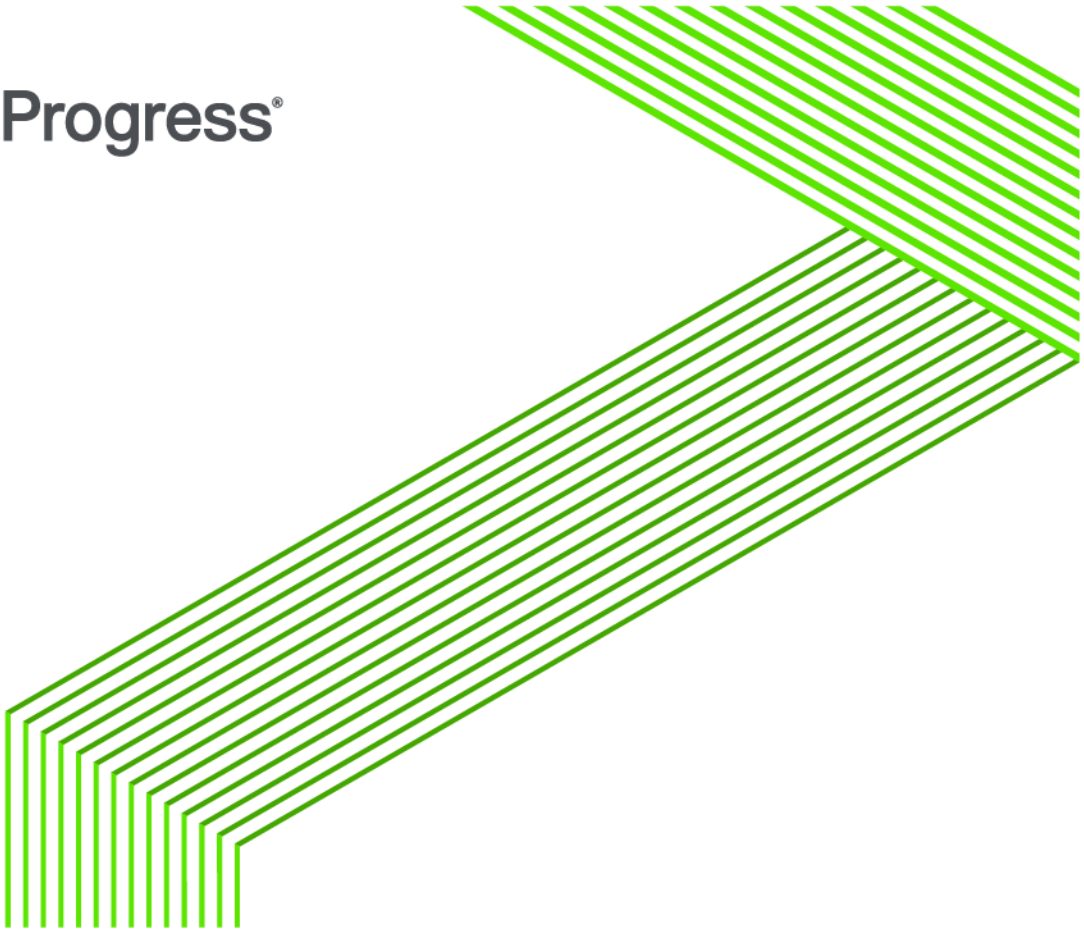


Progress® DataDirect® Hybrid Data Pipeline
Installation Guide

Release 4.6.1

Progress® DataDirect® Hybrid Data Pipeline

Copyright

Updated: 2019/10/14

Table of Contents

1

Welcome to the DataDirect Hybrid Data Pipeline Installation Guide

Progress® DataDirect® Hybrid Data Pipeline is a light-weight software service that provides simple, secure access to your cloud and on-premises data sources for your business intelligence tools and applications.

The Hybrid Data Pipeline server must be installed prior to installing supporting components such as the On-Premises Connector, the ODBC driver, or the JDBC driver. During the installation of the server, the installer generates configuration and certificate files that must be used for the installation of the other supporting components.

See the following topics for detailed instructions on installing Hybrid Data Pipeline and supporting components.

- Product requirements on page 8

  Product requirements for each component you plan to use must be met.

- Deployment guidelines on page 11 and Deployment scenarios on page 12

  Your deployment scenario will dictate how you install and configure Hybrid Data Pipeline.

- Installing and upgrading the Hybrid Data Pipeline server on page 47

  The server must be installed before installing supporting components.

- Installing the Hybrid Data Pipeline Driver for ODBC on page 169

  To run ODBC client applications, install the ODBC driver.

- Installing the Hybrid Data Pipeline Driver for JDBC on page 183

  To run JDBC client applications, install the JDBC driver.

- Installing the Hybrid Data Pipeline On-Premises Connector on page 191

Install the On-Premises Connector for secure connections from cloud applications to on-premise data stores without having to setup a VPN or other gateway.

Refer to the User's Guide for more information on building out and administrating your Hybrid Data Pipeline environment.

For details, see the following topics:

- Product requirements
- Deployment guidelines
- Deployment scenarios

Product requirements

Hybrid Data Pipeline provides access to multiple data sources through a single, unified interface. The Hybrid Data Pipeline server can be supported with the installation and configuration of additional components such as the On-Premises Connector, the ODBC driver, and the JDBC driver.

Note: For REST-based data access for mobile apps and desktop applications, no local software is needed.

Before proceeding with the installation of the server or additional components, confirm that your environment meets the requirements described in the following sections.

- Hybrid Data Pipeline server
- On-Premises Connector
- JDBC driver
- ODBC driver
- Browser for Hybrid Data Pipeline Web UI

Hybrid Data Pipeline server

The Hybrid Data Pipeline server must be installed on a 64-bit Linux machine with, at minimum, 4 cores and 8 GB of RAM.

Note: The OpenJDK 8 JRE is installed with the server and used at runtime. However, you may integrate an external JRE to support the service. OpenJDK 8 and Oracle Java 8 JREs are supported for external integration. See External JRE support and integration on page 42 for details.

Platform	64-bit
Linux • 4 core and 8 GB RAM minimum	Operating System • Centos 4, 5, 6, 7 • Oracle 4, 5, 6, 7 • Red Hat Enterprise 4, 5, 6, 7 • SUSE Enterprise Server 10, 11, 12, 13 • Ubuntu 16 and higher

On-Premises Connector

The On-Premises Connector must be installed on a 64-bit Windows machine with, at minimum, 4 cores and 8 GB of RAM.

Note: The OpenJDK 8 JRE is installed with the On-Premises Connector and used at runtime. However, you may integrate an external JRE to support the On-Premises Connector. OpenJDK 8 and Oracle Java 8 JREs are supported for external integration. See External JRE support and integration on page 42 for details.

Platform	64-bit
Windows • 4 core and 8 GB RAM minimum	Operating System • Windows 10 • Windows 8.1 • Windows 7 • Windows Server 2012 Service Pack 2 • Windows Server 2008

JDBC driver

An installation of the JDBC driver requires 21 MB of hard disk space at minimum. A supported JVM must be defined on your system path. The following JVM implementations are supported.

JVM (32-bit and 64-bit JVMs supported)
• Oracle Java 8 and 11 • OpenJDK 8 and 11

ODBC driver

An installation of the ODBC driver requires 132 MB of hard disk space at minimum. The following platforms are supported.

Platform	32-bit	64-bit
AIX	• 7.1 • 6.1 • 5.3 Fixpack 5	• 7.1 • 6.1 • 5.3 Fixpack 5 or higher
HP-UX PA-RISC	• 11i Version 3.0 (B.11.3x) • 11i Version 2.0 (B.11.23)	*na*
HP-UX IPF	• 11i Version 3.0 (B.11.3x) • 11i Version 2.0 (B.11.23)	• 11i Version 3.0 (B.11.3x) • 11i Version 2.0 (B.11.23)
Linux	• CentOS Linux 4, 5, 6, 7 • Debian 7.11, 8.5 • Oracle Linux 4, 5, 6, 7 • Red Hat Enterprise 4, 5, 6, 7 • SUSE Enterprise Server 10, 11, 12 • Ubuntu 14.04, 16.04	• CentOS Linux 4, 5, 6, 7 • Debian 7.11, 8.5 • Oracle Linux 4, 5, 6, 7 • Red Hat Enterprise 4, 5, 6, 7 • SUSE Enterprise Server 10, 11, 12 • Ubuntu 14.04, 16.04
Oracle Solaris on SPARC	• Oracle Solaris 11, 11 Express • Oracle Solaris 8, 9, 10	• Oracle Solaris 11, 11 Express • Oracle Solaris 8, 9, 10
Oracle Solaris x86: Intel	• Oracle Solaris 11, 11 Express • Oracle Solaris 10	*na*

Platform	32-bit	64-bit
Oracle Solaris x64: Intel and AMD	*na*	• Oracle Solaris 11, 11 Express • Oracle Solaris 10
Windows	• Windows 10 • Windows 8.1 • Windows 7 • Windows Server 2016 • Windows Server 2012 • Windows Server 2008	• Windows 10 • Windows 8.1 • Windows 7 • Windows Server 2016 • Windows Server 2012 • Windows Server 2008

Browser for Hybrid Data Pipeline Web UI

The following browsers are supported.

Browser	Version
Chrome	Chrome 53.0 and higher
Edge	42 and higher
Firefox	Firefox 48 and higher
Internet Explorer	Internet Explorer 11.0 and higher
Safari	Safari 9.1 and higher

Deployment guidelines

Hybrid Data Pipeline is a highly adaptable software service that can be securely integrated into a variety of network environments. Follow these guidelines to get your Hybrid Data Pipeline environment up and running.

- Determine how to deploy Hybrid Data Pipeline. Hybrid Data Pipeline can be deployed either on a standalone node or behind a load balancer on one or more nodes. See Deployment scenarios on page 12 for detailed information.
- Determine which components you need to install and configure in addition to the Hybrid Data Pipeline server. The ODBC driver must be installed to support ODBC applications, and the JDBC driver to support JDBC applications. The On-Premises Connector can be installed for direct, secure access to on-premises data sources.
- Ensure that Product requirements on page 8 are met for each component you are installing. At this time, the Hybrid Data Pipeline server must be installed on a Linux 64-bit machine.

- Collect the information needed for server installation. For example, host and port information must be supplied during the installation of the Hybrid Data Pipeline server. The information you need, in part, depends on your deployment scenario.
- Install the Hybrid Data Pipeline server. See Installing and upgrading the Hybrid Data Pipeline server on page 47 for details.
- After installation of at least one Hybrid Data Pipeline server, you can modify your environment to use an external JRE at runtime as opposed to the embedded JRE that is shipped with the product package. See External JRE support and integration on page 42.
- After the installation of the server, proceed with the installation of supporting components. See the following topics for details.
  - Installing the Hybrid Data Pipeline Driver for ODBC on page 169
  - Installing the Hybrid Data Pipeline Driver for JDBC on page 183
  - Installing the Hybrid Data Pipeline On-Premises Connector on page 191
- Build out the Hybrid Data Pipeline environment. Refer to the Progress DataDirect Hybrid Data Pipeline User's Guide for detailed information.
  - Establish a single-tenant or multitenant architecture.
  - Use the Web UI or Administrators API to provision users.
  - Use the Web UI or Data Sources API to create data sources to support queries to data stores such as Oracle and Salesforce.
- Configure your OData applications to query the data sources you have created. Refer to the Progress DataDirect Hybrid Data Pipeline User's Guide for details.
- Configure the ODBC and JDBC drivers, as well as your ODBC and JDBC applications, to query data sources. Refer to the Progress DataDirect Hybrid Data Pipeline User's Guide for details.

Deployment scenarios

Hybrid Data Pipeline can be deployed on a standalone machine or on one or more nodes behind a load balancer. Many configurations and best practices are contingent on how Hybrid Data Pipeline has been deployed.

For a production environment, Hybrid Data Pipeline should be deployed on one or more nodes behind a load balancer to support scalability and availability. In a load balancer deployment, client application requests must be directed to the load balancer which forwards requests to the node or nodes running the service. When multiple nodes have been deployed, requests are distributed across the cluster. See Load balancer deployment on page 26 for more information.

When deployed on a standalone node, the service is installed on a single host machine that manages all queries, simplifying maintenance and administration. A standalone deployment is not recommended for a production environment because it does not provide the scalability and availability of a load balancer deployment. However, a standalone deployment may be required due to resource limitations and other restrictions. If a standalone deployment is required in production, then, as a matter of best practices, the deployment should include an external system database and a user-specified key location. See Standalone deployment on page 13 for details.

Important: There is currently no migration path from a standalone deployment to a load balancer deployment. Therefore, a standalone deployment is not recommended for environments where scaling up the service may be desired. A standalone node deployment is also not recommended for security and system recovery purposes. If you want to move from a test environment to a production environment, you should begin by deploying Hybrid Data Pipeline on a single node behind a load balancer. When deploying the service on a single node behind a load balancer, you can increase availability and scalability as demanded, and address security and recovery concerns as required.

Whether you deploy the service on a standalone node or behind a load balancer, Hybrid Data Pipeline can be run on-premises or in the cloud. See the following topics for more information.

- Exposing on-premises data sources to cloud-based applications on page 41
- Connecting an application in the cloud to on-premises data sources on page 42.

In addition, after at least one installation of the Hybrid Data Pipeline server, you can modify your environment to use an external JRE at runtime as opposed to the embedded JRE that is shipped with the product package. See External JRE support and integration on page 42.

Standalone deployment

Hybrid Data Pipeline configuration depends in part on whether you are deploying the service on a standalone node or deploying the service on one or more nodes behind a load balancer. The standalone deployment simplifies installation and administration of the service. For this reason, the standalone deployment is an efficient way to test proof of concepts and evaluate the service. In a standalone deployment, the service is installed on a single host machine and queries must be directed to this machine.

Hybrid Data Pipeline is largely configured during the installation process. The following configuration details should be addressed before installation to ensure a successful standalone deployment.

- Login credentials for standalone deployment on page 14

  Passwords for the default administrator and user accounts must be specified during installation of the Hybrid Data Pipeline server. When initially logging in to the Web UI or using the API, you must authenticate as one of these users.

- System database for standalone deployment on page 14

  A system database is required for storing user and configuration information. For standalone deployments, you can use either the embedded internal database or a supported external database to serve as the system database. However, an external system database should be used in production environments.

