
infamft.api.url	Specify the URL used to access Informatica Managed File Transfer. Default: `http://localhost:8000/informaticamft`
infamft.api.username	Specify the user account with which to access Informatica Managed File Transfer. The migration tool uses this account to create resources and other objects in Informatica Managed File Transfer. Default: `Administrator`
infamft.api.password	Specify the password with which to access Informatica Managed File Transfer. Use the password for the user account specified with the `infamft.api.username` parameter.
dxconsole.api.url	Specify the URL used to access the B2B Data Exchange Operations Console. Default: `http://localhost:18080/dx-console`

Parameter	Description
dxconsole.api.username	Specify the user account with which to access B2B Data Exchange. Default: `sys`
dxconsole.api.password	Specify the password with which to access B2B Data Exchange. Use the password for the user account specified with the `dxconsole.api.username` parameter.

Migration Tool Commands and Syntax

To run the migration tool, use the following command line syntax:

```
-c <command> -f migration.conf [-mf <mapping file name>] [-pf <private key properties file name>]
```

-c, --command <command>

Required. The following table describes the commands that you can run:

System	Requirement
migrateResources	Migrate OEM Managed File Transfer connections to Informatica Managed File Transfer and B2B Data Exchange.
migrateWebUsers	Migrate OEM Managed File Transfer web users to Informatica Managed File Transfer and B2B Data Exchange.
migrateEndpoints	Migrate OEM Managed File Transfer endpoints to Informatica Managed File Transfer and B2B Data Exchange.
migrateResoucesAndEndpoints	Migrate OEM Managed File Transfer connections and remote endpoints to Informatica Managed File Transfer and B2B Data Exchange.
migrateWebUsersAndEndpoints	Migrate OEM Managed File Transfer web users and hosted endpoints to Informatica Managed File Transfer and B2B Data Exchange.
migrateCertificatesAndKeys	Migrate OEM Managed File Transfer certificates and keys endpoints to Informatica Managed File Transfer and B2B Data Exchange.
migrateAll	Migrate OEM Managed File Transfer certificates, keys, connections, web users, and endpoints to Informatica Managed File Transfer and B2B Data Exchange.

-f, --config <migration configuration file name>

Required. Specify the name of the migration configuration file.

-mf, --mappingFile <mapping file name>

Required when you use the command `migrateEndpoints`. Specify the name of the resource and web user mapping file to be used by the migration process.

-pf, --privateKeyPropertiesFile <private keys property file name>

Required when you use the command `migrateCertificatesAndKeys` or `migrateAll`. Specify the certificate alias to the private key passphrase mapping file to be used by the migration process.

Endpoint Migration

You can use the migration tool to create endpoints in Informatica Managed File Transfer and B2B Data Exchange.

Use the `migrateEndpoints` command to migrate OEM Managed File Transfer endpoints to Informatica Managed File Transfer endpoints.

For each OEM endpoint, the migration tool creates an MFT Receive endpoint and an MFT Send endpoint.

All the common fields for the OEM Managed File Transfer endpoint and the Informatica Managed File Transfer endpoint are copied to the created endpoint without change, for example, read patterns, schedules, and backup options.

Web User Migration

You can use the Informatica migration tool to create web users in Informatica Managed File Transfer and B2B Data Exchange.

For Local Listener hosts in OEM Managed File Transfer, each mailbox represents a user. Use the `migrateWebUser` command to migrate the mailboxes associated with Local Listeners to web users in Informatica Managed File Transfer. The migration process creates web users using the default `webuser` template in Informatica Managed File Transfer.

You can set a default password that the migration process assigns to these web users. This default password can be configured in the migration configuration file with the parameter `infamft.webuser.password`.

Web User and Endpoint Migration

You can use the migration tool to create web users and hosted endpoints in Informatica Managed File Transfer and B2B Data Exchange.

Use the `migrateWebUsersAndEndpoints` command to create web users and hosted endpoints.

For an OEM endpoint that is connected to the organization environment, use this command to create an MFT Hosted Receive endpoint and an MFT hosted Send endpoint.

For each relevant endpoint, the corresponding OEM Managed File Transfer mailbox is migrated to the Informatica Managed File Transfer web user. After that, the OEM Managed File Transfer endpoint is migrated to create Informatica Managed File Transfer endpoints. The Informatica Managed File Transfer web user is used in the generated Informatica Managed File Transfer hosted endpoints.

Resource and Endpoint Migration

You can use the migration tool to create resources and remote endpoints in Informatica Managed File Transfer and B2B Data Exchange.

Use the `migrateResourcesAndEndpoints` command to create resources and remote endpoints.

For an OEM endpoint that is connected to a server hosted in a partner environment, use this command to create an MFT Remote Receive endpoint and an MFT Remote Send endpoint.

For each relevant endpoint, the corresponding OEM Managed File Transfer host and mailbox is migrated to the Informatica Managed File Transfer resource. After that, the OEM Managed File Transfer endpoint is migrated to create Informatica Managed File Transfer endpoints. The Informatica Managed File Transfer resource which is migrated is automatically set as the value for the Source and Target Connection project variables in the generated Informatica Managed File Transfer endpoints.

Certificate and Key Migration

Use the migration tool to migrate user certificates to Informatica Managed File Transfer and B2B Data Exchange.

In OEM Managed File Transfer there is no distinction between the certificates based on usage, such as SSH Keys, SSL Certificates, or PGP Keys. The migration tool migrates each certificate in OEM Managed File Transfer to all three types in Informatica Managed File Transfer. For each User Certificate present in OEM Managed File Transfer, the migration tool create the following artifacts:

- SSH Private Key
- SSH Public Key
- SSL Key Pair (private key store)
- OpenPGP Private Key
- OpenPGP Public Key

Use the `migrateCertificatesAndKeys` command to migrate user certificates and private and public keys from OEM Managed File Transfer to Informatica Managed File Transfer.

To export a private key, you must provide a private key passphrase. Provide a key passphrase file that contains the passphrases. Specify the file name in the command with the `-pf <passphraseFile>` option.

The passphrase file must be in JSON format and associate the user alias name to the corresponding private key file passphrase. The passphrases must be encrypted using the B2B Data Exchange encryption tool.

Migrate All

Use the `migrateAll` command to migrate certificates, resources, web users, and endpoints from OEM Managed File Transfer to Informatica Managed File Transfer.

The migration process first migrates certificates, and then endpoint data based on filters specified in the migration configuration file.

For each remote endpoint, the migration tool migrates the resource and then migrates the endpoint, using the created resource in the endpoint project variables. For each hosted endpoint, the migration tool migrates the

mailbox to an Informatica Managed File Transfer web user and then migrates the endpoint using the created web user n the endpoint variables.

Migrate non-B2B Data Exchange Objects

You can migrate non-B2B Data Exchange objects from OEM Managed File Transfer to Informatica Managed File Transfer.

OEM Managed File Transfer might contain hosts and mailboxes that are not used in B2B Data Exchange, but you might want to migrate these objects. To do so, in the migration configuration file, set the parameter `migrate.nonDx.mailboxes` to value `true`.

You can specify which objects to migrate with the following options:

- If you use the `migrateResources` or `migrateResourceAndEndpoints` command option, only the resources that are not used in B2B Data Exchange are migrated.
- If you use the `migrateWebUusers` or `migrateWebUsersAndEndpoints` command option, only the mailboxes that are not used in B2B Data Exchange are migrated.
- If `migrateAll` is specified, the resources and webusers that are not used in B2B Data Exchange are migrated.

This parameter has no effect when the `migrateEndpoint` or `migrateCertificatesAndKeys` command option is specified.

Migrating OEM Managed File Transfer Command Properties

During the migration process, values are extracted from the OEM Managed File Transfer mailbox commands for certain variables in the Informatica Managed File Transfer template projects. These values determine the endpoint project variable values. Value extraction applies for remote endpoints and for FTP, FTPS and SSH FTP endpoints.

Values are extracted from the OEM Managed File Transfer commands if the commands match several predefined patterns.

For remote receive endpoints, the following properties are extracted:

- Source Directory
- File Pattern to Download
- Is Pattern Wildcard
- Delete from Source After Download

For remote send endpoints, the following property is extracted:

- Target Directory

Resource Mapping File

As part of the installation, sample resource mapping files are provided. Each protocol has its own resource mapping file. In addition, when you use the `migrateResources` or `migrateResourcesAndEndpoint` commands to create resources, the migration tool generates a resource mapping file named `Endpoint_Resource_Mapping_Generated.txt`.