- Shared files and the key location for standalone deployment on page 18

  The installation program creates shared files used in the operation of the data access service. During installation, you choose where and how these files should be stored. In a production environment, the files used to connect to the system database should be secured on a machine separate from the machines hosting the Hybrid Data Pipeline service and the system database. In addition, all shared files should be backed up as a matter of best practices. In the case of system failure, these backups can be used to restore the service.

- Access ports for standalone deployment on page 19

  The access ports used for Hybrid Data Pipeline should be enabled for incoming traffic and unallocated for other purposes.

- SSL certificates for standalone deployment on page 20

To implement SSL/TLS in a Hybrid Data Pipeline environment, an SSL certificate file must be specified during installation. For standalone deployments, a self-signed certificate is available for testing or evaluation purposes, but a PEM file should be specified to enable SSL in a production environment.

- Application and driver configuration for standalone deployment on page 24

  Applications and drivers must be properly configured to ensure a successful deployment of the service.

- Firewall and port redirection using iptables for standalone deployment on page 25

  Hybrid Data Pipeline Web UI and API endpoints are exposed by default on port 8080 for HTTP connections or port 8443 for HTTPS connections. The iptables firewall utility can be used to route connections from the standard HTTP port 80 and HTTPS port 443 to these endpoints.

Login credentials for standalone deployment

You must specify passwords for the default *d2cadmin* and *d2cuser* accounts during installation of the Hybrid Data Pipeline server. The default password policy is not enforced during installation of the server. However, best practices recommend that you follow the default password policy when specifying these account passwords. When initially logging in to the Web UI or using Hybrid Data Pipeline APIs, you must authenticate as one of these users.

Hybrid Data Pipeline default password policy

After installation, Hybrid Data Pipeline enforces the following password policy by default.

- The password must contain at least 8 characters.
- The password must not contain more than 12 characters. A password with a length of 12 characters is acceptable.
- The password must not contain the username.
- Characters from at least three of the following four groups must be used in the password:
  - Uppercase letters A-Z
  - Lowercase letters a-z
  - Numbers 0-9
  - Non-white space special characters

System database for standalone deployment

Hybrid Data Pipeline requires a system database for storing user and configuration information. When deploying the service on a standalone node, you can opt to use either the embedded internal database or a supported external database. A standalone installation with an internal system database is the quickest way to get Hybrid Data Pipeline up and running. With this deployment, the service can be installed and administered from a single machine. This deployment is an efficient way to test and evaluate the service. However, for a production environment, an external system database should be used. An external system database provides better security and more flexibility for backing up system information. As a best practice, the external system database should be replicated, or mirrored, to promote the continuous availability of the service. Configuring Hybrid Data Pipeline to use a system database occurs during installation.

External system databases

Hybrid Data Pipeline requires a system database for storing sensitive information used in the operation of the data access service. For a standalone node deployment, you can opt to use either the embedded internal database or a supported external database. For a load balancer deployment, you must use an external database. Depending on the external database you are using, certain requirements must be met. See the following sections for details.

- Supported databases on page 15
- Oracle requirements
- MySQL Community Edition requirements on page 16
- Microsoft SQL Server requirements on page 17
- PostgreSQL requirements on page 17

Supported databases

Note: Hybrid Data Pipeline supports Amazon RDS instances that are compatible with these supported database versions.

Database	Version
Microsoft Azure SQL Database	Microsoft Azure SQL Database 11
Microsoft SQL Server	Microsoft SQL Server 2016 Microsoft SQL Server 2014
MySQL Community Edition	Support based on MySQL Connector/J 5.1[1]
Oracle Database	Oracle 12c R1, R2 (12.1, 12.2) Oracle 11g R2 (11.2)
PostgreSQL	PostgreSQL 11

[1] Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. MySQL Connector/J 5.1 must be used to support the use of MySQL Community Edition as an external system database. Therefore, you should refer to the MySQL Connector/J 5.1 documentation for information on supported versions of MySQL Community Edition.

Oracle requirements

If you plan to store system information in an external Oracle database, you must provide the following information.

- Hostname (server name or IP address)
- Port information for the database. The default is `1521`.
- SID or Service Name
- Administrator and user account information
  - An administrator name and password. The administrator must have the following privileges:
    - CREATE SESSION
    - CREATE TABLE
    - CREATE ANY SYNONYM
    - CREATE SEQUENCE
    - CREATE TRIGGER
  - A user name and password for a standard account. The standard user must have the CREATE SESSION privileges.

MySQL Community Edition requirements

If you plan on to use a MySQL Community Edition database as an external system database, you must provide the following.

- A MySQL Connector/J driver, version 5.1, and its location

  To download the driver, visit the MySQL developer website at https://dev.mysql.com/.
- Hostname (server name or IP address)
- Port information for the database. The default is `3306`.
- Database Name
- Administrator and user account information:
  - An administrator user name and password. The administrator must have the following privileges:
    - ALTER
    - CREATE
    - DROP
    - DELETE
    - INDEX
    - INSERT
    - REFERENCES
    - SELECT
    - UPDATE
  - A user name and password for a standard account. The standard user must have the following privileges:
    - DELETE

- INSERT
- SELECT
- UPDATE

Microsoft SQL Server requirements

If you plan to store system information in an external SQL Server database, you must take the following steps when setting up the SQL Server database.

1. Create a database schema to be used for storing Hybrid Data Pipeline system information.
2. Create an administrator who can access the newly created schema. The administrator must have the CREATE TABLE privileges.
3. Create a user who can access the newly created schema. The user must have the CREATE SESSION privileges.

After the SQL Server database has been setup, you must provide the following information during installation:

- Hostname (server name or IP address)
- Port information for the database. The default is `1433`.
- Database Name
- Schema Name
- Administrator and user account information
  - An administrator name and password. The administrator must have the CREATE TABLE privileges.
  - A user name and password for a standard account. The user must have the CREATE SESSION privileges.

PostgreSQL requirements

If you plan to store system information on an external PostgreSQL database, you must take the following steps when setting up the PostgreSQL database.

1. Enable the `citext` PostgreSQL extension.
2. Create a database schema to be used for storing Hybrid Data Pipeline system information.
3. Create an administrator who can access the newly created schema. The administrator must have privileges to create tables.
4. Create a user who can access the newly created schema. The user must have privileges to select, insert, update, delete, and sequence tables.

After the PostgreSQL database has been setup, you must provide the following information during installation:

- Hostname (server name or IP address)
- Port information for the database. The default is `5432`.
- Database Name
- Administrator and user account information
  - An administrator name and password. The administrator must have privileges to create tables.
  - A user name and password for a standard account. The user must have privileges to select, insert, update, delete, and sequence tables.

Shared files and the key location for standalone deployment

Hybrid Data Pipeline requires the specification of a *key location* during installation. For a standalone deployment, if you use the default key location, the installation program writes the shared files used in the operation of the data access service to the local keystore directory (<install_dir>/ddcloud/keystore). If you specify a different location as the key location, the installation program writes the shared files to two separate locations. The files necessary for connecting to the system database are stored in the specified location, while files tied to the Hybrid Data Pipeline server are stored in the local keystore directory (<install_dir>/ddcloud/keystore).

In a production environment, the files used to connect to the system database should be secured on a machine separate from the machines hosting the Hybrid Data Pipeline service and the system database. Therefore, a separate location should be specified for the key location.

Whether located in a single directory or two separate directories, all shared files should be backed up as a matter of best practices. In the case of system failure, these backups can be used to restore the service.

Note: During installation of the Hybrid Data Pipeline server, four configuration and certificate files are generated. These files are used in the installation of components, including the ODBC driver, the JDBC driver, and the On-Premises Connector. In a standalone node installation, the location of these files is independent of the shared location. These files are written to the <install_dir>/redist directory.

Shared files

The following files are used to connect to the system database. When the default location is used for the key location, these files are stored in the local keystore directory (<install_dir>/ddcloud/keystore). When a non-default location is used, these files are stored in the location specified during installation.

- .backup: A backup copy of the contents of the install directory from the previous install. This is used to restore the contents of the directory if there is an error during an upgrade.
- key: Reference to the file containing the encryption key for the Hybrid Data Pipeline database.
- key00: Encryption key for the system database. This key is used to encrypt sensitive information such as data source user IDs and passwords, security tokens, access tokens and other user or data source identifying information. If this is not present, or was over written during the installation, then you will not be able decrypt any of the encrypted information in the system database.
- key-cred: Encryption key for credentials contained in Hybrid Data Pipeline configuration files. Examples of credentials in the config files include the user ID and password information for the system database.
- db/*: Encrypted information about the system database. The contents of these files are encrypted using the key-cred key. Used by the installer when performing an upgrade or installing on an additional node. If these are not present, or do not have valid encoding, the installation or upgrade will fail.
- dddrivers/*: A directory of internally supported drivers that have been updated after a product upgrade.
- drivers/*: The directory used for integrating third party drivers with Hybrid Data Pipeline.
- plugins/*: JAR files for external authentication plugins

The following files are tied to the Hybrid Data Pipeline server. They are stored in the local keystore directory (<install_dir>/ddcloud/keystore) whether or not the default key location is specified during installation.

- authKey: Authentication key for the On-Premises Connector. This key is used to encrypt the user ID and password information in the On-Premises Connector configuration file. The key in this file is encrypted using a key built into the On-Premises Connector. This encrypted key is included in the OnPremise.properties configuration file distributed with the On-Premises Connector. If this is overwritten or incorrect, the On-Premises Connector will not be able to authenticate with Hybrid Data Pipeline.

- `ddcloud.jks`: Sun SSL keystore. This keystore contains the Hybrid Data Pipeline server SSL certificate if the SSL termination is done at the Hybrid Data Pipeline server.
- `ddcloud.bks`: Bouncy Castle SSL keystore. This keystore contains the same SSL certificate as the `ddcloud.jks` keystore. This keystore is in the Bouncy Castle keystore format and is used when the server is configured to run in FIPS compliant mode. Should only be present with FIPS enabled.
- `ddcloudTrustStore.jks`: Sun SSL truststore. This trustore contains the root CA certificate needed to validate the server SSL certificate. This truststore is distributed with the On-Premises Connector and with the ODBC and JDBC drivers, allowing these components to validate the Hybrid Data Pipeline server certificate.
- `ddcloudTrustStore.bks`: Bouncy Castle SSL truststore. Should only be present with FIPS enabled. This truststore contains the root CA certificate needed to validate the server SSL certificate in the Bouncy Castle keystore format. The Bouncy Castle SSL library does not use the default Java `cacerts` file, so this truststore is populated with the contents of the default `cacerts` file and the root certificate needed to validate the Hybrid Data Pipeline server certificate. Should only be present with FIPS enabled.
- `key-opc`: Contains the unencrypted encryption key. The `authKey` above contains the encrypted version of this key. This key is not shipped with the On-Premises Connector.

Access ports for standalone deployment

Multiple access ports on the machine hosting the Hybrid Data Pipeline server must be opened and unassigned to other functions. The following tables document the required ports and default port numbers for standalone deployments. The installation program for the Hybrid Data Pipeline server confirms that default ports are available and allows new port values to be assigned when needed. Port values are passed during the installation of Hybrid Data Pipeline servers.

Server Access Port

For a standalone installation, a Server Access Port must be available across the firewall of the Hybrid Data Pipeline server. Using an HTTPS port is recommended.

Name	Default	Description
HTTP Port	8080	Port that exposes Hybrid Data Pipeline
HTTPS Port	8443	SSL port that exposes Hybrid Data Pipeline

Server Internal Ports

The Shutdown Port must be opened. However, as a matter of best practice, the Shutdown Port should not be available outside the firewall of the Hybrid Data Pipeline server. For a standalone node installation, a port for the Internal API must be opened. Using the Internal API SSL Port is recommended.

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Internal API SSL Port	8090	SSL port for the Internal API
Shutdown Port	8005	Shutdown port

On-Premises Access Ports

The Message Queue Port must be opened. For a standalone node installation with the On-Premises Connector, the On-Premises Access Port and a Notification Server Port must be available across the firewall. Using the SSL port is recommended.

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
SSL Port	11443	SSL port for the Notification Server
Message Queue Port	8282	Port for the message queue

SSL certificates for standalone deployment

To implement SSL/TLS in a Hybrid Data Pipeline environment, an SSL certificate file must be specified during installation. In a standalone deployment, the Hybrid Data Pipeline server needs a server certificate and all intermediate certificates all the way to the root of the certificate chain to establish trust. During installation, you can specify a self-signed certificate for testing or evaluation purposes. However, as documented below, a PEM file should be specified to enable SSL in a production environment.

Note: The ODBC driver, JDBC driver, and On-Premises Connector need only the root certificate to verify the trust of the server certificate supplied during the SSL handshake. During installation of the server, the required certificate files are written to the `<install_dir>/redist` directory. These and other files in the `redist` directory must be used in the installation of the ODBC driver, JDBC driver, and On-Premises Connector.

An SSL/TLS implementation secures the following communications in a standalone deployment.

- Communications between a Hybrid Data Pipeline user and the Hybrid Data Pipeline Web UI.
- Communications between applications using the REST API, including the OData API, and the Hybrid Data Pipeline server.
- Communications between the JDBC or ODBC drivers and the Hybrid Data Pipeline server.
- Communications between the On-Premises Connector and the Hybrid Data Pipeline server.

The PEM file

To implement SSL/TLS, a standalone Hybrid Data Pipeline deployment should be configured with a server certificate issued by a certificate authority. For a client to verify the authenticity of a certificate, it needs to be able to verify the signatures of all of the certificates in the chain. As such, the entire certificate chain must be supplied when configuring the Hybrid Data Pipeline server including the root certificate.

A PEM file must consist of a private key, a CA server certificate, and additional certificates that make up the trust chain. The trust chain must contain a root certificate and, if needed, intermediate certificates.

A PEM encoded file includes Base64 data. The private key is prefixed with a "-----BEGIN PRIVATE KEY-----" line and postfixed with an "-----END PRIVATE KEY-----". Certificates are prefixed with a "-----BEGIN CERTIFICATE-----" line and postfixed with an "-----END CERTIFICATE-----" line. Text outside the prefix and postfix lines is ignored and can be used for metadata.

You may need to create a PEM file by converting different key and certificate files into separate PEM files, and then concatenating these files into a single PEM file. In some cases, you may need to first convert key and certificate files into a PKCS12 (pfx) file and then convert the PKCS12 file into a PEM file. The PEM file should include the private key and required certificates, as shown in PEM file format on page 21.

PEM file format

A PEM file must consist of a private key, a CA server certificate, and additional certificates that make up the trust chain. The trust chain must contain a root certificate and, if needed, intermediate certificates.

A PEM encoded file includes Base64 data. The private key is prefixed with a "-----BEGIN PRIVATE KEY-----" line and postfixed with an "-----END PRIVATE KEY-----". Certificates are prefixed with a "-----BEGIN CERTIFICATE-----" line and postfixed with an "-----END CERTIFICATE-----" line. Text outside the prefix and postfix lines is ignored and can be used for metadata.

The following example PEM file contains a private key, a CA server certificate, one intermediate trust chain certificate, and a root certificate. The ellipses (...) represent additional lines of text in the certificate or key that have been removed.

```
# Private key
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDBj08sp5++4anG
cmQxJjAkBgNVBAoTHVByb2dyZXNzIFNvZnR3YXJlIENvcnBvcmF0aW9uMSAwHgYD
VQQDDBcqLmF3cy10ZXN0LnByb2dyZXNzLmNvbTCCASIwDQYJKoZIhvcNAQEBBQAD
...
bml6YXRpb252YWxzaGEyZzIuY3JsMIGgBggrBgEFBQcBAQSBkzCBkDBNBggrBgEF
BQcwAoZBaHR0cDovL3NlY3VyZS5nbG9iYWxzaWduLmNvbS9jYWNlcnQvZ3Nvcmdh
z3P668YfhUbKdRF6S42Cg6zn
-----END PRIVATE KEY-----

# Server CA certificate
-----BEGIN CERTIFICATE-----
MIIFaDCCBFCgAwIBAgISESHkvZFwK9Qz0KsXD3x8p44aMA0GCSqGSIb3DQEBCwUA
VQQDDBcqLmF3cy10ZXN0LnByb2dyZXNzLmNvbTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAMGPTyynn77hqcYnjWsMwOZDzdhVFY93s2OJntMbuKTHn39B
...
bml6YXRpb252YWxzaGEyZzIuY3JsMIGgBggrBgEFBQcBAQSBkzCBkDBNBggrBgEF
BQcwAoZBaHR0cDovL3NlY3VyZS5nbG9iYWxzaWduLmNvbS9jYWNlcnQvZ3Nvcmdh
bml6YXRpb252YWxzaGEyZzJyMS5jcnQwPwYIKwYBBQUHMAGGM2h0dHA6Ly9vY3Nw
lffygD5IymCSuuDim4qB/9bh7oi37heJ4ObpBIzroPUOthbG4gv/5blW3Dc=
-----END CERTIFICATE-----

# Trust chain intermediate certificate
-----BEGIN CERTIFICATE-----
MIIEaTCCA1GgAwIBAgILBAAAAAABRE7wQkcwDQYJKoZIhvcNAQELBQAwVzELMAkG
C33JiJ1Pi/D4nGyMVTXbv/Kz6vvjVudKRtkTIso21ZvBqOOWQ5PyDLzm+ebomchj
SHh/VzZpGhkdWtHUfcKc1H/hgBKueuqI6lfYygoKOhJJomIZeg0k9zfrtHOSewUj
...
dHBzOi8vd3d3Lmdsb2JhbHNpZ24uY29tL3JlcG9zaXRvcnkvMDMGA1UdHwQsMCow
KKAmoCSGImh0dHA6Ly9jcmwuZ2xvYmFsc2lnbi5uZXQvcm9vdC5jcmwwPQYIKwYB
K1pp74P1S8SqtCr4fKGxhZSM9AyHDPSsQPhZSZg=
-----END CERTIFICATE-----

# Trust chain root certificate
-----BEGIN CERTIFICATE-----
MIIDdTCCAl2gAwIBAgILBAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzELMAkG
YWxTaWduIG52LXNhMRAwDgYDVQQLEwdSb290IENBMRswGQYDVQQDExJHbG9iYWxT
aWduIFJvb3QgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDaDuaZ
...
jc6j40+Kfvvxi4Mla+pIH/EqsLmVEQS98GPR4mdmzxzdzxtIK+6NiY6arymAZavp
38NflNUVyRRBnMRddWQVDf9VMOyGj/8N7yy5Y0b2qvzfvGn9LhJIZJrglfCm7ymP
HMUfpIBvFSDJ3gyICh3WZlXi/EjJKSZp4A==
-----END CERTIFICATE-----
```

See also

The PEM file on page 20
Generating a PEM file on page 22

Generating a PEM file

A PEM file must consist of a private key, a CA server certificate, and additional certificates that make up the trust chain. The trust chain must contain a root certificate and, if needed, intermediate certificates.

You may need to create a PEM file by converting different key and certificate files into separate PEM files, and then concatenating these files into a single PEM file. In some cases, you may need to first convert key and certificate files into a PKCS12 file and then convert the PKCS12 file into a PEM file. The resulting PEM file should include the private key and required certificates, as shown in PEM file format on page 21.

The following sections describe a number of ways to convert key and certificate files, using OpenSSL or the Java keytool as appropriate.

- Converting a PKCS12 (pfx) file to a PEM file on page 22
- Converting a Java jks keystore file to a PKCS12 file on page 23
- Converting PKCS7 (p7b) file certificates to PEM file certificates on page 23
- Converting PKCS7 file certificates to PKCS12 file certificates and adding the private key to the PKCS12 file on page 23
- Converting DER certificates to PEM file certificates on page 24
- Creating a PEM file from a private key and Base64 encoded certificates on page 24

Converting a PKCS12 (pfx) file to a PEM file

1. Use the following OpenSSL command to determine whether the private key is password protected.

   ```
   openssl pkcs12 -info -in target.pfx
   ```

   a. If the key is password protected, you will be prompted for a password. Proceed to **Step 2**.

   b. If the key is not password protected, then information on the PKCS12 file, such as file structure and algorithms used, is provided. Proceed to **Step 5**.

2. Enter the password when prompted. Information on the PKCS12 file, such as file structure and algorithms used, is provided.
3. Use the following OpenSSL command to extract the private key from the PKCS12 file.

   ```
   openssl pkcs12 -in target.pfx -nocerts -out ppkey.pem
   ```

4. Remove the passphrase from the private key. Then, skip to **Step 6**.

   ```
   openssl rsa -in ppkey.pem -out privatekey.pem
   ```

5. Use the following OpenSSL command to extract the private key from the PKCS12 file.

   ```
   openssl pkcs12 -in target.pfx -nocerts -out privatekey.pem
   ```

6. Extract the root certificates from the PKCS12 file.

   ```
   openssl pkcs12 -in rootcert.pfx -cacerts -nodes -nokeys > rootcert.pem
   ```

7. Extract server certificates from the PKCS12 file.

```
openssl pkcs12 -in servercert.pfx -clcerts -nodes -nokeys > servercert.pem
```

8. Concatenate the certificates and private key in a single PEM file. In this example, the Linux/UNIX `cat` command is used to concatenate root certificate, server certificate, and private key.

```
cat rootcert.pem servercert.pem privatekey.pem > server.bundle.pem
```

9. Confirm that the PEM file has the private key and the required certificates as described in PEM file format on page 21.

The resulting `server.bundle.pem` file should be specified during the installation of the Hybrid Data Pipeline server.

Converting a Java jks keystore file to a PKCS12 file

A Java jks keystore file must first be converted to a PKCS12 file. The PKCS12 file can then be converted to a PEM file.

1. Use the following Java keytool command to convert the jks file into a pfx file.

```
keytool -importkeystore -srckeystore keystore.jks -srcstoretype JKS -deststoretype
PKCS12 -destkeystore target.pfx
```

2. Enter the keystore password and keystore file alias when prompted.
3. Use the resulting `target.pfx` file to create a PEM file by following the instructions in Converting a PKCS12 (pfx) file to a PEM file on page 22.

Converting PKCS7 (p7b) file certificates to PEM file certificates

These instructions assume that the private key is already available as a PEM file.

1. Use the following OpenSSL command to convert PKCS7 file certificates to PEM file certificates.

```
openssl pkcs7 -print_certs -in certificates.p7b -out certificates.pem
```

2. Concatenate the certificate and private key files. In this example, the Linux/UNIX `cat` command is used.

```
cat certificates.pem privatekey.pem > server.bundle.pem
```

3. Confirm that the resulting PEM file has the private key and the required certificates as described in PEM file format on page 21.

The resulting `server.bundle.pem` file should be specified during the installation of the Hybrid Data Pipeline server.

Converting PKCS7 file certificates to PKCS12 file certificates and adding the private key to the PKCS12 file

After the certificate and private key files have been converted to the PKCS12 format, the PKCS12 file can then be converted to a PEM file.

1. Use the following OpenSSL command to convert a PKCS7 file to a PKCS12 file.

```
openssl pkcs7 -print_certs -in certificate.p7b -out certificate.cer
```

2. Use the following command to add the private key to the PKCS12 file.

```
openssl pkcs12 -export -in certificate.cer -inkey privatekey.key -out target.pfx
-certfile CACert.cer
```

3. Use the resulting `target.pfx` file to create a PEM file by following the instructions in Converting a PKCS12 (pfx) file to a PEM file on page 22.

Converting DER certificates to PEM file certificates

The DER extension is used for binary DER files. These files may also use the CER and CRT extensions.

These instructions assume that the private key is already available as a PEM file.

1. Use the following OpenSSL command to convert DER certificates to PEM file certificates.

```
openssl x509 -inform der -in certificates.cer -out certificates.pem
```

2. Concatenate the certificate and private key files. In this example, the Linux/UNIX `cat` command is used.

```
cat certificates.pem privatekey.pem > server.bundle.pem
```

3. Confirm that the PEM file has the private key and the required certificates as described in PEM file format on page 21.

The resulting `server.bundle.pem` file should be specified during the installation of the Hybrid Data Pipeline server.

Creating a PEM file from a private key and Base64 encoded certificates

PEM files use Base64 encoding. Therefore, no conversion process is required. However, the Base64 encoded certificates and the private key must be concatenated in a single PEM file.

These instructions assume that the private key is already available as a PEM file.

1. Concatenate the certificate and private key files. In this example, the Linux/UNIX `cat` command is used.

```
cat Base64rootcert.pem Base64servercert.pem privatekey.pem > server.bundle.pem
```

2. Confirm that the PEM file has the private key and the required certificates as described in PEM file format on page 21

The resulting `server.bundle.pem` file should be specified during the installation of the Hybrid Data Pipeline server.

See also

The PEM file on page 20
PEM file format on page 21

Application and driver configuration for standalone deployment

Client applications must be appropriately configured. In conjunction with ODBC and JDBC applications, ODBC and JDBC drivers will also need to be configured. OData applications will need their own modifications.

For the most part, configuration of the ODBC and JDBC drivers is handled during the installation of the drivers. If the drivers are installed using the configuration files generated by the Hybrid Data Pipeline server installation, then they will use the DNS of the host machine. Nevertheless, you may wish to configure the drivers in other ways.

OData applications must be modified to use the DNS of the host machine for HTTP or HTTPS requests. In addition, OData applications should be configured for SSL as appropriate.

Firewall and port redirection using iptables for standalone deployment

Hybrid Data Pipeline Web UI and API endpoints are exposed by default on port 8080 for HTTP connections or port 8443 for HTTPS connections. The iptables firewall utility can be used to route connections from the standard HTTP port 80 and HTTPS port 443 to these endpoints. In this scenario, ports 80 and 443 will be accessible to everyone, while ports 8080 and 8443 are only accessible to processing running on the server.

The instructions in the following topics can be applied to RedHat 7, Oracle 7 and Centos 7 distributions of Linux.

Please see the documentation for your Linux distribution for more information about configuring the firewall.

Note: If you are using a Suse 12 distribution of Linux, use the YaST2 Firewall setting GUI to configure your firewall. In Suse 12 you can find the firewall setting under **Applications > System Tools > YaST > Adiministrator Settings/Security and Users/Firewall**.

Disabling firewalld

If you are using a later version of Linux, it may have come configured with the newer firewalld software. Consult the documentation for firewalld to determine how to configure it in a similar way, and how to disable firewalld and use iptables.

To disable firewalld, use the following commands in a console window.

```
systemctl disable firewalld
```

```
systemctl stop firewalld
```

Installing iptables

Installing iptable requires root privileges.

1. Log in with an admin account.
2. Run `sudo -s`
3. Use `yum` to install the iptables services:
   a) `yum install iptables`
   b) `yum install iptables-ipv6`

Creating the iptables configuration file

Create the file /etc/sysconfig/iptables containing the content displayed here (your configuration may be slightly different). This will require root privileges.

```
# Generated by iptables-save v1.4.21 on Thu Jun 23 09:05:43 2016
*nat
:PREROUTING ACCEPT [1100:133346]
:INPUT ACCEPT [1:48]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A PREROUTING -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 8080
-A PREROUTING -p tcp -m tcp --dport 443 -j REDIRECT --to-ports 8443
-A PREROUTING -p tcp --dport 8080 -j MARK --set-mark 1
-A PREROUTING -p tcp --dport 8443 -j MARK --set-mark 2
COMMIT
# Completed on Thu Jun 23 09:05:43 2016
# Generated by iptables-save v1.4.21 on Thu Jun 23 09:05:43 2016
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [378:34583]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -m mark --mark 1 -j DROP
-A INPUT -p tcp -m state --state NEW -m tcp --dport 8080 -j ACCEPT
-A INPUT -m mark --mark 2 -j DROP
-A INPUT -p tcp -m state --state NEW -m tcp --dport 8443 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A INPUT -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
# Completed on Thu Jun 23 09:05:43 2016
```

Starting the iptables service

Start the iptables service using the `service` command.

```
service iptables start
```

Load balancer deployment

Hybrid Data Pipeline configuration depends in part on whether you are deploying the service on a standalone node or deploying the service on one or more nodes behind a load balancer. A load balancer deployment offers high availability and scalability, and is therefore the best option for production environments. In a load balancer deployment, the service is installed on one or more nodes behind a load balancer. Requests are handled by the load balancer which distributes requests across nodes.