When you use the migration tool to subsequently create endpoints in B2B Data Exchange, the migration tool uses the resource mapping file to identify data in the process of populating the endpoint fields.

The resource mapping file links the name of the migrated OEM endpoint with a Generated Resource Name. The Generated Resource Name is the name of the resource that the migration process creates to correspond to the migrated OEM endpoint. The mapping file is created in JSON format and can be modified to customize resource migration.

Note: The Generated Resource Name is also used to populate the Connection variables in the template project associated with a generated endpoint.

The migration tool creates a separate resource mapping file for each protocol. Resource mapping files are created in the directory `<B2B Data Exchange Installation>/dx-tools/mftMigration\<transport type>`. If you choose to customize the resource mapping file, create and save a backup copy before you modify the file.

A sample resource mapping file is provided in the installation for each endpoint protocol. The sample mapping file has the following structure:

```
{
 "endpoint1" : "resource1",
 "endpoint2" : "resource2"
},
```

When you migrate endpoints with the `migrateEndpoints` command, you must specify the name of the related resource mapping file to be used by the migration process.

Resource Mapping File Syntax

A mapping file contains JSON code that maps OEM hosts and mailboxes to resources that are created during migration. OEM host and mailbox properties are stored in Host XML files. Each section in a mapping file links a specific OEM host or mailbox property from the Host XML file to the corresponding Informatica Managed File Transfer resource property.

You can use also rules or conditions to specify how and when the migration tool maps OEM host and mailbox properties to resource properties.

Resource Mapping Example

The following JSON code shows an example of a mapping in a mapping file:

```
{
  "cleoModelXPath": "/Host/Address",
  "infaMFTTabName": "Basic",
  "infaMFTDisplayName": "Host",
  "rules": []
},
```

The following table describes the elements shown in the example:

System	Requirement
cleoModelXPath	Specifies the XPath value for a property in the OEM Host XML file.
infaMFTTabName	Specify the Tab Name of the corresponding property in Informatica Managed File Transfer.
infaMFTDisplayName	Specify the Display Label of the corresponding property in Informatica Managed File Transfer.
rules	Specify rules that the migration tool will use to map properties for endpoints.

This example maps the property specified by the XPath `"/Host/Address"` in the OEM Host XML. The OEM property maps to the Informatica Managed File Transfer property named `Host` located in the tab named `Basic`.

Resource Mapping Rules

Mapping rules specify how the migration tool maps an XPath value for a property in the OEM Host XML file to a corresponding property in Informatica Managed File Transfer.

You can apply the following rules:

Enumeration Rule

Use this rule when the OEM property has a fixed set of values, and there is a corresponding fixed set of values in Informatica Managed File Transfer. This rule specifies the list of individual mappings for the property values.

Custom Rule

Use this rule to run custom Java code to map a property. For more information contact Informatica Customer Support.

To use a custom rule, create an Informatica Managed File Transfer project associated with the `dx-mft-migration` module. After implementing the `CustomMapper` interface, create a jar and copy the jar to the directory `<B2B Data Exchange Installation>/dx-tools/lib`.

Enumeration Rule Example

The following JSON code shows an example of an enumeration rule:

```
"rules": [
  {
      "type" : "enumeration",
      "values" : [
          {
              "cleoValue" : "Passive",
              "infaMFTValue" : "Yes"
          },
          {
              "cleoValue" : "Active",
              "infaMFTValue" : "No"
          }
      ]
  }
]
```

If you trace through this example, you see that one of the rules maps the property specified by the value `"cleoValue" : "Passive"` to `"infaMFTValue" : "Yes"`.

Custom Rule Example

The following JSON code shows an example of a custom rule:

```
"rules": [
            {
               "type" : "custom",
               "mapperClass" : "com.mycompany.EmailMapper"
            }
         ]
```

The `mapperClass` element specifies the name of the class that implements the mapping interface.

Resource Mapping Conditions

If the way you define an endpoint property depends on a certain dependency, you can specify a condition to control under what circumstances the OEM host and mailbox properties are mapped to resource properties.

Condition Example

The following JSON code shows an example of a condition:

```
{
  "cleoModelXPath": "/Host/Activedataportlow",
  "infaMFTDisplayName": "Data Connection Start Port",
  "mappingCondition" : {
                   "cleoModelXPath" : "/Host/Datachannelmode",
                   "cleoModelValue" : "Active"
                },
  "rules": []
},
```

If you trace through this example, the element `mappingCondition` contains the element `cleoModelXPath` that specifies an XPath element for an OEM property. It also contains the element `cleoModelValue` that specifies a conditional value for the OEM property. The migration tool uses the mapping to create endpoints when a partner endpoint OEM property specified by the XPath has the value `Active`. If the value specified in the condition is not met, the mapping is ignored.

Resource Mapping Static Values

You can provide a predetermined value for an endpoint property by using a static value in a mapping file.

Static Value Example

The following JSON code shows an example of a static value:

```
{
  "infaMFTDisplayName": "Data Connection Start Port",
  "value" : "Active",
  "rules": []
},
```

If you trace through this example, the Informatica Managed File Transfer property labelled `Data Connection Start Port` will be assigned the value `Active`. This mapping ignores the OEM value, so the element `cleoModelXPath`, that specifies an XPath element for an OEM property, is not present in the mapping.

Resource Mapping Variable Values

The migration process might require the migration of variables. Variables are defined by key-value pairs where the key is the name of the variable and the value is the value of that variable for the object that is migrated.

The migration tool can migrate values associated with the following names:

resourceName

The name of the resource that the migration tool creates.

hostname

The name of the OEM host.

mailboxName

The name of the OEM mailbox

To assign a value to an Informatica Managed File Transfer property, specify the variable name prefixed with the `$` symbol in the `value` element.

Variable Values Example

The following JSON code shows an example of a variable value assignment:

```
"value" : "$resourceName"
```

This code assigns the value specified by the element `resourceName`.

HTTP/HTTPS Endpoint Migration

The migration process extracts values from the OEM Managed File Transfer mailbox commands for HTTP and HTTPS hosts. The migration process uses these values to create the project variables `Get_URI` and `Destination_URI`.

For OEM Managed File Transfer HTTP/HTTPS hosts, the URI that creates HTTP requests is constructed at runtime with the data in the HTTP Host configuration. The OEM Managed File Transfer host configuration includes an HTTP tab that specifies the command for the mailbox, the HTTP method, the URI request path, query parameters, and headers for the request.

The migration tool does not migrate query parameters and headers. Since the migration process uses template projects, the receive project uses the HTTP GET method explicitly and the send project uses the HTTP POST method explicitly. Migration is based on the assumption that the OEM Managed File Transfer mailbox is configured with the HTTP Get method to receive files and POST method to send files. If the mailbox is configured to use other methods instead, either those mailboxes must be migrated manually or if the tool is used for migration, the generated migrated endpoints and project used in each endpoint must be edited and updated.

The migration process checks the mailbox command and the request path that is specified in the OEM Managed File Transfer host configuration. For a receive endpoint, the tool constructs a final URI with the request path and concatenates any additional path specified in the command. For the send endpoint, the final URI is same as the request path specified in the host configuration for the corresponding mailbox command.

If there is more than one command in the mailbox, only the first is considered for URI extraction. Once the URIs are extracted, they are applied to the corresponding project variable values for the relevant endpoint.

Configuration Example

In this example, the HTTP Host configuration GET command has the following settings:

- Command: `GET`
- Method: `GET`
- Path: `/v1/api/download`

The HTTP Host configuration PUT command has the following settings:

- Command: `PUT`
- Method: `PUT`
- Path: `/v1/api/download`

The host configuration has the following Receive Mailbox command:

```
GET edifiles
```

The host configuration has the following Send Mailbox command:

```
POST inventory.txt
```

The URI parameters will be provided the following values:

- `Get_URI`: `/v1/api/download/edifiles`
- `Destination_URI`: `/v1/api/upload/`

AS2 Endpoint Migration

Informatica Managed File Transfer supports AS2 Remote Send endpoints and AS2 Hosted Receive endpoints. Remote Receive and Hosted Send endpoint types are not applicable for AS2.

Remote Send

The remote server details are defined in the OEM Managed File Transfer AS2 host settings. The authentication details, if there are any, are configured in the mailbox. In the HTTP Settings tab of the OEM configuration, the **AS2-From** field is set to the organization AS2 ID and the **AS2-To** field is set to the partner AS2 ID. After this, you can send AS2 messages with OEM Managed File Transfer to the remote server.