Hybrid Data Pipeline is largely configured during the installation process. When installing the service on multiple nodes behind a load balancer, the initial installation of the Hybrid Data Pipeline server is used as a template for installations on additional nodes. The following configuration details should be addressed before installation to ensure a successful load balancer deployment.

- Login credentials for load balancer deployment on page 27

  Passwords for the default administrator and user accounts must be specified during installation of the Hybrid Data Pipeline server. When initially logging in to the Web UI or using the API, you must authenticate as one of these users.

- Load balancer configuration on page 28

  Hybrid Data Pipeline can be deployed on one or more nodes behind a load balancer to provide high availability and scalability. Hybrid Data Pipeline supports two types of load balancers.

  - Network load balancers that support the TCP tunneling protocol (such as HAProxy)
  - Cloud load balancers that support the WebSocket protocol (such as the AWS application load balancer and the Azure application gateway)

- System database for load balancer deployment on page 34

  A system database is required for storing user and configuration information. For load balancer deployments, an external database is required to serve as the system database. As a best practice, the external system database should be replicated, or mirrored, to promote the continuous availability of the service.

- Shared files and the key location for load balancer deployment on page 38

  The specification of a *key location* is required during installation. The installation program writes shared files used in the operation of the data access service to this directory. As a matter of best practices, the key location should be secured on a machine separate from the machines hosting the Hybrid Data Pipeline service or the machine hosting the system database.

- Access ports for load balancer deployment on page 39

  The access ports used for Hybrid Data Pipeline should be enabled for incoming traffic and unallocated for other purposes.

- SSL certificates for load balancer deployment on page 39

  SSL/TLS encrypted communications between client applications and the load balancer are supported. In addition, all communications between the On-Premises Connector and the load balancer are SSL/TLS encrypted. SSL connections between the load balancer and the Hybrid Data Pipeline nodes are currently not supported.

- Client application configuration for load balancer deployment on page 40

  Applications and drivers must be properly configured to ensure a successful deployment of the service.

- Browser configuration for load balancer deployment on page 41

  For load balancer deployments, the browser you use to connect to the Web UI must have cookies enabled.

Login credentials for load balancer deployment

You must specify passwords for the default *d2cadmin* and *d2cuser* accounts during installation of the Hybrid Data Pipeline server. The default password policy is not enforced during installation of the server. However, best practices recommend that you follow the default password policy when specifying these account passwords. When initially logging in to the Web UI or using Hybrid Data Pipeline APIs, you must authenticate as one of these users.

Hybrid Data Pipeline default password policy

After installation, Hybrid Data Pipeline enforces the following password policy by default.

- The password must contain at least 8 characters.
- The password must not contain more than 12 characters. A password with a length of 12 characters is acceptable.
- The password must not contain the username.

- Characters from at least three of the following four groups must be used in the password:
  - Uppercase letters A-Z
  - Lowercase letters a-z
  - Numbers 0-9
  - Non-white space special characters

Load balancer configuration

The Hybrid Data Pipeline product package does not include a load balancer. However, Hybrid Data Pipeline can be deployed on one or more nodes behind a load balancer to provide high availability and scalability. Hybrid Data Pipeline supports two types of load balancers: network load balancers that support the TCP tunneling protocol and cloud load balancers that support the WebSocket protocol. In turn, the load balancer must be configured to support the Hybrid Data Pipeline environment according to the following criteria.

- The load balancer must be configured to accept HTTPS connections on port 443 and unencrypted HTTP connections on port 80.
- The load balancer must be configured for SSL termination to support encrypted communications between clients and the load balancer. The configuration of the load balancer depends in part on the type of SSL certificate supplied. See SSL certificates for load balancer deployment on page 39 for details.
- The load balancer must support session affinity. The load balancer must either be configured to supply its own cookies or to pass the cookies generated by the Hybrid Data Pipeline service back to the client. The Hybrid Data Pipeline service provides a cookie named `C2S-SESSION` that can be used by the load balancer. For ODBC and JDBC applications, the ODBC and JDBC drivers automatically use cookies for session affinity. OData applications should be configured to echo cookies for optimal performance.
- The load balancer must pass the hostname in the Host header when a request is made to an individual Hybrid Data Pipeline node. For example, if the hostname used to access the cluster is `hdp.mycorp.com` and the individual nodes behind the load balancer have the hostnames `hdpsvr1.mycorp.com`, `hdpsvr2.mycorp.com`, `hdpsvr3.mycorp.com`, then the Host header in the request forwarded to the Hybrid Data Pipeline node must be the load balancer hostname `hdp.mycorp.com`.
- The load balancer must supply the X-Forwarded-Proto header to indicate to the Hybrid Data Pipeline node whether the request was received by the load balancer as an HTTP or HTTPS request.
- The load balancer must supply the X-Forwarded-For header for IP address filtering. The X-Forwarded-For header is also required if the client IP address is needed for Hybrid Data Pipeline access logs. If the X-Forwarded-For header is not supplied, the IP address in the access logs will always be the load balancer's IP address.
- The load balancer may be configured to run HTTP health checks against nodes with the Health Check API.
- Additional configuration is required for the following scenarios.
  - If you are using the On-Premises Connector with a network load balancer such as HAProxy, see Configuring a network load balancer with the On-Premises Connector on page 29 for additional configuration requirements.
  - If you are using the On-Premises Connector with a cloud load balancer such as the AWS Application Load Balancer or the Azure Application Gateway, see Configuring a cloud load balancer with the On-Premises Connector on page 32 for additional configuration details.

Configuring a network load balancer with the On-Premises Connector

When running Hybrid Data Pipeline behind a network load balancer with an On-Premises Connector, the load balancer must be configured to route requests for on-premises data sources to the correct server nodes.

There are two general steps involved in configuring your load balancer to support on-premises data access. First, a custom Access Control List must be created to direct requests for the On-Premises Connector to cluster nodes. Second, a backend notification pool that specifies the on-premises port for each cluster node must be created. The following instructions explain how an HAProxy load balancer can be configured to support Hybrid Data Pipeline access to backend data sources using the On-Premises Connector. These instructions may be adapted for other load balancers, such as NGINX and F5.

The Hybrid Data Pipeline installation program automatically generates an HAProxy configuration file for each installation of the server. These HAProxy configuration files are written to the `HAProxy` subdirectory in the key location directory specified during installation. These files must be merged to create a single HAProxy configuration file for a load balancer deployment of Hybrid Data Pipeline.

Take the following steps to create an HAProxy configuration file for a load balancer deployment using the On-Premises Connector.

1. Create an Access Control List (ACL) to direct requests for the On-Premises Connector to each Hybrid Data Pipeline server.

   Note: Options 1 and 2 below may be used in combination.

   - **Option 1.** Use a custom header to direct requests. Each entry should be prefaced with `acl`.

     In this example, the custom header `X-DataDirect-OPC-Host` is used to direct requests to the server `service2.myserver.com` through the default On-Premises Port `40501`.

     ```
     acl is_opa_hdr_service2_myserver_com_40501 hdr(X-DataDirect-OPC-Host)
     -i opa_service2_myserver_com_40501
     use_backend opa_service2_myserver_com_40501 if is_opa_hdr_service2_myserver_com_40501
     ```

   - **Option 2.** Use URL routing to direct requests. Each entry should be prefaced with `acl`.

     In this example, URL routing is used to direct requests to the server `service2.myserver.com` through the default On-Premises Port `40501`.

     ```
     acl is_opa_url_service2_myserver_com_40501 path_end
     -i /connect/opa_service2_myserver_com_40501
     use_backend opa_service2_myserver_com_40501 if is_opa_url_service2_myserver_com_40501
     ```

2. Add each Hybrid Data Pipeline server to the backend notification pool section using the `server` keyword.

   In the following example, the server `server2.myserver.com` has been added to the `backend hdp_notification_pool section`, and health checks have been enabled at the root with the `option httpchk` property.

   ```
   backend hdp_notification_pool
       mode http
       option http-tunnel
       balance roundrobin
       option httpchk HEAD /
       http-check expect status 200

       #HDP Notification Server Definitions
       server server1.myserver.com 11.22.111.105:11280 check
       server server2.myserver.com 11.22.111.106:11280 check
   ```

3. Create a backend pool that specifies the On-Premises Port for each Hybrid Data Pipeline server that supports the On-Premises Connector by adding a backend section to the configuration file.

   For example, the following `backend` section is for a node on the `service2.myserver.com` server using the default On-Premises Port `40501`. Health checks have been enabled at the root with the `option httpchk` property.

```
backend opa_service2_myserver_com_40501
    mode http
    option http-tunnel
    option httpchk HEAD /
    http-check expect status 200
    server service2.myserver.com 11.22.111.106:40501 check
```

4. Add each Hybrid Data Pipeline server to the default backend pool using the `server` keyword.

   In the following example, `server2.myserver.com` has been added to the `backend hdp_default_backend` pool, and health checks have been enabled by specifying the `/api/healthcheck` endpoint with the `option httpchk` property.

```
backend hdp_default_backend
     mode http
     balance roundrobin
     option httpchk HEAD /api/healthcheck
     http-check expect status 200
     cookie HDP_SESSION insert nocache

     #HDP Server Definitions
     server service1.myserver.com 11.22.11.105:8080 check cookie service1.myserver.com

     server service2.myserver.com 11.22.111.106:8080 check cookie service2.myserver.com
```

Example

The following example demonstrates an HAProxy configuration file for using the load balancer with two server nodes that have the On-Premises connector enabled, `server1.myserver.com` and `server2.myserver.com`. To create this file, the required sections were copied from the generated configuration file for `service2.myserver.com` into the generated file for `service1.myserver.com`. Copied sections are indicated with comments.

```
global
        log 127.0.0.1 local0
        chroot /var/lib/haproxy

        daemon

defaults
        log     global
        mode    http
        option  httplog
        option  dontlognull
        timeout connect 5s
        timeout client  15m
        timeout server  15m

#---------------------------------------------------------------------
# Configuration for OPC with load balancer.
#---------------------------------------------------------------------
frontend lb_opc_nodes
    bind *:80
     #Replace /common/hdpsmoke/shared/redist/ddcloud.pem with the location of the
     #loadbalancers SSL certificate
     bind *:443 ssl crt /common/hdpsmoke/shared/redist/ddcloud.pem

     #In production port 80 should be a permanent  redirected to 443 by uncommenting the
```

```
     #following line
     #redirect scheme https code 301 if !{ ssl_fc }

    mode http
    default_backend hdp_default_backend

     #Define rules for HDP Notification Servers
     acl is_hdp_notification2 path_end -i /connect/X_DataDirect_Notification_Server
     use_backend hdp_notification_pool if is_hdp_notification2

    acl is_hdp_notification hdr(X-DataDirect-OPC-Host) -i X_DataDirect_Notification_Server

     use_backend hdp_notification_pool if is_hdp_notification

     #Rules for on-premises connection to service.myserver.com
     acl is_url_opa_service1_myserver_com_40501  path_end
     -i /connect/opa_service1_myserver_com_40501
    use_backend opa_service1_myserver_com_40501 if is_url_opa_service1_myserver_com_40501


     acl is_hdr_opa_service1_myserver_com_40501 hdr(X-DataDirect-OPC-Host)
     -i opa_service1_myserver_com_40501
    use_backend opa_service1_myserver_com_40501 if is_hdr_opa_service1_myserver_com_40501


    #Rules for on-premises connection to service2.myserver.com. These rules were copied

     #from the service2.myserer.com configuration file.
     acl is_url_opa_service2_myserver_com_40501  path_end
     -i /connect/opa_service2_myserver_com_40501
    use_backend opa_service2_myserver_com_40501 if is_url_opa_service2_myserver_com_40501


     acl is_hdr_opa_service2_myserver_com_40501 hdr(X-DataDirect-OPC-Host)
     -i opa_service2_myserver_com_40501
    use_backend opa_service2_myserver_com_40501 if is_hdr_opa_service2_myserver_com_40501

backend hdp_notification_pool
     mode http
     option http-tunnel
     balance roundrobin
     option httpchk HEAD /
     http-check expect status 200

 #HDP Notification Server Definitions
     server service1.myserver.com 11.22.111.105:11280 check
     #The following server argument was copied from the service2.myserver.com
     #configuration file
     server service2.myserver.com 11.22.111.106:11280 check


backend opa_service1_myserver_com_40501
     mode http
     option http-tunnel
     option httpchk HEAD /
     http-check expect status 200
     server service1.myserver.com 11.22.111.105:40501 check

#The following section was copied from the service2.myserver.com configuration file.
backend opa_service2_myserver_com_40501
     mode http
     option http-tunnel
     option httpchk HEAD /
     http-check expect status 200
     server service2.myserver.com 11.22.111.106:40501 check

backend hdp_default_backend
     mode http
```

```
    balance roundrobin
    option httpchk HEAD /api/healthcheck
    http-check expect status 200
    cookie HDP_SESSION insert nocache

#HDP Server Definitions
    server service1.myserver.com 11.22.11.105:8080 check cookie service1.myserver.com
    #The following server argument was copied from the service2.myserver.com
    #configuration file
    server service2.myserver.com 11.22.111.106:8080 check cookie service2.myserver.com
```

Configuring a cloud load balancer with the On-Premises Connector

Hybrid Data Pipeline can be deployed on a web service, such as Amazon Web Services or Microsoft Azure, behind a cloud load balancer that supports the WebSocket protocol. When using an On-Premises Connector, the cloud load balancer must be configured to route requests for on-premises data sources to the correct server nodes.

The instructions in this section describe how an Amazon Web Services load balancer must be configured to support Hybrid Data Pipeline. These instructions assume that you have completed the following deployment tasks.

- Created a Virtual Private Cloud (VPC) to host a Hybrid Data Pipeline environment.
- Created AWS compute instances in the VPC for each node that will be used to support the Hybrid Data Pipeline environment.
- Provisioned an RDS database instance to operate as a system database for storing user and configuration information.
- Created a file system on a node in the VPC to be used as the key location for shared files.
- Installed the Hybrid Data Pipeline server on each node that will be hosting the service.
  - The key location specified during the initial installation must reside on a node in the VPC.
  - The system database specified during initial installation must be the RDS database instance for storing user and configuration information.
- Created an AWS Application Load Balancer in the VPC to connect to Hybrid Data Pipeline.