Hosted Receive

The AS2 Local Listener is configured separately than the host in OEM Managed File Transfer. An AS2 Host and mailbox are created to receive messages. If there was already a host defined for the partner, the mailbox can be created under the same host.

In the HTTP mailbox settings, the **AS2-From** field is set to the partner AS2 ID and the **AS2-To** field is set to the organization AS2 ID. After this, AS2 messages that the OEM Managed File Transfer Listener receives are routed to the relevant AS2 host and mailbox.

After the mailbox receives an incoming AS2 message, the B2B Data Exchange endpoint configured to use that mailbox picks up the message files.

Migrated Objects

The migration process migrates and creates the following AS2 objects:

- AS2 resource

- Remote Send endpoint. The endpoint uses the AS2 resource to send AS2 messages to the partner.
- Web User. The web user has an AS2 ID set according to the **To ID** OEM mailbox setting.
- Hosted Receive endpoint. The endpoint uses the web user created to receive AS2 messages from the partner.

AS2 Migration Commands

Migration Commands for AS2

The migration commands work differently for AS2 endpoints, because there are no Remote Receive and Hosted send endpoints and because of differences in the AS2 configuration in OEM Managed File Transfer. For AS2 migration, the followings commands are used with the following differences:

1. migrateResources. Creates only the AS2 resource for the selected endpoint.
2. migrateWebUsers. Does not migrate AS2 related objects in the target system.
3. migrateResourcesAndEndpoints. Creates all the AS2 migration objects.
4. migrateWebUsersAndEndpoints. Does not migrate AS2 related objects in the target system.
5. migrateEndpoints - Creates only the two types of AS2 endpoints.
6. migrateAll. Creates all the AS2 migration objects.

AS2 Migration Objects

The following AS2 resource properties are migrated:

- URL
- AS2 From ID
- AS2 To ID
- Request Encrypted
- Encryption Method
- Trading Partner's Certificate - Encryption Certificate
- Trading Partner's Certificate - Signing Certificate
- Request Compressed
- My Certificates - Signing Certificate Alias
- Authentication - Username
- Authentication - Password
- Retry Delay
- HTTPS Client Certificate Alias
- SSLMinimumProtocolVersion

The following SSH FTP receive project properties are migrated:

- Email On Fail
- Email On Successful Receive
- Execute On Fail
- Execute On Successful Receive

- Include Failure In Subject Of Email

The following SSH FTP send project properties are migrated:

- Terminate On Fail
- Email On Fail
- Email On Successful Send
- Execute On Fail
- Execute On Successful Send
- Include Failure In Subject Of Email
- Do Not Send Zero Length Files
- Destination AS2 Connection
- Destination Directory
- Put Content Type
- Put Subject
- As2 Receipt Desired
- As2 Receipt Destination
- As2 Receipt email

FTP Migration Objects

When you use the migration tool to migrate FTP endpoints, the following resource properties are migrated:

- Server address
- Port
- Username
- Password
- Data channel mode
- Active mode data port low
- Active mode data port high
- Connection timeout
- Retry delay
- Command retries are migrated as connection retries for the resource

The following FTP Receive endpoint project properties are migrated:

- Default Data Type
- Terminate On Fail
- Email On Fail
- Email On Successful Send
- Execute On Fail
- Execute On Successful Send

- Include Failure In Subject Of Email
- Delete Zero Length Files
- Get Number Of Files Limit

FTPS Migration Objects

The following FTPS resource properties are migrated:

- Server address
- Port
- Username
- Password
- Data channel mode
- Security mode
- SSL Minimum Protocol Version
- Client Certificate alias
- Active mode data port low
- Active mode data port high
- Connection timeout
- Retry delay
- Command retries are migrated as connection retries for the resource

The following FTPS receive project properties are migrated:

- Default Data Type
- Terminate On Fail
- Email On Fail
- Email On Successful Receive
- Execute On Fail
- Execute On Successful Receive
- Include Failure In Subject Of Email
- Delete Zero Length Files
- Get Number Of Files Limit
- Source FTPS Connection
- Source Directory
- File Pattern To Download
- Is Pattern Wildcard
- Delete From Source After Download

The following FTPS send project properties are migrated:

- Default Data Type

- Terminate On Fail
- Email On Fail
- Email On Successful Send
- Execute On Fail
- Execute On Successful Send
- Include Failure In Subject Of Email
- Do Not Send Zero Length Files
- Destination FTPS Connection

SSH FTP Migration Objects

The following SSH FTP resource properties are migrated:

- Server address
- Port
- Username
- Password
- PreferredCipherAlgorithm
- PreferredMACAlgorithm
- Private Key File
- Private Key Password
- Certificate Alias
- Connection timeout
- Retry delay
- Command retries are migrated as connection retries for the resource

The following SSH FTP receive project properties are migrated:

- Terminate On Fail
- Email On Fail
- Email On Successful Receive
- Execute On Fail
- Execute On Successful Receive
- Include Failure In Subject Of Email
- Delete Zero Length Files
- Get Number Of Files Limit
- Source Connection
- Source Directory
- File Pattern To Download
- Is Pattern Wildcard
- Delete From Source After Download

The following SSH FTP send project properties are migrated:

- Terminate On Fail
- Email On Fail
- Email On Successful Send
- Execute On Fail
- Execute On Successful Send
- Include Failure In Subject Of Email
- Do Not Send Zero Length Files
- Destination Connection
- Destination Directory

HTTP Migration Objects

The following HTTP resource properties are migrated:

- Server address
- Port
- Username
- Password
- Connection timeout

The following HTTP receive project properties are migrated:

- Get URI
- Source HTTP Connection
- Terminate On Fail
- Email On Fail
- Email On Successful Receive
- Execute On Fail
- Execute On Successful Receive
- Include Failure In Subject Of Email
- Delete Zero Length Files

The following HTTP send project properties are migrated:

- Destination URI
- Destination HTTP Connection
- Terminate On Fail
- Email On Fail
- Email On Successful Send
- Execute On Fail
- Execute On Successful Send
- Include Failure In Subject Of Email

- Do Not Send Zero Length Files
- Successful Put Response Phrase

HTTPS Migration Objects

The following HTTPS resource properties are migrated:

- Server address
- Port
- Username
- Password
- Connection timeout
- SSLMinimumProtocolVersion
- Client Certificate Alias

The following HTTPS receive project properties are migrated:

- Get URI
- Source HTTPS Connection
- Terminate On Fail
- Email On Fail
- Email On Successful Receive
- Execute On Fail
- Execute On Successful Receive
- Include Failure In Subject Of Email
- Delete Zero Length Files

The following HTTPS send project properties are migrated:

- Destination URI
- Destination HTTPS Connection
- Terminate On Fail
- Email On Fail
- Email On Successful Send
- Execute On Fail
- Execute On Successful Send
- Include Failure In Subject Of Email
- Do Not Send Zero Length Files
- Successful Put Response Phrase

PGP Encryption and Certificate Migration Objects and Limitations

When you use the migration tool to migrate PGP encryption objects, the following Remote Receive project properties are migrated:

- Mailbox Packaging
- PGP Compression Algorithm
- PGP Hash Algorithm
- PGP V3 Signature
- OpenPGP Decrypt Inbound
- OpenPGP Certificate Password
- OpenPGP Force Signature
- OpenPGP SecretKey CN

The following Remote Send project properties are migrated:

- Mailbox Packaging
- PGP Compression Algorithm
- PGP Encryption Algorithm
- PGP Hash Algorithm
- PGP Integrity Check
- PGP Signature Verification
- PGP V3 Signature
- OpenPGP Encrypt Outbound
- OpenPGP Armored Base64
- OpenPGP Compressed
- OpenPGP PublicKey CN

The following Hosted Receive project properties are migrated:

- Mailbox Packaging
- PGP Compression Algorithm
- PGP Hash Algorithm
- PGP V3 Signature
- OpenPGP Decrypt Inbound
- OpenPGP Certificate Password
- OpenPGP SecretKey CN

The following Hosted Send project properties are migrated:

- Mailbox Packaging
- PGP Compression Algorithm
- PGP Encryption Algorithm
- PGP Hash Algorithm
- PGP Integrity Check

- PGP Signature Verification
- PGP V3 Signature
- OpenPGP Encrypt Outbound
- OpenPGP Encrypted
- OpenPGP Armored Base64
- OpenPGP Compressed
- OpenPGP PublicKey CN

The following PGP encryption and certificate related properties are not supported:

- Unzip Use Path
- Zip Compression Level
- Zip Subdirectories Into Individual Zip Files
- PGP Compression Algorithm
- PGP Encryption Algorithm
- PGP Hash Algorithm
- PGP Integrity Check
- PGP V3 Signature
- Mailbox Packaging
- OpenPGP Encrypt Outbound
- OpenPGP Decrypt Inbound
- OpenPGP Certificate
- OpenPGP Certificate Alias
- OpenPGP Password
- OpenPGP Encrypted
- OpenPGP Signed
- OpenPGP Armored Base64
- OpenPGP Compressed
- OpenPGP Encrypt to My Certificate
- OpenPGP Force Encryption
- OpenPGP Force Signature
- OpenPGP Allow non OpenPGP

Hosted Endpoint Properties Migration

The following hosted endpoint receive project properties are migrated:

- Email On Fail
- Email On Successful Receive
- Execute On Fail

- Execute On Successful Receive
- Include Failure In Subject Of Email

The following hosted endpoint send project properties are migrated:

- Email On Fail
- Email On Successful Send
- Execute On Fail
- Execute On Successful Send
- Include Failure In Subject Of Email

Migration Status

The migration tool writes the migration status for each object to a file named `MigrationStatus.xml` in the directory `<B2B Data Exchange Installation>\dx-tools\`. The `MigrationStatus.xml` file can be used for troubleshooting purposes. In addition to the status file, the migration tool also creates a log file named `mftmigration.log` in the directory `<B2B Data Exchange Installation>\dx-tools\logs`, with further details regarding the migration process and any errors that might have occured.

For a migrated resource, the `MigrationStatus.xml` file contains the following details:

Element	Description
<host>	Identifies the host alias.
<mailbox>	Identifies the mailbox alias.
<status>	Status of the migration.
<infaMFTResourceName>	Name of the Informatica Managed File Transfer resource that has been generated.
<message>	If the migration fails, this field contains a message with the cause of the failure.

For a migrated web user, the `MigrationStatus.xml` file contains the following details:

Element	Description
<mailbox>	Identifies the mailbox alias.
<status>	Status of the migration.
<infaMFTWebUserName>	Name of the Informatica Managed File Transfer web user that has been generated.
<message>	If the migration fails, this field contains a message with the cause of the failure.

For a migrated endpoint, the `MigrationStatus.xml` file has the following details:

Element	Description
<name>	Name of the OEM endpoint that was migrated.
<status>	Status of the migration.
<infaMFTReceiveEndpointName>	Name of the Informatica Managed File Transfer receive endpoint that has been generated.
<infaMFTSendEndpointName>	Name of the Informatica Managed File Transfer send endpoint that has been generated.
<oemMFTEndpointName>	Updated name of the OEM endpoint that was migrated.
<message>	If the migration fails, this field contains a message with the cause of the failure.

For a migrated certificate or key, the `MigrationStatus.xml` file contains the following details:

Element	Description
<Alias>	Alias or the migrated certificate or key.
<Status>	Status of the migration.
<KeyType>	Type of key: SSL, SSH, or OpenPGP.
<IsPublic>	Specifies whether the migrated certificate or key is public or private.
<message>	If the migration fails, this field contains a message with the cause of the failure.

Status File Example

The following JSON code shows an sample status:

```
<MigrationResult>
 <partner name="PartnerE">
  <Object type="resource">
    <host>PartnerE</host>
    <mailbox>e1</mailbox>
    <status>success</status>
    <infaMFTResourceName>PartnerE_e1</infaMFTResourceName>
   </Object>
   <Object type="endpoint">
    <name>E_send1</name>
    <status>success</status>
    <infaMFTReceiveEndpointName>INFA_MFT_E_send1</infaMFTReceiveEndpointName>
    <infaMFTSendEndpointName>E_send1</infaMFTSendEndpointName>
   </Object>
 </partner>
</MigrationResult>
```

Migrating Endpoint Data

After you upgrade B2B Data Exchange and install Informatica managed File Transfer, you can migrate OEM Managed File Transfer endpoint configuration data. To migrate endpoint configuration data from the OEM Managed File Transfer to Informatica Managed File Transfer, perform the following steps:

1. Configure the `migration.conf` file located in the `<B2B Data Exchange Installation>\dx-tools\mftMigration` directory.
2. Ensure that the following services are running:
   - B2B Data Exchange DX-Console
   - B2B Data Exchange DX-Server
   - OEM Managed File Transfer service
   - Informatica Managed File Transfer services
3. To run the migration tool, change directory to the `<B2B Data Exchange Installation>\dx-tools\` directory and type the migration command:

   ```
   -c <command> -f migration.conf [-mf <mapping file name>] [-pf <private key properties file name>]
   ```

   and select from the following commands:

System	Requirement
migrateResources	Migrate OEM Managed File Transfer connections to Informatica Managed File Transfer.
migrateWebUsers	Migrate OEM Managed File Transfer web users to Informatica Managed File Transfer.
migrateEndpoints	Migrate OEM Managed File Transfer endpoints to Informatica Managed File Transfer.
migrateResoucesAndEndpoints	Migrate OEM Managed File Transfer connections and remote endpoints to Informatica Managed File Transfer.
migrateCertificatesAndKeys	Migrate OEM Managed File Transfer web users and hosted endpoints to Informatica Managed File Transfer.
migrateAll	Migrate OEM Managed File Transfer certificates, keys, connections, web users, and endpoints to Informatica Managed File Transfer.

   You can select to migrate resources and then endpoints, or migrate both resources and endpoints at the same time, or migrate all at the same time.

4. Test the MFT Connections in B2B Data Exchange.

Testing MFT Connections

To test the MFT Connections in B2B Data Exchange, perform the following steps:

1. In the Navigator, click **Partner Management** > **MFT Connections**.
2. When you finish adding or editing an MFT Connection, click **Test**.

   The **Test Results** window displays the results of the connection test.

Migration Limitations

The following limitations apply to the migration tool and migration procedure.

The migration tool does not migrate the following OEM Managed File Transfer settings and objects:

- Global settings
- Schedules that you manage in OEM Managed File Transfer
- Proxy settings
- Listeners
- VLNavigator portal objects
- VLNavigator navigator objects

When you use the migration tool to migrate OEM Managed File Transfer endpoints, the process cannot be reversed.

Configuration Solutions

Perform the following configuration activities to address migration limitations:

Limitation	Workaround
Non-B2B Data Exchange actions are not migrated. The migration tool addresses the <receive>, <send>, <collect> and <release> actions for migration and does not migrate or report any other actions associated with the OEM Managed File Transfer mailboxes.	Create projects in Informatica Managed File Transfer that correspond to the actions in the OEM Managed File Transfer mailboxes, and assign these projects to the B2B Data Exchange endpoints.
Non-B2B Data Exchange mailboxes and host/mailbox properties are not migrated. Only resources are migrated. The migration tool only migrates B2B Data Exchange-related endpoints. For hosts or mailboxes that are not directly related to B2B Data Exchange endpoints, the migration tool only migrates the resources and web users of the non-B2B Data Exchange hosts and mailboxes.	Create projects in Informatica Managed File Transfer for the non-B2B Data Exchange mailbox actions using the migrated resources/web-users and schedule them accordingly.
OEM Managed File Transfer users from VLNavigator are not migrated. The migration tool does not migrate or report the users and objects in VLNavigator.	Create Admin Users in Informatica Managed File Transfer for the corresponding users in VLNavigator.