The following general steps must be taken to configure routing and listening rules in the AWS Application Load Balancer. The corresponding topics provide detailed instruction for each step.

1. Create a target group for default routing to the Hybrid Data Pipeline service API on page 32
2. Create a target group for notifications on page 33
3. Create a target group for on-premises access on page 33
4. Configure target routing on page 34

Once the Application Load Balancer has been configured with listener and target group rules, you can install On-Premises Connectors.

Create a target group for default routing to the Hybrid Data Pipeline service API

Take the following steps to create a target group for default routing.

1. Use the AWS console to create a load balancer target group.
2. Specify target group details.

```
Name - <Name for your HDP cluster nodes>
Protocol – HTTP
Port 8080
Target type – Instance
VPC <Name of your VPC>
```

3. Set up health checks.

```
Protocol: HTTP
Port: 8080
Path: /api/healthcheck
```

4. Save the target group.
5. Register each Hybrid Data Pipeline instance as a target on port 8080.
6. Set the stickiness attribute for the target group to 5 minutes.

Create a target group for notifications

Take the following steps to create a target group for notifications.

1. Use the AWS console to create a load balancer target group.
2. Specify target group details.

```
Target Group Name: <Name for your Notification Server Group>
Protocol HTTP
Port 11280
Target type instance
VPC <Name of your VPC>
```

3. Set up health checks.

```
Protocol: HTTP
Path: /
Port: Select traffic port
```

4. Save the target group.
5. Register each Hybrid Data Pipeline instance as a target on port 11280.
6. Disable stickiness via the stickiness attribute.

Create a target group for on-premises access

Take the following steps to create a target group for on-premises access.

1. Use the AWS console to create a load balancer target group.
2. Specify target group details.

```
Target Group Name: <Name for your 1st OPA Target Group>
Protocol HTTP
Port 40501
Target type instance
VPC <Name of your VPC>
```

3. Set up health checks.

```
Protocol: HTTP
Path: /
Port: Select traffic port
```

4. Save the target group.
5. Register the first Hybrid Data Pipeline instance as a target on port 40501.
6. Disable stickiness via the stickiness attribute.
7. Repeat steps 1 through 6 for each Hybrid Data Pipeline instance.

Configure target routing

Take the following steps to configure target routing.

1. Create a rule to route to the notifications target group by setting **Path is** to `/connect/X_DataDirect_Notification_Server`.

   Note: For load balancers that support routing with HTTP headers, the header `X-DataDirect-OPC-Host:X_DataDirect_Notification_Server` should be used.

2. For each node running the Hybrid Data Pipeline service, create a rule to route to the corresponding on-premises access target by setting **Path is** to `/connect/<opa_routing_key>`.

   Note: The format of the `<opa_routing_key>` is `opa_<hosturl>_<opaport>` where `<hosturl>` is the hostname specified during installation with dot characters replaced by underscores, and `<opaport>` is the On-Premises Access port number. For example, the routing key for `nc-d2c02.americas.test.com` on port 40501 would be `opa_nc-d2c73_americas_test_com_40501`.

3. Create a default routing rule. The **Forward to** attribute should be set to the Hybrid Data Pipeline service API target group.

   Important: Setting the default rule for routing requests to the Hybrid Data Pipeline service API must be completed after creating the rules for routing to the On-Premises Access and Notifications servers.

System database for load balancer deployment

Hybrid Data Pipeline requires a system database for storing user and configuration information. When deploying the service behind a load balancer, you must use a supported external database. An external system database ensures that user and configuration information is consistent across multiple nodes behind the load balancer. These nodes use the system information on the external system database to access data and return successful queries. In addition, an external system database provides better security and more flexibility for backing up system information. As a best practice, the external system database should be replicated, or mirrored, to promote the continuous availability of the service. Configuring Hybrid Data Pipeline to use a system database occurs during installation.

External system databases

Hybrid Data Pipeline requires a system database for storing sensitive information used in the operation of the data access service. For a standalone node deployment, you can opt to use either the embedded internal database or a supported external database. For a load balancer deployment, you must use an external database. Depending on the external database you are using, certain requirements must be met. See the following sections for details.

- Supported databases on page 35
- Oracle requirements
- MySQL Community Edition requirements on page 36
- Microsoft SQL Server requirements on page 37
- PostgreSQL requirements on page 37

Supported databases

Note: Hybrid Data Pipeline supports Amazon RDS instances that are compatible with these supported database versions.

Database	Version
Microsoft Azure SQL Database	Microsoft Azure SQL Database 11
Microsoft SQL Server	Microsoft SQL Server 2016 Microsoft SQL Server 2014
MySQL Community Edition	Support based on MySQL Connector/J 5.1[2]
Oracle Database	Oracle 12c R1, R2 (12.1, 12.2) Oracle 11g R2 (11.2)
PostgreSQL	PostgreSQL 11

[2] Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. MySQL Connector/J 5.1 must be used to support the use of MySQL Community Edition as an external system database. Therefore, you should refer to the MySQL Connector/J 5.1 documentation for information on supported versions of MySQL Community Edition.

Oracle requirements

If you plan to store system information in an external Oracle database, you must provide the following information.

- Hostname (server name or IP address)
- Port information for the database. The default is `1521`.
- SID or Service Name
- Administrator and user account information
  - An administrator name and password. The administrator must have the following privileges:
    - CREATE SESSION
    - CREATE TABLE
    - CREATE ANY SYNONYM
    - CREATE SEQUENCE
    - CREATE TRIGGER
  - A user name and password for a standard account. The standard user must have the CREATE SESSION privileges.

MySQL Community Edition requirements

If you plan on to use a MySQL Community Edition database as an external system database, you must provide the following.

- A MySQL Connector/J driver, version 5.1, and its location

  To download the driver, visit the MySQL developer website at https://dev.mysql.com/.
- Hostname (server name or IP address)
- Port information for the database. The default is `3306`.
- Database Name
- Administrator and user account information:
  - An administrator user name and password. The administrator must have the following privileges:
    - ALTER
    - CREATE
    - DROP
    - DELETE
    - INDEX
    - INSERT
    - REFERENCES
    - SELECT
    - UPDATE
  - A user name and password for a standard account. The standard user must have the following privileges:
    - DELETE

- INSERT
- SELECT
- UPDATE

Microsoft SQL Server requirements

If you plan to store system information in an external SQL Server database, you must take the following steps when setting up the SQL Server database.

1. Create a database schema to be used for storing Hybrid Data Pipeline system information.
2. Create an administrator who can access the newly created schema. The administrator must have the CREATE TABLE privileges.
3. Create a user who can access the newly created schema. The user must have the CREATE SESSION privileges.

After the SQL Server database has been setup, you must provide the following information during installation:

- Hostname (server name or IP address)
- Port information for the database. The default is `1433`.
- Database Name
- Schema Name
- Administrator and user account information
  - An administrator name and password. The administrator must have the CREATE TABLE privileges.
  - A user name and password for a standard account. The user must have the CREATE SESSION privileges.

PostgreSQL requirements

If you plan to store system information on an external PostgreSQL database, you must take the following steps when setting up the PostgreSQL database.

1. Enable the `citext` PostgreSQL extension.
2. Create a database schema to be used for storing Hybrid Data Pipeline system information.
3. Create an administrator who can access the newly created schema. The administrator must have privileges to create tables.
4. Create a user who can access the newly created schema. The user must have privileges to select, insert, update, delete, and sequence tables.

After the PostgreSQL database has been setup, you must provide the following information during installation:

- Hostname (server name or IP address)
- Port information for the database. The default is `5432`.
- Database Name
- Administrator and user account information
  - An administrator name and password. The administrator must have privileges to create tables.
  - A user name and password for a standard account. The user must have privileges to select, insert, update, delete, and sequence tables.

Shared files and the key location for load balancer deployment

Hybrid Data Pipeline requires the specification of a *key location* during installation. The installation program writes shared files used in the operation of the data access service to this directory. For a load balancer deployment, the key location must be accessible to the node or nodes running the service.

Shared files

The following files are stored in the key location for a load balancer deployment.

- `.backup`: A backup copy of the contents of the install directory from the previous install. This is used to restore the contents of the directory if there is an error during an upgrade.
- `key`: Reference to the file containing the encryption key for the Hybrid Data Pipeline database.
- `key00`: Encryption key for the system database. This key is used to encrypt sensitive information such as data source user IDs and passwords, security tokens, access tokens and other user or data source identifying information. If this is not present, or was over written during the installation, then you will not be able decrypt any of the encrypted information in the system database.
- `key-cred`: Encryption key for credentials contained in Hybrid Data Pipeline configuration files. Examples of credentials in the config files include the user ID and password information for the system database.
- `db/*`: Encrypted information about the system database. The contents of these files are encrypted using the `key-cred` key. Used by the installer when performing an upgrade or installing on an additional node. If these are not present, or do not have valid encoding, the installation or upgrade will fail.
- `dddrivers/*`: A directory of internally supported drivers that have been updated after a product upgrade.
- `drivers/*`: The directory used for integrating third party drivers with Hybrid Data Pipeline.
- `plugins/*`: JAR files for external authentication plugins.
- `authKey`: Authentication key for the On-Premises Connector. This key is used to encrypt the user ID and password information in the On-Premises Connector configuration file. The key in this file is encrypted using a key built into the On-Premises Connector. This encrypted key is included in the `OnPremise.properties` configuration file distributed with the On-Premises Connector. If this is overwritten or incorrect, the On-Premises Connector will not be able to authenticate with Hybrid Data Pipeline.
- `ddcloud.jks`: Sun SSL keystore. This keystore contains the Hybrid Data Pipeline server SSL certificate if the SSL termination is done at the Hybrid Data Pipeline server.
- `ddcloud.bks`: Bouncy Castle SSL keystore. This keystore contains the same SSL certificate as the `ddcloud.jks` keystore. This keystore is in the Bouncy Castle keystore format and is used when the server is configured to run in FIPS compliant mode. Should only be present with FIPS enabled.
- `ddcloudTrustStore.jks`: Sun SSL truststore. This trustore contains the root CA certificate needed to validate the server SSL certificate. This truststore is distributed with the On-Premises Connector and with the ODBC and JDBC drivers, allowing these components to validate the Hybrid Data Pipeline server certificate.
- `ddcloudTrustStore.bks`: Bouncy Castle SSL truststore. Should only be present with FIPS enabled. This truststore contains the root CA certificate needed to validate the server SSL certificate in the Bouncy Castle keystore format. The Bouncy Castle SSL library does not use the default Java `cacerts` file, so this truststore is populated with the contents of the default `cacerts` file and the root certificate needed to validate the Hybrid Data Pipeline server certificate. Should only be present with FIPS enabled.
- `key-opc`: Contains the unencrypted encryption key. The `authKey` above contains the encrypted version of this key. This key is not shipped with the On-Premises Connector.
- `global.properties`: Stores properties and other information shared between nodes in a cluster.

- `redist/*`: Redistributable files. These files are used to install the On-Premises Connector and the ODBC and JDBC drivers.

Access ports for load balancer deployment

Multiple access ports on nodes hosting the Hybrid Data Pipeline server must be opened and unassigned to other functions. The following tables document the required ports and default port numbers. The installation program for the Hybrid Data Pipeline server confirms that default ports are available and allows new port values to be assigned when needed. Port values are passed during the installation of Hybrid Data Pipeline servers.

Server Access Port

A Server Access Port must be opened for the load balancer. As a matter of best practices, the load balancer should be configured for SSL/TLS termination.

Name	Default	Description
HTTP Port	8080	Port that exposes Hybrid Data Pipeline

Server Internal Ports

The Shutdown Port must be opened. However, as a matter of best practice, the Shutdown Port should not be available outside the firewall of the Hybrid Data Pipeline server. For a load balancer installation, the Internal API Port on any node must be open to all the other nodes in the cluster. The Internal API Port should not be available outside the firewall.

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Shutdown Port	8005	Shutdown port

On-Premises Access Ports

The Message Queue Port must be opened. For a load balancer installation with the On-Premises Connector, the On-Premises Access Port and the TCP Notification Server Port must be opened for the load balancer.

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
Message Queue Port	8282	Port for the message queue

SSL certificates for load balancer deployment

The following SSL encrypted communications are supported for a load balancer deployment.

- Communications between the browser and the Hybrid Data Pipeline Web UI when the load balancer is configured for SSL.
- Communications between applications using the REST API, including the OData API, and the load balancer.

- Communications between the JDBC or ODBC drivers and the load balancer.
- Communications between the On-Premises Connector and the load balancer.

Important: SSL connections between the load balancer and the Hybrid Data Pipeline nodes are currently not supported.

The following guidelines should be used when implementing SSL in a Hybrid Data Pipeline environment.

- The load balancer needs to be configured with the root certificate and any intermediate certificates necessary to establish the chain of trust to the root certificate.
- The root certificate must be specified as the SSL certificate during installation of the Hybrid Data Pipeline server. When intermediate certificates are required for the trust chain, then the SSL certificate must be supplied in a PEM file format. When there are no intermediate certificates, then the SSL certificate can be supplied in either DER or PEM file format.
- The SSL certificate specified during installation is used to generate the trust stores for the ODBC driver, JDBC driver, and On-Premises Connector. These files are written to the `redist` directory of the key location upon installation. Before installing the ODBC driver, the JDBC driver, or the On-Premises Connector, the trust store and properties files in the `redist` directory must be copied to the installer directory of the component you are installing.

Client application configuration for load balancer deployment

Client applications must be appropriately configured. In conjunction with ODBC and JDBC applications, ODBC and JDBC drivers will also need to be configured. OData applications will need their own modifications.

For the most part, configuration of the ODBC and JDBC drivers is handled during the installation of the drivers. If the drivers are installed using the configuration files generated by the Hybrid Data Pipeline server installation, then they will use the hostname of the load balancer or machine hosting the server. However, you may wish to configure the drivers in other ways.

OData applications must be modified to use the hostname of the load balancer for HTTP or HTTPS requests. Additionally, for optimal performance, OData applications should be configured to echo cookies for session affinity. OData applications must also be configured appropriately for SSL. See Node-to-node communication in OData Hybrid Data Pipeline load balancer environment on page 40 for details on communication between nodes when an OData client cannot be configured to echo cookies.