Limitation	Workaround
The migration tool does not migrate schedules managed in the OEM Managed File Transfer.	Create Schedules, Monitors and Triggers in Informatica Managed File Transfer for the corresponding schedule objects in OEM Managed File Transfer.
The migration tool does not migrate global configuration settings such as date format or admin email.	Configure the Global Settings in Informatica Managed File Transfer with settings corresponding to those in OEM Managed File Transfer.
The migration tool does not migrate or report endpoints or resources for SMTP or MLLP protocols or MQ or Mailbox objects.	Create the SMTP, MQ, MLLP, or Mailbox resources in Informatica Managed File Transfer. Create projects using these resources with actions corresponding to those in OEM Managed File Transfer. Schedule the project actions.
The migration tool does not migrate or report endpoints or resources or web users for AS3, OFTP, eb XML, EBICS, fasp, HSP, RNIF, WS, AS/400, or Cleo HTTPS protocols.	Informatica Managed File Transfer does not support AS3, OFTP, eb XML, EBICS, fasp, HSP, RNIF, WS, AS/400, or Cleo HTTPS protocols.
The migration tool does not migrate the proxy server configurations or settings.	After migration, configure the Gateway Manager and the resource proxy configurations in Informatica Managed File Transfer.
Passwords for hosted users (web users) and private keys are not migrated.	The migration tool generates the web users either with a default password, or generates passwords based on the password policy and then sends emails to the web users. The Informatica Managed File Transfer admin must configure the password generation logic before running the migration tool and inform the partners on the follow-up actions to either change the default passwords after the first login or use the newly generated passwords.
Cleo commands are not migrated. The migration tool uses parameterized template projects to create endpoints. The template projects include only the CD, GET, and PUT commands and -DEL option. All other commands such as QUOTE, SET, LCOPY, LDELETE, or LREPLACE are not part of the template projects.	Create a backup of the template projects and then modify the template projects, or create projects. Add the mailbox actions that use commands other than CD, GET, and PUT.
Multiple commands within an action are not migrated. If the action task for a mailbox contains multiple commands, such as GET for multiple file patterns, or any other command followed by more than one GET command, then only the first GET command is considered for the file download pattern for migration.	Create projects for the actions or modify the template projects.

CHAPTER 11

Installing and Configuring the B2B Data Exchange Accelerator for Data Archive

This chapter includes the following topics:

Installing and Configuring B2B Data Exchange Accelerator for Data Archive Overview

The B2B Data Exchange accelerator is a plug-in for Data Archive that enables you to archive events that B2B Data Exchange generates with Data Archive. The accelerator utilizes the advanced archiving capabilities of

Data Archive, such as detailed archive parameters, recurring archive jobs, and easily accessible archive repositories.

After you install B2B Data Exchange Accelerator for Data Archive, configure the archive project based on the archiving requirements in your organization. Perform the following configuration steps:

1. Create the source and target connections.
2. To secure access to the source connections, configure access roles and access users, and then create a security group.
3. Create the history database tables and indexes.
4. Create the seamless access layer for the history database.
5. Create the file archive user and the file archive folder.
6. Schedule archive jobs, and then archive the B2B Data Exchange repository.
7. To view archived documents and events in the B2B Data Exchange Operations Console, configure system properties and assign user permissions.
8. To view archived documents and events in the Data Discovery portal, configure the relevant Data Archive search to browse data, search data, or search by-reference documents.

Pre-Installation Steps

Before you install the B2B Data Exchange accelerator in Data Archive, make sure that your system meets the minimum requirements and follow the pre-installation steps.

1. Make sure you have an active installation of Data Archive. A limited Data Archive version is provided with B2B Data Exchange.
2. Create and assign privileges to the B2B Data Exchange production database and history database users.
3. For archive projects to or from the history database, configure the history database location and credentials in the client and server copies of the dx-configuration.properties file:

Property	Description
dx.archive.jdbc.url	Location of the history database. You replace the default value with one of the following values: - For Oracle, use the following format: `jdbc:informatica:oracle://<oracle host>:<oracle port>;SID=<oracle sid>` - For Microsoft SQL Server, use the following format: `jdbc:informatica:sqlserver://<sqlserver host>:<sql server port>;DatabaseName=<database name>` The default value is `${dx.archive.jdbc.url}`.
dx.archive.jdbc.username	Name of the history database user. You replace the default value with the database user name. The default value is: `${dx.archive.jdbc.username}`
dx.archive.jdbc.password	Encrypted password for the history database user. You encrypt the password with the password encryption utility and replace the default value with the encrypted string. The default value is: `${dx.archive.jdbc.password}`

Note: To determine the specific location and credentials for the history database, consult the database administrator.

4. To enable archiving document attachments, copy the library file from the folder `<DX installation directory>/ILM-accelerator/lib` to the folder `<ILM installation directory>/webapp/WEB-INF/lib/`.
5. In the Data Archive installation directory, open the `conf.properties` file and set the value of the following properties:
   - Set the value of the `informia.useDbaViewsInSeamlessAccess` property to `false`.
   - Set the value of the `informia.proceduresToExecute.inArchiveFromHistory` property to `java://com.informatica.b2b.dx.ilm.MoveDXDocStoreDatabaseDAOImpl`.

   Note: Back up the `conf.properties` file before you modify the property.
6. Restart Data Archive.

Database User Privileges

When you prepare the production database and history database, you assign database privileges to users according to the archive scenario requirements. Set up the database users before you install the accelerator and create archive projects.

Note: To avoid user conflicts, set up a unique database user for each database.

The following table describes the production database privileges to assign to the production database user:

Component	Privileges
Rows	- Select - Insert - Update - Delete
Tables and views	- Create - Alter - Drop

The following table describes the history database privileges to assign to the history database user:

Component	Privileges
Rows	- Select - Insert - Update - Delete
Tables and views	- Create - Alter - Drop
Synonyms and links	- Create - Delete

In addition to the history database privileges, the history database user needs to access and modify rows in the production database.

The following table describes the production database privileges to assign to the history database user:

Component	Privileges
Rows	- Select - Insert - Update - Delete

Installing the B2B Data Exchange Accelerator for Data Archive

Install the B2B Data Exchange accelerator for Data Archive after you install B2B Data Exchange and Data Archive.

Before you install the accelerator, install Data Archive and follow the pre-installation steps.
The minimum supported version of Data Archive is 6.1. If you have Data Archive version 6.1 installed, also install EBF 11801 and EBF 11672.

1. Log in to Data Archive with administrator privileges and click **Accelerators** > **Enterprise Data Manager**.

   The Enterprise Data Manager appears.
2. In the Enterprise Data Manager, click **File** > **Import** > **Accelerator**.

   The **Import Metadata Options** window appears.
3. Select **Continue Import through EDM** and click **OK**.
4. Navigate to the location `<DXInstallationDir>/ILM-accelerator` and select to import all the `XML` files in the directory.

   Note: Do not import the sub-folders in the directory.

   The Enterprise Data Manager displays a progress window during the import process.
5. To verify the import process, restart the Enterprise Data Manager and make sure that the accelerator appears in the `B2B Data Exchange` node of the Explorer pane.
6. To add the accelerator to drop-down lists in Data Archive, log in to the database with the B2B Data Exchange history database credentials and run the SQL script on the Data Archive repository. The script is located in one of the following locations:

Database	Path
Oracle	<DXInstallationDir>/ILM-accelerator/sql/oracle_ilm_repository_update.sql
Microsoft SQL Server	<DXInstallationDir>ILM-accelerator/sql/sqlserver_ilm_repository_update.sql

Source and Target Connections

You must create a connection for each source database that you want to archive data documents from. One source database is the database that stores the documents that you want to archive, the production

database. For restore jobs, the source database is the history database, where the data was originally archived.

There are two types of source connections, one to archive data from the production database to the history database, and the other from any database to the file archive.

You must also create a target connection for each database that you want to archive data to. The target database is the location where you want to archive data to.

There are two types of target connections, a connection to a target database, or to a file archive. The first one is used for mid-term storage, whereas the latter is used for long-term storage.

Configuring a Source Connection from Production Database to History Database

Configure the Data Archive source connection before you archive events from the production database to the history database.

For information about creating source connections, see the *Data Archive Administrator Guide*.

Note: The production database and history database must use the same database system, either SQL Server or Oracle.

1. Log in to Accelerator.
2. Click **Administration** > **New Source Connection**.
3. Enter the database-specific connection properties.
4. Set the application version of the connection to **B2B Data Exchange 10.2.3**.
5. Set the property **Source / Staging Attachment Location** to the root path for the production document store.

   The path is the same as the path defined for the B2B Data Exchange system property `dx.system.document.store.folder`.
6. Set the property **Target Attachment Location** to the path of a location that can hold the archived document store (history database).

   The path is the same as the path defined for the B2B Data Exchange system property `dx.archive.document.store.folder`.
7. If the connection is to an SQL Server database, select the option **Compile ILM Functions**.

Note: The properties **Source / Staging Attachment Location** and **Target Attachment Location** cannot have the same value. Both locations must be accessible to the Data Archive archive process.

Configuring a Source Connection from History Database to Data Archive

Configure the Data Archive source connection from the history database to the data archive.

For information about creating source connections, see the *Data Archive Administrator Guide*.

1. Log in to Accelerator.
2. Click **Administration** > **New Source Connection**.
3. Enter the database-specific connection properties.
4. Set the application version of the connection to **B2B Data Exchange 10.2.1**.