Node-to-node communication in OData Hybrid Data Pipeline load balancer environment

In an OData Hybrid Data Pipeline load balancer environment, the load balancer and OData clients should be configured to handle cookies to achieve session affinity and optimize OData query performance. The load balancer should supply its own cookies or pass the cookies generated by the Hybrid Data Pipeline service back to the OData client. In turn, the OData client should echo cookies to allow the load balancer to direct query requests to the node that initially received the query.

However, it is not always possible to configure an OData client to echo cookies. In such cases, Hybrid Data Pipeline uses an internal mechanism called the distributed file persistence manager. When a query is executed that requires file persistence, execution results are stored temporarily on the node that initially received the query. The manager associates the query with the node and the execution results stored there. If a request from the same query is routed to a different node in the cluster, the manager obtains the persisted execution results from the original node. The query results are then returned to the client by the node that received the request.

The distributed file persistence manager requires node-to-node communication using the HTTP protocol to achieve session affinity. The Internal API Port specified during Hybrid Data Pipeline server installation is the port used for this node-to-node communication. Data remains secure in the following respects. First, the Internal API Port (8190 default) is not exposed externally to the public facing network. Each node registers itself using this port, and communications are restricted. Second, a UUID is generated during the node registration process. This UUID is passed in as an HTTP header to confirm the validity of node-to-node communications. Third, the service stores persisted files on only a temporary basis.

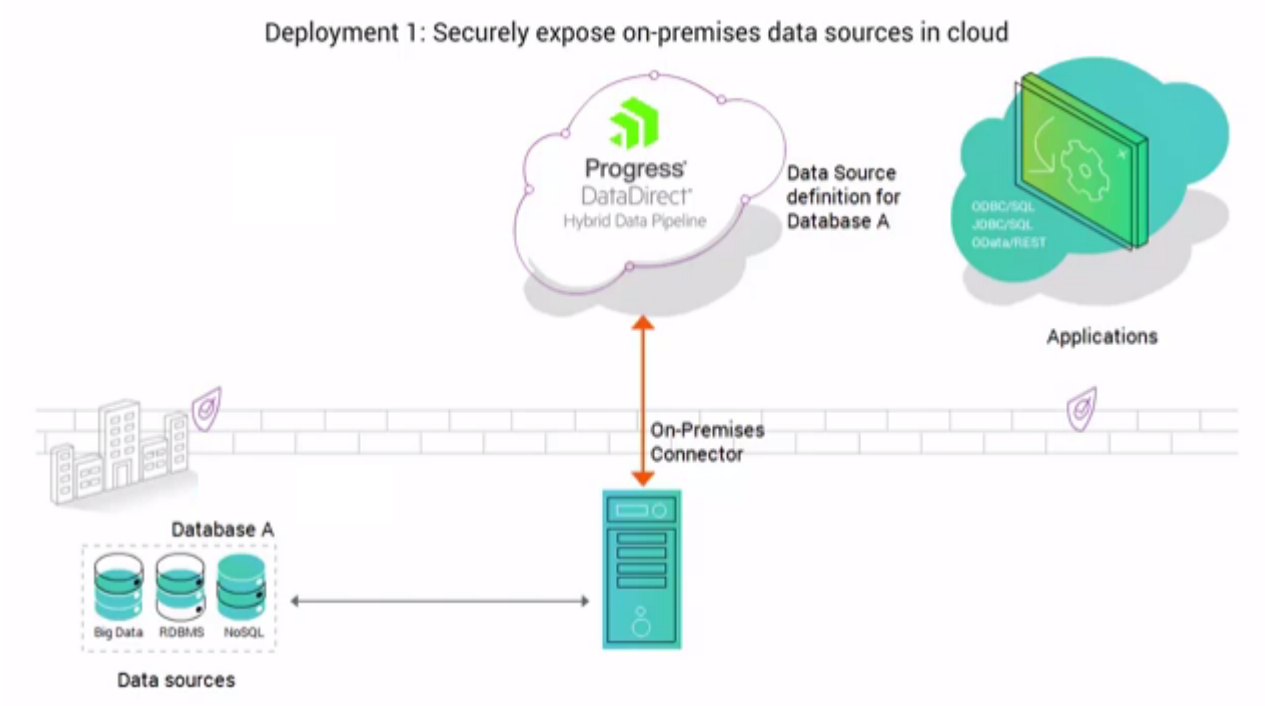
Browser configuration for load balancer deployment

For load balancer deployments of Hybrid Data Pipeline, the browser you use to connect to the Web UI must have cookies enabled.

Exposing on-premises data sources to cloud-based applications

This scenario describes a deployment where on-premises data sources are exposed for secure access by cloud-based applications. For this deployment, a Hybrid Data Pipeline server is installed in the cloud, and the On-Premises Connector is used to perform secure connections through the firewall to the backend data store. The cloud-based application is located in a separate cloud but connects with Hybrid Data Pipeline through an API such as OData, ODBC, or JDBC.

This deployment could be suitable for an independent software vendor who wants to embed Hybrid Data Pipeline services in the cloud to give the cloud application users access to their data that resides in the data center or other on-premises systems.

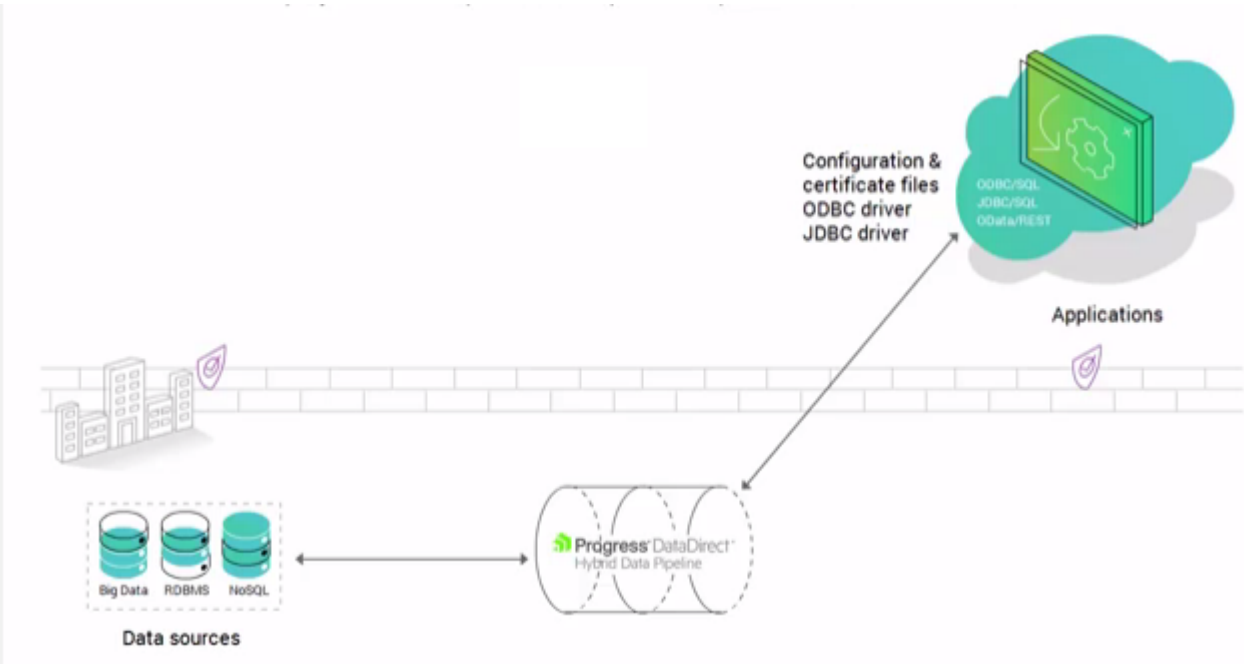


For a more detailed discussion of this scenario, watch a video.

Connecting an application in the cloud to on-premises data sources

This scenario describes a deployment where the Hybrid Data Pipeline server is installed behind a firewall with on-premises data sources while a number of applications reside in the cloud. With the Hybrid Data Pipeline server behind a firewall, a cloud-based service does not need to be maintained, and SSL can be used to secure your data.

This deployment scenario could be suitable when using cloud-based OData applications, for example, creating a real-time connectivity between Salesforce and an on-premises database.



For a more detailed discussion of this scenario, watch a video.

External JRE support and integration

Hybrid Data Pipeline uses an embedded JRE at runtime. However, you can integrate an external JRE with a standing deployment of Hybrid Data Pipeline. The following JREs are currently supported.

- Oracle Java 8 JRE
- OpenJDK 8 JRE

Hybrid Data Pipeline must be installed on at least one server before you proceed with integrating an external JRE. Files associated with the embedded JRE can then be used to modify the external JRE you wish to use with the Hybrid Data Pipeline server or the On-Premises Connector.

Note: Using an external JRE with the server is exclusive from using an external JRE with the On-Premises Connector. That is, the server can run on an external JRE while the On-Premises Connector runs on the embedded JRE, and vice versa.

The following work flow outlines the procedure for integrating an external JRE. See the corresponding topics for details.

1. Modify the external JRE.

- **Option 1**. Non-FIPS environment.
- **Option 2**. FIPS environment.

Note: FIPS is not supported for the On-Premises Connector with either embedded or external JREs.

2. If integrating the external JRE with the server, configure the server to use the JRE.
3. If integrating the external JRE with the On-Premises Connector, configure the connector to use the JRE.

Modify the external JRE for a non-FIPS environment

Take the following steps to modify an external JRE for a non-FIPS environment.

Note:

- `<hdp_install_dir>` is the installation directory of the Hybrid Data Pipeline server.
- `<external_jre_home>` is the home directory of the external JRE.

1. Enable the Unlimited Strength Jurisdiction Policy according to the JRE vendor documentation. Depending on the vendor and version, the Unlimited Strength Jurisdiction Policy may be enabled by default.

   Note: Enabling the Unlimited Strength Jurisdiction Policy is the only modification required for using an external JRE with the On-Premises Connector. Therefore, the remaining steps can be ignored if the JRE is to be used only with the On-Premises Connector.

2. Copy the `<hdp_install_dir>/ddcloud/utils/jre/lib/ext/bc-fips-1.0.0.jar` file to the `<external_jre_home>/lib/ext` directory.
3. Merge the contents of the embedded JRE `<hdp_install_dir>/ddcloud/utils/jre/lib/security/java.policy.sun` file into the external JRE `<external_jre_home>/lib/security/java.policy` file.

   Note:

   - Any previously made customizations to the `<external_jre_home>/lib/security/java.policy` should be preserved.
   - Any permissions for data sources in the embedded JRE `java.policy.sun` file should be carried over to the external JRE `java.policy` file.

4. Merge the contents of the embedded JRE `<hdp_install_dir>/ddcloud/utils/jre/lib/security/java.security.sun` file into the external JRE `<external_jre_home>/lib/security/java.security` file.

   Note:

   - Any previously made customizations to the `<external_jre_home>/lib/security/java.security` should be preserved.
   - Any properties enabled in the embedded JRE `java.security.sun` file should be carried over to the external JRE `java.security` file.

What to do next:

- Configure the server to use the external JRE.

- Configure the On-Premises Connector to use the external JRE.

Modify the external JRE for a FIPS environment

Take the following steps to modify an external JRE for a FIPS environment.

Note: FIPS is not supported for the On-Premises Connector with either embedded or external JREs.

Note:

- `<hdp_install_dir>` is the installation directory of the Hybrid Data Pipeline server.
- `<external_jre_home>` is the home directory of the external JRE.

1. Enable the Unlimited Strength Jurisdiction Policy according to the JRE vendor documentation. Depending on the vendor and version, the Unlimited Strength Jurisdiction Policy may be enabled by default.
2. Copy the `<hdp_install_dir>/ddcloud/utils/jre/lib/ext/bc-fips-1.0.0.jar` file to the `<external_jre_home>/lib/ext` directory.
3. Merge the contents of the embedded JRE `<hdp_install_dir>/ddcloud/utils/jre/lib/security/java.policy.bcfips` file into the external JRE `<external_jre_home>/lib/security/java.policy` file.

   Note:

   - Any previously made customizations to the `<external_jre_home>/lib/security/java.policy` should be preserved.
   - Any permissions for data sources in the embedded JRE `java.policy.bcfips` file should be carried over to the external JRE `java.policy` file.

4. Merge the contents of the embedded JRE `<hdp_install_dir>/ddcloud/utils/jre/lib/security/java.security.bcfips` file into the external JRE `<external_jre_home>/lib/security/java.security` file.

   Note:

   - Any previously made customizations to the `<external_jre_home>/lib/security/java.security` should be preserved.
   - Any properties enabled in the embedded JRE `java.security.bcfips` file should be carried over to the external JRE `java.security` file.

What to do next:

Configure the server to use the external JRE.

Configure the server to use the external JRE

Once you have modified the external JRE, you can configure the server to use the external JRE by performing an upgrade installation of the server. During the upgrade, you will be prompted specify whether you are using the embedded JRE or an external JRE. If you select external JRE, you must specify the path to the external JRE.

Note: For complete upgrade instructions, refer to the Progress DataDirect Hybrid Data Pipeline Installation Guide.

If you are using a response file to perform a silent upgrade, best practices recommend that you use the installation program to generate the response file. However, you may opt to edit the response file manually. If editing the response file manually, you must add Java configuration options to the response file. The options and values depend on whether the response file is based on the GUI installation template or the console mode installation template.

GUI mode

```
#Java Configuration#
------------------
SPECIFY_JAVA_HOME_NO=0
SPECIFY_JAVA_HOME_YES=1
HDP_JAVA_HOME_DIR=/usr/lib/jvm/jre-1.8.0-openjdk-1.8.0.181-3.b13.el7_5.x86_64
```

`SPECIFY_JAVA_HOME_NO` indicates whether you are using an external JRE. If you are using an external JRE, specify `0`.

`SPECIFY_JAVA_HOME_YES` indicates whether you are using an external JRE. If you are using an external JRE, specify `1`.

`HDP_JAVA_HOME_DIR` specifies the path to the external JRE to be used at runtime.

Console mode

```
#Java Configuration#
-------------------
SPECIFY_JAVA_HOME_YESNO=\"Yes\",\"\"
HDP_JAVA_HOME_DIR_CONSOLE=\"/usr/lib/jvm/java-1.8.0-openjdk-1.8.0.102-4.b14.el7.x86_64/jre\"
```

Important: The escape characters, as shown in this example, are required for a response file based on the console mode template.