5. Set the property **Source / Staging Attachment Location** to the root path for the history database. This is the same path as defined for the B2B Data Exchange system property `dx.archive.document.store.folder`. This value should match the value for the property **Target Attachment Location** for the connection to the production database.
6. Set the property **Target Attachment Location** to the path of a location that has sufficient space to temporarily store documents for the archived document store.
7. If the connection is to an SQL Server database, select the option **Compile ILM Functions**.
8. Set the property **Database Link To Production** to the same path as the history database target connection.

Note: The properties **Source / Staging Attachment Location** and**Target Attachment Location** cannot have the same value. Both locations must be accessible to the Data Archive archive process.

Configuring a Source Connection from Production Database to File Archive

Configure the Data Archive source connection from the production database to the file archive.

For information about creating source connections, see the *Data Archive Administrator Guide*.

Note: The production database and history database must use the same database system, either SQL Server or Oracle.

1. Log in to Accelerator.
2. Click **Administration** > **New Source Connection**.
3. Enter the database-specific connection properties.
4. Set the application version of the connection to **B2B Data Exchange 10.2.1**.
5. Set the property **Source / Staging Attachment Location** to the root path for the document store.

   This is the same path as defined for the B2B Data Exchange system property `dx.system.document.store.folder`.
6. Set the property **Target Attachment Location** to the path of a location that has sufficient space to temporarily store documents for the archived document store.
7. If the connection is to an SQL Server database, select the option **Compile ILM Functions**.

Note: The properties **Source / Staging Attachment Location** and**Target Attachment Location** cannot have the same value. Both locations must be accessible to the Data Archive archive process.

Configuring a Target Connection from Production Database to History Database

Configure the Data Archive target connection from the production database to the history database.

For information about creating target connections, see the *Data Archive Administrator Guide*.

1. Log in to Accelerator.
2. Click **Administration** > **New Target Connection**.
3. Enter the database-specific connection properties.
4. Set the application version of the connection to **B2B Data Exchange 10.2.1**.

5. Define the property **Database Link To Source**.

   The database link is used to access the meta-data tables from the production database. Consult with your database administrator regarding how to set up a database link.

Note: If the link server name contains special characters enclose the special character with double quotes.

Configuring a Target Connection from History Database to File Archive

Configure the Data Archive target connection from the history database to the file archive.

For information about creating target connections, see the *Data Archive Administrator Guide*.

1. Log in to Accelerator.
2. Click **Administration** > **New Target Connection**.
3. Enter the database-specific connection properties.
4. Set the application version of the connection to **B2B Data Exchange 10.2.1**.
5. Define the connection type as **Optimized File**.
6. Disable the option **Use Mined Source Schema**.

Configuring a Target Connection from Production Database to File Archive

Configure the Data Archive target connection from the production database to the file archive.

For information about creating target connections, see the *Data Archive Administrator Guide*.

1. Log in to Accelerator.
2. Click **Administration** > **New Target Connection**.
3. Enter the database-specific connection properties.
4. Set the application version of the connection to **B2B Data Exchange 10.2.1**.
5. Define the connection type as **Optimized File**.
6. Disable the option **Use Mined Source Schema**.

Securing Data Archive Connections

Secure the Data Archive source connections so that only specific users can use and access the connections.

Access roles determine the data that users can access in Data Discovery searches. You use the Data Discovery portal to search for documents that are archived to the Data Archive. Access roles also restrict which users can view and download files that contain exported search results. Users can only download the exported files if the user is assigned to the same access role as the entity.

To secure source connections, first create an access role and associate it with an entity, then assign the access role to a user. Next, create a security group and assign the users that are allowed to access the B2B Data Exchange repository (production) source connection to the group.

Configuring and Assigning the B2B Data Exchange and FAS Access Roles

Access roles determine the data that users can access in Data Discovery searches. Users can only download the exported files if the user is assigned to the same access role as the entity. Create an access role and associate it with an entity, then assign the access role to a user.

Create an access role associated with the entity production database, and an access role associated with the entity FAS production database, and then assign the access roles to users.

1. Log in to Accelerator.
2. Click **Administration** > **Manage Roles**.
3. Click **New Role**.

   The role name cannot contain special characters.
4. Click **Assign Role to New Entity** and provide the name **B2B Data Exchange Access Role**.

   The name cannot contain special characters.
5. For **Application Version** select **B2B Data Exchange 10.2.1**.
6. For **Application** select **DX_SCHEMA B2B Data Exchange Database**.
7. For **Entity Name** type **Processing Data**.
8. To create a second entity named **FAS Processing Data**, click **Add Role**.
9. Click **Assign Role to New Entity** and provide a name, for example **FAS Access Role**.

   The name cannot contain special characters.
10. For **Application Version** select **B2B Data Exchange 10.2.1**.
11. For **Application** select **DX_SCHEMA B2B Data Exchange Database**.
12. For **Entity Name** type **FAS Processing Data**.
13. To assign the **B2B Data Exchange Access Role** entity to a user, click **Administration** > **Manage Roles**.
14. Select a user and click the **Edit** icon next to the user.

    The **Edit User** page appears.
15. Click **Add Role**.
16. For **Product** select **Data Archive**.
17. For **Role** select **B2B Data Exchange Access Role**.
18. Click **Save**.
19. To assign the **FAS Access Role** entity to a user, click **Administration** > **Manage Roles**.
20. Select a user and click the **Edit** icon next to the user.

    The **Edit User** page appears.
21. Click **Add Role**.
22. For **Product** select **Data Archive**.
23. For **Role** select **FAS Access Role**.
24. Click **Save**.

Assign a Connection to a Security Group

Assign a connection to a security group.

1. Log in to Accelerator.
2. Click **Administration** > **Manage Security Groups**.
3. Click **New Security Group**.

   The **Create or Edit a Security Group** page appears.
4. Name the security group, for example **B2B Data Exchange Security Group**.
5. Select the source connection to the production database.
6. Click **Add Permission**.

   A window appears with a list of defined permissions.
7. Select the permission and click **Select**.

   The permission appears in the list of permissions.
8. Select **Application** and for the value select **DX_SCHEMA B2B Data Exchange Database**.
9. Click **Add User**.

   A window appears with a list of users.
10. Select the users that are allowed to access the B2B Data Exchange repository source connection and click **Select**.

    The user appears in the list of users.
11. Enter the user properties.
12. Click **Save**.
13. Follow the same steps for the connection to the history database.

Creating the History Database Tables and Indexes

Create tables and indexes in the history database is required when you create the seamless access layer, and to assure optimized performance.

1. Log in to Accelerator.
2. Select **Jobs** > **Schedule a Job**.
3. In the **Projects/Programs to Run** area select **Standalone Programs**, and click **Add Item**.

   The **Program** dialog box appears.
4. Select **Create Tables**, and click **Select**.
5. Select the source repository.
6. Select the target history database as the destination repository.
7. In the **Schedule** area, select the option to run once or start the job immediately.
8. Click **Schedule**.

Note: When the program Create Indexes runs, it prevents the same events from being archived multiple times into the same history database. Several constraints are added to the history database to represent primary keys.

Create the Seamless Access Layer for the History Database

Create the seamless access layer after you run an archive job or pre-create the tables for the history database.

The database administrator creates the seamless access layer by executing the relevant script located in `<DX installation directory>/ILM-accelerator/sql`:

1. For Oracle: `oracle_seamless_access_script.sql`
2. For SQL Server: `sqlserver_seamless_access_script.sql`

Replace the following system variables in the script:

1. Replace `&linkName` with the database link.
2. Replace `&databaseName` with the schema name of the production database.

The program `Create Seamless Data Access` performs a similar function as the scripts. However, the scripts generate a proper view for in-lining certain entity names, such as partner name, with the event table, when data is archived to the file archive. This in-lining allows you to find events based on partner or account name.

Creating a File Archive User

You must create a file archive user before you create a file archive folder. The file archive user can access the file archive folder.

Data Archive 5.3.6

Create a file archive user with the `sa_user` role.

To create a user, run the following command with the `npa_admin` tool:

```
add_user <username>, <password>
```

The user must be able to query the NPA system data. To enable this capability, run the following command with the `npa_admin` tool:

```
add_user_role dxarchive, query, npa_system
```

Data Archive 6.1

To create a file archive user, perform the following steps:

1. Login to the FAS service using SSASQL, for example with the following command:
   ```
   SSASQL meta meta dba/dba
   ```
2. To create a user, type the following command:
   ```
   create authorization dx_fas /dx_fas
   ```
3. To assign DBA privileges, type the following command:
   ```
   cgrant DBA to dx_fas
   ```
4. To commit the changes, type the following command:
   ```
   commit
   ```

Creating a File Archive Folder

In Data Archive, select and run the `Create Archive Folder` program to create the file archive folder and initialize the file archive.

When you run the `Create Archive Folder` program, define the target connection.

Creating an Archive Job

To set up an archive job for a production or history database, perform the following task.

1. Log in to Accelerator.
2. Click **Workbench** > **Manage Archive Projects**.
3. Click **New Archive Project**.
4. Provide a name for the project.
5. Set the action to **Archive and Purge**.

   This option removes data from the B2B Data Exchange repository after they are archived and also ensures that by-reference documents are archived and then deleted.
6. Select the source and target connections.
7. If the target is a file archive, then only select the option **Include Reference Data**.

   This option ensures that important reference data, such as partner names and account numbers, are also stored in the file archive for each archived event.
8. Click **Next**.
9. Click **Add Entity**.
   - If the target connection is a database, select the entity **Processing Data**.
   - If the target connection is the File Archive Service, select **FAS Processing Data**.
10. Set **Role** to the access role created in "Configuring and Assigning the B2B Data Exchange and FAS Access Roles" on page 163.
11. Set the archive job parameters.

    For more information, see "Archive Job Parameters" on page 167.
12. Click **Next**.
13. To save the project only, click **Publish**.
14. To save the project and immediately schedule a run, click **Publish and Schedule**.

Archive Job Parameters

The following list contains archive job parameters. The parameters `Event Age`, `Include with reconcile status`, and `Include intermediate documents` apply to the whole event hierarchy. Other parameters apply to the root event of the hierarchy.

Event Age

Required. Specifies how old an event must be, in days, before it is archived. For example, if the event was created on 2011-09-01 and the date on which the archive job runs is 2011-09-06, then the age of the event is 5 days. If a value of zero is supplied, then all the events are archived regardless of their age. The event age is counted in the number of whole days. An event created at 01:00 hours or at 23:00 hours on the same day will have the same age in days.

Partner

Optional. The partner to which the root of the event hierarchy must belong. If the root does not belong to the given partner, then that hierarchy is not archived. The partners in the rest of hierarchy (on the child events) do not have to be same partner.

Account

Optional. The account with which the root event of the event hierarchy is associated. If the root event is not related to the given account, then that hierarchy is not archived. The accounts in the rest of hierarchy (on the child events) do not have to be related to the same account.

You can only select an account that is associated with the chosen partner. It is not possible to select an account before choosing a partner.

Event Type

Optional. The event type required for the root event of the event hierarchy. If the root event does not match the event type, the hierarchy is not archived. Other events in the hierarchy do not have to match the event type.

Event Status

Optional. The event status required for the root event of the event hierarchy. If the root event does not match the status, the hierarchy is not archived. If this parameter is selected, the status of any event except the root event is ignored. If no value is specified, then all the events in the hierarchy must have a final status.

Reconciliation Status

Optional. The reconciliation status required for the associated correlation tickets, before the event is archived. The reconciliation tickets can have the following possible status groups:

Any

The ticket status is ignored.

Closed

All the tickets completed normally or are closed after time-out.

Closed and Timed-out

All the tickets completed normally or are closed after time-out. If a ticket timed-out, then this status applies.

Root Events Without Partners

Required. In some scenarios, events that are created are not associated with a partner. This option allows those events to be archived. Enabling this option means that events with no associated partner are archived together for the selected partner or account.

Intermediate Documents

Required. Defines whether the archive job archives intermediate documents or log blobs.

Specifying `no` would result in data loss, as intermediate documents will not be copied to the archive but just deleted.

Scheduling Archive Jobs

Archive job scheduling depends on the type of archive job. Database to database archiving is performed when you archive from the production database to the history database. Database to file archiving is performed when you archive from the production database to the file archive, or from the history database to file archive.

Scheduling Archiving from the Production Database to History Database

Perform the following steps to archive files from the production database to the history database.

1. Log in to Accelerator.
2. Select **Jobs** > **Schedule a Job**.
3. Select **Projects** and click **Add Item**.
4. From the Programs list, select the production to history database program that you want to schedule, according to the database type.
5. Select **Standalone Programs** and click **Add Item**.
6. From the Programs list, select **Create Indexes**.
7. Select the source and target connections that are configured for the archive project.
8. Define relevant schedule parameters.
9. Click **Schedule**.

Archiving from a Database to the File Archive

To archive documents from the history database to the file archive, or from the production database to the file archive you schedule the following programs:

1. Archive the B2B Data Exchange repository and move the files from the database document store to the staging area.
2. Load the archived data into the file archive.
3. Load the documents from the staging area into the file archive.

Scheduling Archiving from a Database to the File Archive

Perform the following steps to archive the production or history database to the file archive.

1. Log in to Accelerator.
2. Select **Jobs** > **Schedule a Job**.

3. Select **Projects** and click **Add Item**.
4. To archive the B2B Data Exchange repository and move the files from the database document store to the staging area, from the Programs list, select the **DX <Database Type> Archive** program, according to the database type.
5. Select **Standalone Programs** and click **Add Item**.
6. To load the archived data into the file archive, from the Programs list, select **File Archive Loader**.
7. Ensure that the field **Archive Job Id** is empty.

   The value is determined when the program runs.
8. Select **Standalone Programs** and click **Add Item**.
9. To load the documents from the staging area into the file archive, from the Programs list, select **Load External Attachments**.
10. For the property **Directory** provide the same value as provided for the property **Target Attachment Location** from the source connection.
11. For the property **Target Archive Store** provide the same value as provided for the same property **Target Attachment Location** for the archive project.
12. Set the field **Purge after Load** to **Yes**.
13. Define relevant schedule parameters.
14. Click **Schedule**.
15. If the job is not scheduled to run immediately, you can view the job if you select **Jobs** > **Manage Jobs**. **Schedule**.

Viewing Archived Events

You can view archived events in the B2B Data Exchange Operations Console, or the Data Archive Data Discovery portal.

Before you view archived events in the Operations Console, configure the relevant system properties and assign user privileges.

Alternatively, you can use the Data Discovery portal to view archived events. Use the Data Discovery portal to search for and view events and their details.

Use the **Browse Data** option to find information directly associated with the event itself, for example the start and complete time. This option provides a direct view of all the data that is available in the archived B2B Data Exchange repository.

Use the **Search File Archive** option to search for data based on archived top-level entities. The difference between the **Search File Archive** option and the **Browse Data** option is that with the first search you can easily drill down to the data associated with an event, for example to event blobs.

You can also use the Data Discovery portal to view archived events for by-reference documents.

Configuring B2B Data Exchange System Properties

Before you can view the archived events from the history database in the B2B Data Exchange Operations Console, you must update the relevant system properties.

Modify the following files:

```
<DXInstallationDir>/conf/dx-configuration.properties
<DXInstallationDir>/DataExchange/tomcat/shared/classes/dx-configuration.properties
```

Back up the files before you update them.

1. Go to the following directory and locate the file named dx-configuration.properties:

   ```
   <DXInstallationDir>/conf/
   ```

2. Use a text editor to open the file.
3. Search for the following text:

   ```
   dx.archive.jdbc.url
   ```

   Set this value to the location of the history database.
4. Search for the following text:

   ```
   dx.archive.jdbc.username
   ```

   Set this value to the user name for the user enabled to access the history database.
5. Search for the following text:

   ```
   dx.archive.jdbc.password
   ```

   Set this value to the password for the user enabled to access the history database.
6. Add the following parameter:

   ```
   dx.archive.document.store.folder
   ```

   Set this value to the location where the pass-by-reference documents are archived.
7. Save the dx-configuration.properties file.

   B2B Data Exchange maintains two copies of the dx-configuration.properties. The contents of the files must be identical.
8. Copy the updated dx-configuration.properties file to the following directory:

   ```
   <DXInstallationDir>/DataExchange/tomcat/shared/classes/
   ```
9. Restart B2B Data Exchange.

Viewing Archived Events in the B2B Data Exchange Operations Console

After you update the relevant system properties, you can view events archived in the history database through the B2B Data Exchange Operations Console.

1. In the B2B Data Exchange Operations Console Navigator, click **Administration** > **User Groups**.

   The **User Groups** page appears.
2. Create a user group and enable the Operator privilege **View Archived Events**.
3. Assign relevant users to the user group.
4. When an Operator with the relevant permissions logs into B2B Data Exchange, in the **Events** section of the Operations Console, the option **View Archived Events** appears.

Browsing Data with the Data Discovery Portal

Use the Data Discovery portal to search for and view events and their details. Use the **Browse Data** option to find information directly associated with the event itself, for example the start and complete time. This option provides a direct view of all the data that is available in the archived B2B Data Exchange repository.

1. Log in to Accelerator.
2. Click **Data Discovery** > **Browse Data**.

   The **Browse Data** page appears.
3. For the **Archive Folder**, select the relevant FAS folder.
4. For the **Entity**, select **FAS Processing Data**.
5. Select **Table** to search.
6. Expand the **Data Columns** section.
7. In the **Available Columns** panel, select the columns to be present in the search results.
8. In the **Where Clause** panel, add any SQL conditions that need to be applied to the search. To check the SQL query, click **Preview SQL**.
9. Click **Search**.

   The results panel appears with a list of the columns in each table in the entity.
10. To export the data, select **CSV** or **SQL** and then click **Export**.

Defining Search Options to Search the File Archive with the Data Discovery Portal

You can use the **Search File Archive** option to search for data based on archived top-level entities, which are for B2B Data Exchange-only events.

Before you use the **Search File Archive** option, set up the search options.

1. Log in to Accelerator.
2. Click **Data Discovery** > **Search Options**.

   The **View Search Options** page appears.
3. For **Application Version**, select **B2B Data Exchange 10.2.1**.
4. For **Application**, select **DX_SCHEMA B2B Data Exchange Database**.
5. For **Entity**, select **FAS Processing Data**.
6. Click **Edit**.

   The **Edit Search Options** page appears with a list of the columns in each table in the entity.
7. Click **Add Entity Table** and select **DX_VIEW_ARCHIVE_EVENT**.
8. In the **Event** table ensure that you do not select anything in the columns **Display**, **Search**, and **Sort**.
9. In the **DX_VIEW_ARCHIVE_EVENT** table, in the columns **Display**, **Search**, and **Sort**, select the columns to be displayed, searched and sorted.

   It is recommended to select all the columns, and then deselect **H_LEVEL**, **SAVEPOINT_ID**, and **CORRELATION_STATE**.
10. Click **Save**.

Searching the File Archive with the Data Discovery Portal

After you set up search options, you can use the **Search File Archive** option to search for data based on archived top-level entities. The difference between the **Search File Archive** option and the **Browse Data** option is that with the first search you can easily drill down to the data associated with an event, for example to event blobs.

1. Log in to Accelerator.
2. Click **Data Discovery** > **Search File Archive**.

   The **Search File Archive** page appears.
3. For the **Archive Folder**, select the FAS archive folder.
4. For **Entity**, select **DX_VIEW_ARCHIVE_EVENT**.
5. Select the search parameters.

   For more information, see the *Data Archive Administrator Guide*.
6. Click **View**.

   The **Search Results** pane appears with a list of the columns related to the entity.
7. To view additional information about a selected event, click **View Archived Data** or **Technical View**.

   In the **DX_EVENT_BLOBS** table, there are links to the data in the **OBJECT** column. The data cannot be viewed directly as it largely contains binary data.
8. To export selected data, click **Export Data**. To export all data, click **Export All Data**.

Configuring and Assigning the By-Reference Access Role

Before you can view archived by-reference documents, the entity that holds the archived documents must be accessible. Create an access role and associate it with an entity, then assign the access role to a user.

The application **External Attachments** and entity **AM_ATTACHMENT_ENTITY** are automatically created, when the program `Load External Attachments` is run.

1. Log in to Accelerator.
2. Click **Administration** > **Manage Roles**.
3. Click **New Role**.

   The role name cannot contain special characters.
4. Click **Assign Role to New Entity** and provide the name **By Reference Access Role**.

   The name cannot contain special characters.
5. For **Application Version** select **B2B Data Exchange 10.2.1**.
6. For **Application** select **External Attachment**.
7. For **Entity Name** type **AM_ATTACHMENT_ENTITY**.
8. To assign the **By Reference Access Role** entity to a user, click **Administration** > **Manage Roles**.
9. Select a user and click the **Edit** icon next to the user.

   The **Edit User** page appears.
10. Click **Add Role**.
11. For **Product** select **Data Archive**.
12. For **Role** select **By Reference Access Role**.
13. Click **Save**.

Viewing Archived By-Reference Documents

Enter a short description of the task here (optional).

1. Log in to Accelerator.
2. Click **Data Discovery** > **Search File Archive**.

   The **Search File Archive** page appears.
3. For the **Archive Folder**, select the FAS archive folder.
4. For **Entity**, select **DX_VIEW_ARCHIVE_EVENT**.
5. Select the search parameters.

   For more information, see the *Data Archive Administrator Guide*.
6. Click **View**.

   The **Search Results** pane appears with a list of the columns related to the entity.
7. To view additional information about a selected event, click **View Archived Data** or **Technical View**.
8. In the **DX_EVENT_BLOBS** table, find the event blob file name in the **FULL_FILE_NAME** column. Select the last two elements in the file path, that is the file name and directory.
9. To find the by-reference documents, start another search. Click **Data Discovery** > **Search File Archive**.

   The **Search File Archive** page appears.
10. For the **Archive Folder**, select the same archive folder.
11. For **Entity**, select **AM_ATTACHMENT_ENTITY**.
12. For **Table**, select **AM_ATTACHMENT**.
13. Select the search parameters. For the first search row, select **Attachment Directory** with the operator **Contains**. For the next value, supply the name of the directory in which the event blob file is located.
14. Add a second search row. Select **Attachment Name** with the operator **Contains**. For the next value, supply the event blob file name.
15. Click **View**.

    The results panel appears with a list of the columns in each table in the entity.
16. To view or download the original event blob file, click **Click to view** in the **Attachment Data** column.

Limitations

The following limitations apply to the Data Archive Accelerator.

- By-reference document are only moved from the document store if the archive job is configured with the `Archive and Purge` option. With the `Archive Only` option, the documents reamain in the document store, and are not copied to the history database or the staging area for inclusion in the File Archive.
- The document store is moved synchronously with the archive task. The property `Move Attachments in Synchronous Mode` has no meaning for B2B Data Exchange repository archive jobs.
- ·If the document store is moved, then the property `Source / Staging Attachment Location` for the source connection must also be updated.

- Running an archive job with the `Archive Only` is not supported, as this can lead to duplicate events in the history database. It might cause the B2B Data Exchange Operations Console Archived Events view to be unable to show the event details.
- If the program `Create Indexes` is run on the history database, then the archive job might end in an error state. The program `Create Indexes` adds uniqueness constraints to simulate indexed primary keys which would causes the error.
- If the `drop target indexes` property is selected for a target connection, then the program `create indexes` must be run after each archive job.
- If you use Oracle databases, the history database user must be able to create tables, views, and synonyms. The user must have the following privileges: `CONNECT`, `RESOURCE`, `CREATE VIEW`, and `CREATE SYNONYM`.

CHAPTER 12

Uninstallation

This chapter includes the following topics:

Uninstallation Overview

Uninstall B2B Data Exchange to remove the core application and additional components that you installed on the machine.

The uninstallation process does not delete the repositories or the B2B Data Exchange document store.

The uninstallation process depends on the operating system on which B2B Data Exchange is installed, Windows or UNIX.

Uninstalling B2B Data Exchange from Windows Operating Systems

1. Stop all B2B Data Exchange services.
2. In the Add/Remove Programs control panel, right-click **B2B Data Exchange** and select **Uninstall**.

   The **Uninstall B2B Data Exchange** wizard appears.
3. Click **Next**.

   The **Pre-Uninstall Summary** screen appears.
4. Click **Uninstall**.

   The **Uninstall B2B Data Exchange** screen displays the progress of the uninstallation process. When the uninstallation process ends, the **Uninstall Complete** screen appears.
5. Click **Done** to close the wizard.

Uninstalling B2B Data Exchange from UNIX Operating Systems

1. Stop all B2B Data Exchange services.
2. Run the Uninstall.exe file from the B2B Data Exchange installation directory.

   The **Uninstall B2B Data Exchange** section appears.
3. Click **Next**.

   The **Pre-Uninstall Summary** section appears.
4. Click **Uninstall**.

   The uninstaller displays the progress of the uninstallation process. When the uninstallation process ends, the **Uninstall Complete** section appears.
5. Click **Done** to exit the uninstaller.

INDEX

R

S

T

U