`SPECIFY_JAVA_HOME_YESNO` indicates whether you are using an external JRE. If you are using an external JRE, specify `Yes`.

`HDP_JAVA_HOME_DIR_CONSOLE` specifies the path to the external JRE to be used at runtime.

What to do next:

If integrating the external JRE with the On-Premises Connector, configure the connector to use the JRE.

Configure the On-Premises Connector to use the external JRE

To use an external JRE with an On-Premises Connector, the JRE's Unlimited Strength Jurisdiction Policy must be enabled. No other modifications to the JRE are required to use it with an On-Premises Connector. Depending on the vendor and version of the JRE, the Unlimited Strength Jurisdiction Policy may be enabled by default.

Once the Unlimited Strength Jurisdiction Policy has been enabled, you can configure the On-Premises Connector to use the external JRE when installing or upgrading the connector. During installation or upgrade, you will be prompted to specify whether you are using the embedded JRE or an external JRE. If you select external JRE, you must specify the path to the external JRE. For complete installation instructions, refer to the Progress DataDirect Hybrid Data Pipeline Installation Guide.

2

Installing and upgrading the Hybrid Data Pipeline server

The Hybrid Data Pipeline server must be installed prior to installing the On-Premises Connector, the ODBC driver, or the JDBC driver. During the installation of the server, the installer generates configuration and certificate files that must be used for the installation of other supporting components.

Note: The server uses an embedded JRE at runtime. However, you can integrate an external JRE during the installation or upgrade of the server. See also External JRE support and integration on page 42.

For details, see the following topics:

- Installing the Hybrid Data Pipeline server
- Upgrading Hybrid Data Pipeline server
- Stopping and starting the Hybrid Data Pipeline service
- Uninstalling Hybrid Data Pipeline server
- Server installation log files

Installing the Hybrid Data Pipeline server

The Hybrid Data Pipeline installer supports installation of the server in GUI or console mode.

You can deploy Hybrid Data Pipeline on a standalone node, or on one or more nodes behind a load balancer.

Important: There is currently no migration path from a standalone deployment to a load balancer deployment. Therefore, a standalone deployment is not recommended for environments where scaling up the service may be desired. A standalone node deployment is also not recommended for security and system recovery purposes. If you want to move from a test environment to a production environment, you should begin by deploying Hybrid Data Pipeline on a single node behind a load balancer. When deploying the service on a single node behind a load balancer, you can increase availability and scalability as demanded, and address security and recovery concerns as required.

If you are deploying Hybrid Data Pipeline on more than one node behind a load balancer, you must install Hybrid Data Pipeline on each node in the cluster. During the initial installation of the server, the Hybrid Data Pipeline installer writes properties files, encryption keys, and system information to the *key location*. When performing subsequent installations on additional nodes, you will need to specify this key location. The installer uses the files written to the key location during the initial installation to install the server on additional nodes. Hence, for installations on additional nodes, the installer bypasses prompts for load balancing, SSL, external database, and On-Premises Connector configurations.

If you are using the silent installation process to deploy Hybrid Data Pipeline on more than one node behind a load balancer, the response file generated during the initial installation must be modified to install the server on any additional nodes. For a GUI generated response file, you will need to designate the name of an additional node with the `D2C_HOSTNAME` option. For a console generated response file, you will need to designate the name of an additional node with the `D2C_HOSTNAME_CONSOLE` option. See Silent installation process on page 72 for details.

You can also install Hybrid Data Pipeline on a standalone node for a 30 day evaluation period using a Docker image. An installation with a Docker image is for evaluation purposes. It cannot be upgraded to licensed installation, and it cannot be migrated to a load balancer environment. If you want to move from a test environment to a production environment, you should begin by deploying Hybrid Data Pipeline on a single node behind a load balancer with the Hybrid Data Pipeline installation program.

Note: Before proceeding with an installation of the Hybrid Data Pipeline server, you must copy the product file to a temporary directory, for example, `/tmp`.

- If you prefer to use a Graphical User Interface (GUI), see GUI mode installation on page 48.
- If you prefer to use the console, see Console mode installation on page 62.
- If you prefer to use a silent installation, see Silent installation process on page 72.
- If you want to install Hybrid Data Pipeline using a Docker image, see Install using a Docker image on page 103. (30 day evaluation standalone node deployment only)

GUI mode installation

After copying the downloaded product file to a temporary directory, take the following steps to install the Hybrid Data Pipeline server with the installer in GUI mode.

1. From a command-line prompt, navigate to the directory where you saved the product file. Alternatively, place the product file directory on your path before proceeding to the next step.

   The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_`*`nn`*`_LINUX_64_INSTALL.bin`, where *`nn`* is the version of the product.

2. Make the file an executable using the `chmod` command. Then, press **ENTER**. For example:

   ```
   chmod +x ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

3. Run the executable by entering the product file path and pressing **ENTER**.

a) Type the file name and path of the product file. For example:

```
./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
```

b) Press **ENTER**.

c) The **Introduction** window appears. Click **Next** to continue.

Note: If the installer cannot continue with a GUI installation, a message is displayed and the installation continues in console mode.

---

4. The License Agreement window appears. Make sure that you read and understand the license agreement. To continue with the installation, select the **I accept the terms in the License Agreement** option; then, click **Next**.

Note: You can exit the installation program at any time by clicking **Cancel** or return to the previous window by clicking **Previous**.

---

5. Choose the destination directory for the installation. Click **Next** to accept the default installation directory, or select **Choose...** to browse to a different directory, then click **Next**.

   The default installation directory is:

   ```
   /opt/Progress/DataDirect/Hybrid_Data_Pipeline/Hybrid_Server
   ```

   If you do not have `/opt` directory permissions, the installer program installs the drivers to your home directory by default. For example:

   ```
   /home/users/<username>/Progress/DataDirect/Hybrid_Data_Pipeline/Hybrid_Server
   ```

   If the directory contains an existing Hybrid Data Pipeline deployment, you can select a different directory or upgrade the existing installation. To restore the installation directory to its default setting, click **Restore Default Folder**.

6. Choose whether you want to install an evaluation or licensed version of the product. Licensed installations require a valid License Key.

   - Evaluation. Select this option to install an evaluation version that is fully functional for 30 days. Then, click **Next**.
   - Licensed. Select this option if you purchased a licensed version of the product. Type the license key, including any dashes, and then click **Next**.

7. Accept or enter the fully qualified hostname for the Hybrid Data Pipeline server. By default, the installer suggests the name of the current machine. Then, click **Next**.

Note: If the installer is unable to validate the hostname, you are prompted to reenter the hostname or skip validation. Skipping validation is often desired when performing a silent installation. See Silent installation process on page 72 for details.

---

8. Select the installation type.

   - To accept the default values for the remaining options, select **Typical (use existing settings)** and click **Next**. Continue at Step 9 on page 50.
   - To modify installation options, select **Custom (choose configuration values)** and click **Next**. Then, skip to Step 10 on page 50.

You will need to complete a custom installation if you plan to do any of the following:

- Specify the key location. The key location serves as a location for shared files used in the installation and operation of the server. The key location should be secured on a system separate from the system that stores encrypted data, or encrypts or decrypts data.
- Change the Java configuration to use an external JRE
- Enable FIPS
- Use a load balancer
- Change an SSL configuration
- Use MySQL Community Edition as a data store
- Store system information in an external MySQL Community Edition, Oracle, or SQL Server database
- Specify non-default values for ports used by the Hybrid Data Pipeline service
- Use On-Premises Connectors for secure access to on-premises data sources from the cloud

9. Specify passwords for the *d2cadmin* and *d2cuser* user accounts. Continue at Step 14 in "Standalone installation (GUI mode)".

   Best practices recommend that you follow the Hybrid Data Pipeline default password policy when specifying these account passwords. When initially logging in to the Web UI or using the API, you must authenticate as one of these users.

10. Specify the key location. The key location serves as a location for shared files used in the installation and operation of the server. The key location should be secured on a system separate from the system that stores encrypted data, or encrypts or decrypts data.

    - Select **Use default location** to use the default location for a standalone installation. This option cannot be used for a load balancer installation. The default location is `install_dir/ddcloud/keystore`. Click **Next** and proceed to Standalone installation (GUI mode) on page 51.
    - Select **Specify location** to specify a location other than the default for either a standalone installation or a load balancer installation. (Note that you must specify a location for a load balancer installation.) Click **Next** and continue to the next step.

11. Specify passwords for the *d2cadmin* and *d2cuser* user accounts.

    Best practices recommend that you follow the Hybrid Data Pipeline default password policy when specifying these account passwords. When initially logging in to the Web UI or using the API, you must authenticate as one of these users.

12. Select the desired Java configuration.

    Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

    - Select **Use default Java** if you will be using the embedded JRE installed with the server.
    - Select **Java home directory** and provide the path to an external JRE if you will be using a JRE not installed with the server.

13. Select whether you want to enable FIPS on the Hybrid Data Pipeline server.

Important: To implement FIPS, your hardware must support secure random, or you must have a secure random daemon installed.

14. Select whether you will install the Hybrid Data Pipeline server behind a load balancer.
    - Select **Yes** for an installation behind a load balancer. Click **Next**. In the **Hostname** field, type the name or IP address of the server hosting your load balancer. Then, press **ENTER**. Continue at Load balancer installation (GUI mode) on page 57.
    - Select **No** for a standalone installation. Then, click **Next**. Continue at Standalone installation (GUI mode) on page 51.

Standalone installation (GUI mode)

1. Depending on your environment, provide the appropriate SSL certificate information.
    - Select **Certificate file** to specify a PEM file to be used by the server to establish SSL connections with ODBC and JDBC client applications. Type the full path to the PEM file, or click **Choose...** to browse to the location of the PEM file. Then, click **Next**.

      Note: The PEM file must consist of a private key, a public key certificate issued by a certificate authority (CA), and additional certificates that make up the trust chain. See The PEM file on page 20 for more information.
    - Select **Use existing Certificate** to use the self-signed certificate included with the installation. Then, click **Next**.

      Note: The self-signed certificate may be used in a test environment. However, for production, a PEM file with required information should be specified. See The PEM file on page 20 for more information.
2. Select MySQL Community Edition if you plan to use MySQL Community Edition as an external system database or as a data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. However, you can use the MySQL Connector/J driver to use MySQL Community Edition as an external system database or as a data source. If you select MySQL Community Edition, enter the name and location of the MySQL Connector/J jar file in the **Jar Path** field. Then, click **Next** to continue.

   For more information on the MySQL Connector/J driver, refer to the MySQL developer website at https://dev.mysql.com/.
3. Select the type of database you want to use to store system information.
    - Select **Internal Database (supplied by this install)** to use the default internal database. Click **Next** to continue. Proceed to the next step.
    - Select **External Database** to store the system information in an external database. Then, from the drop down box, choose your database vendor. Then, click **Next**.
        - Select **Oracle**, and continue at Step 5 on page 52.
        - Select **MySQLCommunity**, and continue at Step 6 on page 52.
        - Select **MSSQLServer**, and continue at Step 7 on page 52.
        - Select **PostgreSQL**, and continue at Step 8 on page 53.

Note: Users and data sources created in the internal database are specific to the internal database. They are not migrated to the external database if you subsequently modify the Hybrid Data Pipeline server to use an external database.

4. Enter the database port for the internal database. If your environment has already defined a function for the default port, the installer pops up a message so that you can specify a different port. Click **Next**, and continue at Step 10 on page 53.
5. Provide the Oracle connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Select the connection type. Do one of the following:
      - If you connect using the Oracle System Identifier (SID), select **Connect using SID**, then type the SID.
      - Select **Connect using Service Name**, then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name. The global database name typically comprises the database name and domain name.
   d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret;serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

   e) Click **Next**, and continue at Step 9 on page 53.
6. Provide connection information for the MySQL Community Edition external database.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection url. Values should be entered as an ampersand-separated list of *parameter=value*.
   e) Click **Next**, and continue at Step 9 on page 53.
7. Provide the SQL Server connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Type the name of the schema.

e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.

f) Click **Next**, and continue at Step 9 on page 53.

8. Provide the PostgreSQL connection information.

a) Type the name of the host.

b) Type the port number.

c) Type the database name.

d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.

e) Click **Next**Administrator credentials are only required at install, and continue at Step 9 on page 53.

9. Provide the external database credential information.

Note: Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.

Note: If the installer is unable to validate, you are prompted to reenter credentials or skip validation. Skipping validation is often desired when performing a silent installation. See Silent installation process on page 72 for details.

- In the **Admin Username** field, type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- In the **Admin Password** field, type the password for an database administrator account.
- In the **Username** field, type a user name. The standard user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- In the **Password** field, type the user password.

10. Review the Server Access Ports. A Server Access Port must be available to the end user across the firewall. Best security practices recommend using an HTTPS port.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

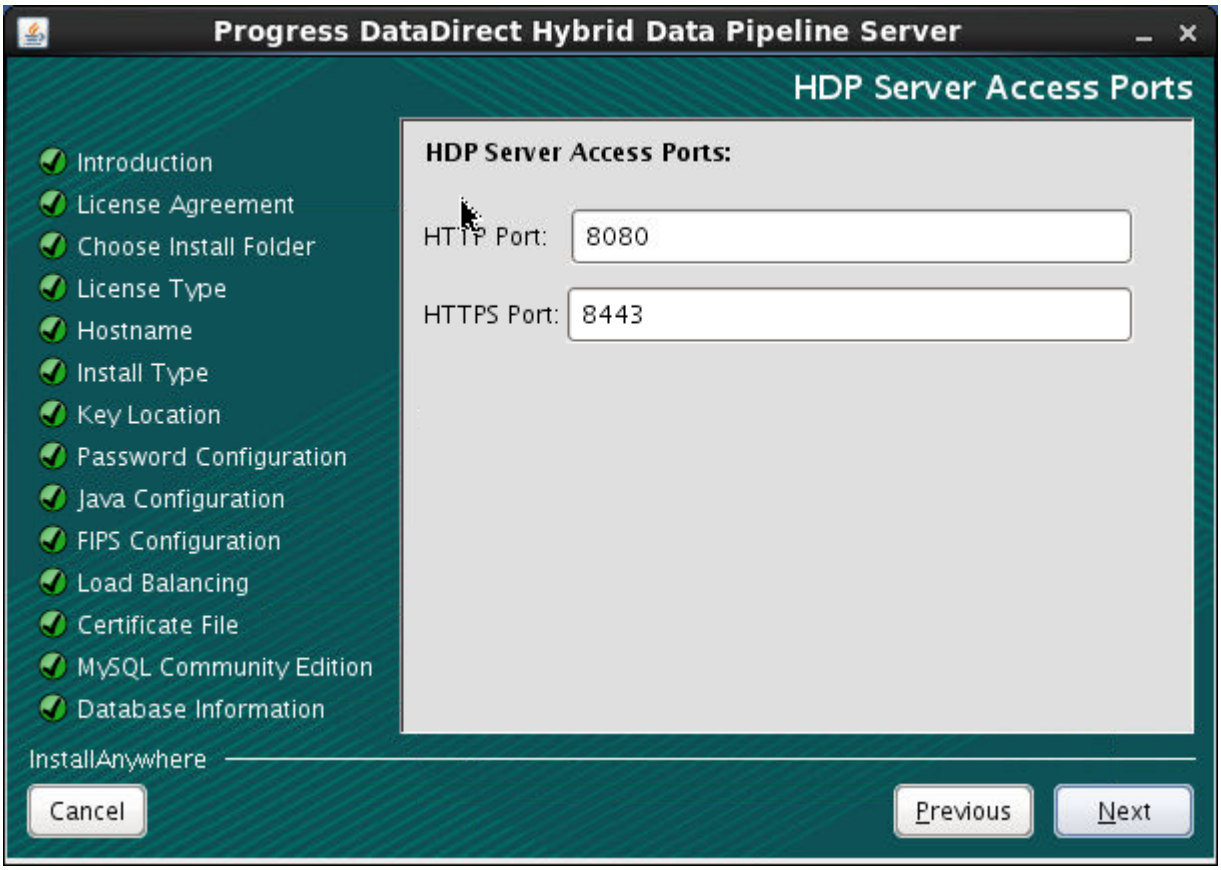


Table 1: Server Access Ports

Name	Default	Description
HTTP Port	8080	Port that exposes Hybrid Data Pipeline
HTTPS Port	8443	SSL port that exposes Hybrid Data Pipeline

11. Select whether you are using the On-Premises Connector.
    - If using the On-Premises Connector, select **Enable On-Premises Connector**. Click **Next** and continue to the next step.
    - If not using the On-Premises Connector, leave the check box empty and click **Next**. Continue at Step 13 on page 55.
12. Review the On-Premises Access Ports. The On-Premises Access Port and a Notification Server Port must be available across the firewall. Best security practices recommend using the SSL Notification Server Port.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

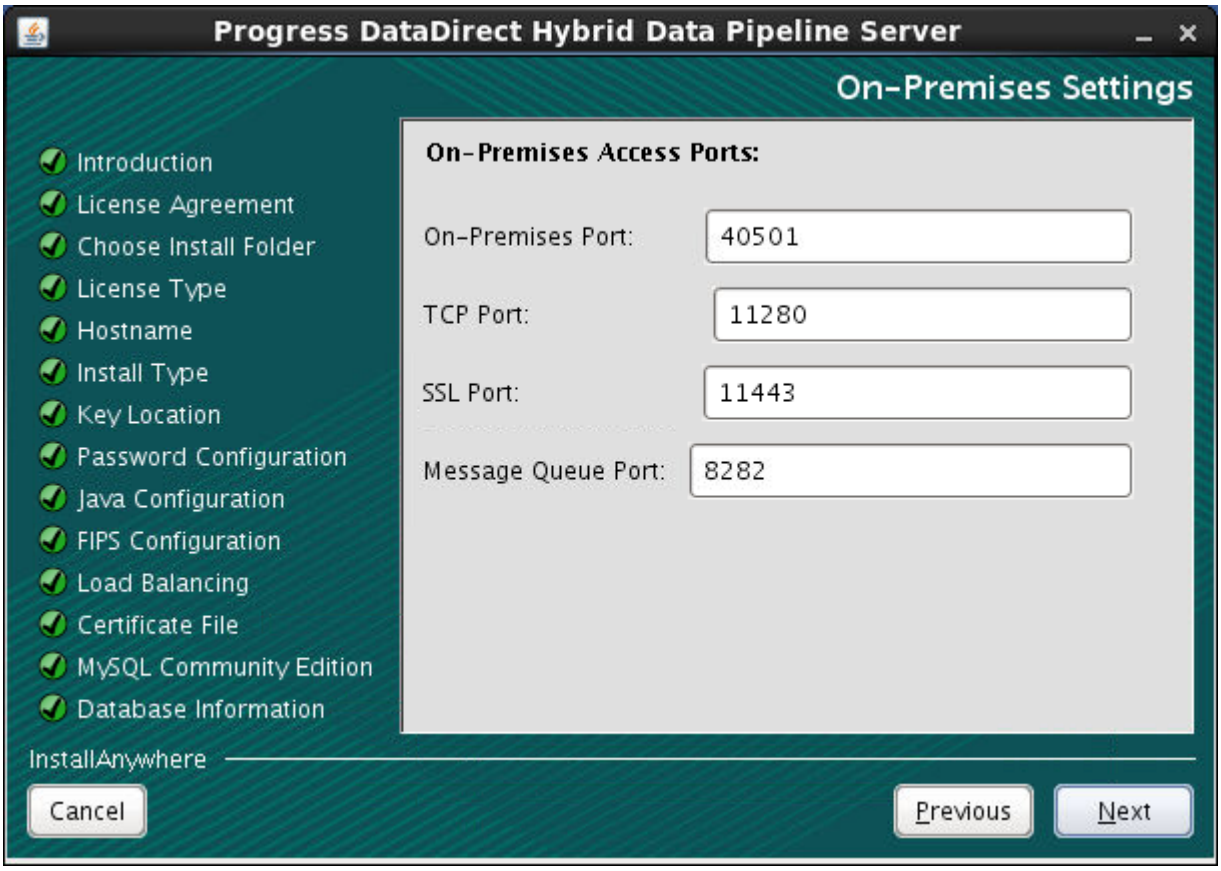


Table 2: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
SSL Port	11443	SSL port for the Notification Server
Message Queue Port	8282	Port for the message queue

13. Review the Server Internal Ports. A port for the internal API and the Shutdown Port must be opened. Best security practices recommend using the Internal API SSL Port.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of the Hybrid Data Pipeline instance.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

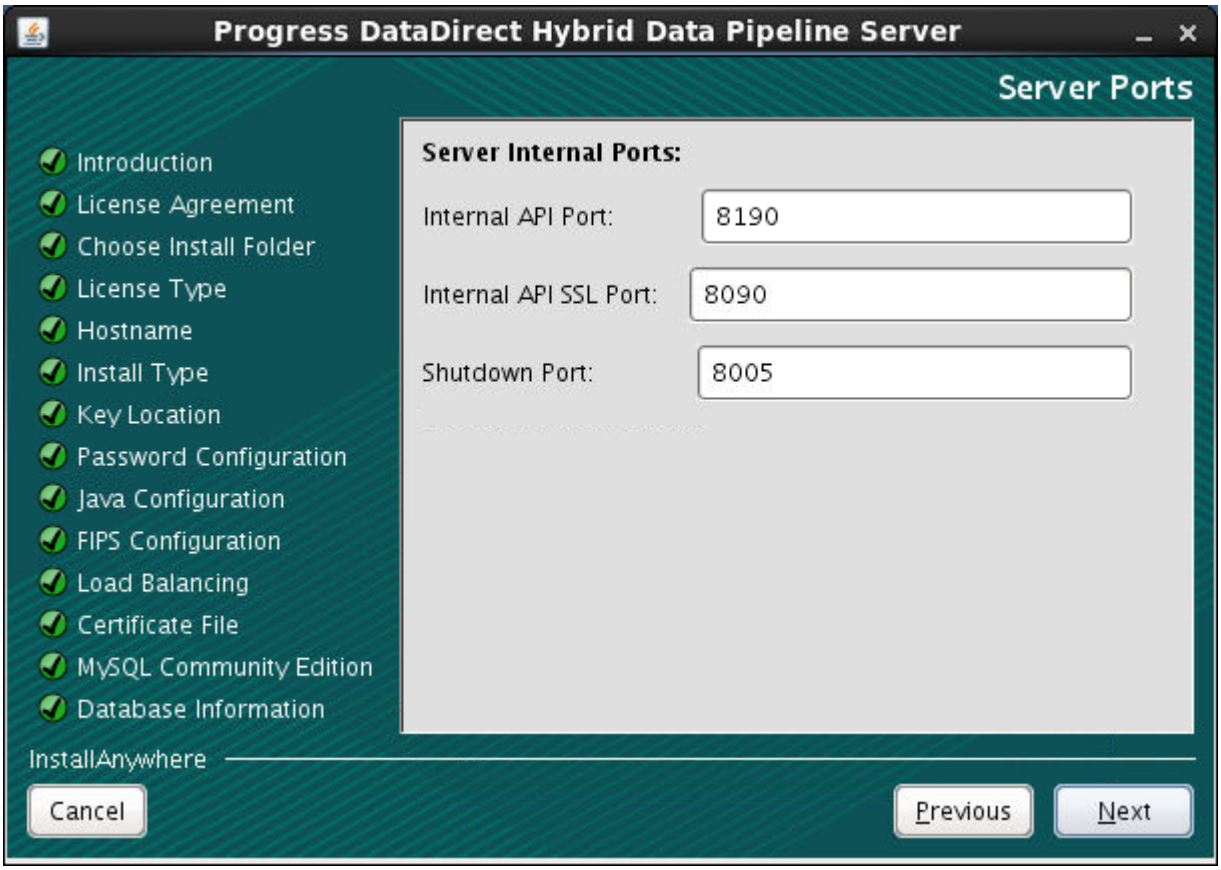


Table 3: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Internal API SSL Port	8090	SSL port for the Internal API
Shutdown Port	8005	Shutdown port

14. Review the installation summary. If you are satisfied with your choices, click **ENTER** to install.
15. After the installation has finished, press **ENTER** to exit the installer.
16. Verify the installation by accessing the Hybrid Data Pipeline user interface from a browser. The login page should appear. For example:

    `https://<myserver>:8443/`

    where *<myserver>* is the fully qualified hostname of the machine where you installed Hybrid Data Pipeline.

    After logging in, administrators can verify product version information by selecting **About** from the question mark drop-down menu. For more information on retrieving version information, refer to "Get Version Information" in the *Progress DataDirect Hybrid Data Pipeline User's Guide*.

Refer to installation log files for a record of any problems that may have occurred during the installation. See Server installation log files on page 166 for details.

What to do next

During installation, the installer generates four configuration and certificate files. These files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. Before installing a component such as the ODBC driver, the JDBC driver, or the On-Premises Connector, these files must be copied to the installer directory of the component you are installing.

The four configuration and certificate files are:

- `config.properties`
- `OnPremise.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`

Load balancer installation (GUI mode)

1. Make the appropriate selection regarding SSL configuration based on your environment.

   Important: If an SSL certificate is not specified, the installer will not generate the configuration and certificate files required for the installation of the On-Premises Connector and the ODBC and JDBC drivers.

   - Select **Yes** to specify the SSL certificate file to be used with the Hybrid Data Pipeline server. The specified file must be the root certificate used to sign the certificate for the load balancer server. PEM, DER, and Base64 encodings are supported. Type the full path to the certificate file, or click **Choose...** to browse to the location of the SSL certificate file. Then, click **Next**.
   - Select **No** if you do not want to specify an SSL certificate.

2. Select MySQL Community Edition if you plan to use MySQL Community Edition as an external system database or as a data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. However, you can use the MySQL Connector/J driver to use MySQL Community Edition as an external system database or as a data source. If you select MySQL Community Edition, enter the name and location of the MySQL Connector/J jar file in the **Jar Path** field. Then, click **Next** to continue.

   For more information on the MySQL Connector/J driver, refer to the MySQL developer website at https://dev.mysql.com/.

3. Select the external database you want to use to store system information from the drop down menu.
   - Select **Oracle**, and continue at Step 4 on page 57.
   - Select **MySQLCommunity**, and continue at Step 5 on page 58.
   - Select **MSSQLServer**, and continue at Step 6 on page 58.
   - Select **PostgreSQL**, and continue at Step 7 on page 58.

4. Provide the Oracle connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Select the connection type. Do one of the following:
      - If you connect using the Oracle System Identifier (SID), select **Connect using SID**, then type the SID.
      - Select **Connect using Service Name**, then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name. The global database name typically comprises the database name and domain name.

d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret; serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

e) Click **Next** and continue at Step 8 on page 58.

5. Provide connection information for the MySQL Community Edition external database.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection url. Values should be entered as a ampersand-separated list of *parameter=value*.
   e) Click **Next** and continue at Step 8 on page 58.
6. Provide the SQL Server connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Type the name of the schema.
   e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
   f) Click **Next** and continue at Step 8 on page 58.
7. Provide the PostgreSQL connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
   e) Click **Next** and continue at Step 8 on page 58.
8. Provide the database credential information for the external database.

Note: Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.

Note: If the installer is unable to validate, you are prompted to reenter credentials or skip validation. Skipping validation is often desired when performing a silent installation. See Silent installation process on page 72 for details.

- In the **Admin Username** field, type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- In the **Admin Password** field, type the password for an database administrator account.
- In the **Username** field, type a user name. The standard user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- In the **Password** field, type the user password.

9. Review the Server Access Port. The Server Access Port must be opened for the load balancer. The default is 8080.

Note: In most cases, the default port works without problems. However, your environment might have already defined a function for the port. If the default port is in use, the installer pops up a message so that you can make the necessary changes.

10. Select whether you are using the On-Premises Connector.

Note: An SSL certificate must be specified in Step 1 on page 57 to use the On-Premises Connector.

- If using the On-Premises Connector, select **Enable On-Premises Connector**. Click **Next** and continue to the next step.
- If not using the On-Premises Connector, leave the check box empty and click **Next**. Continue at Step 12 on page 60.

11. Review the On-Premises Access Ports. The On-Premises Access Port and the TCP Notification Server Port must be opened for the load balancer.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

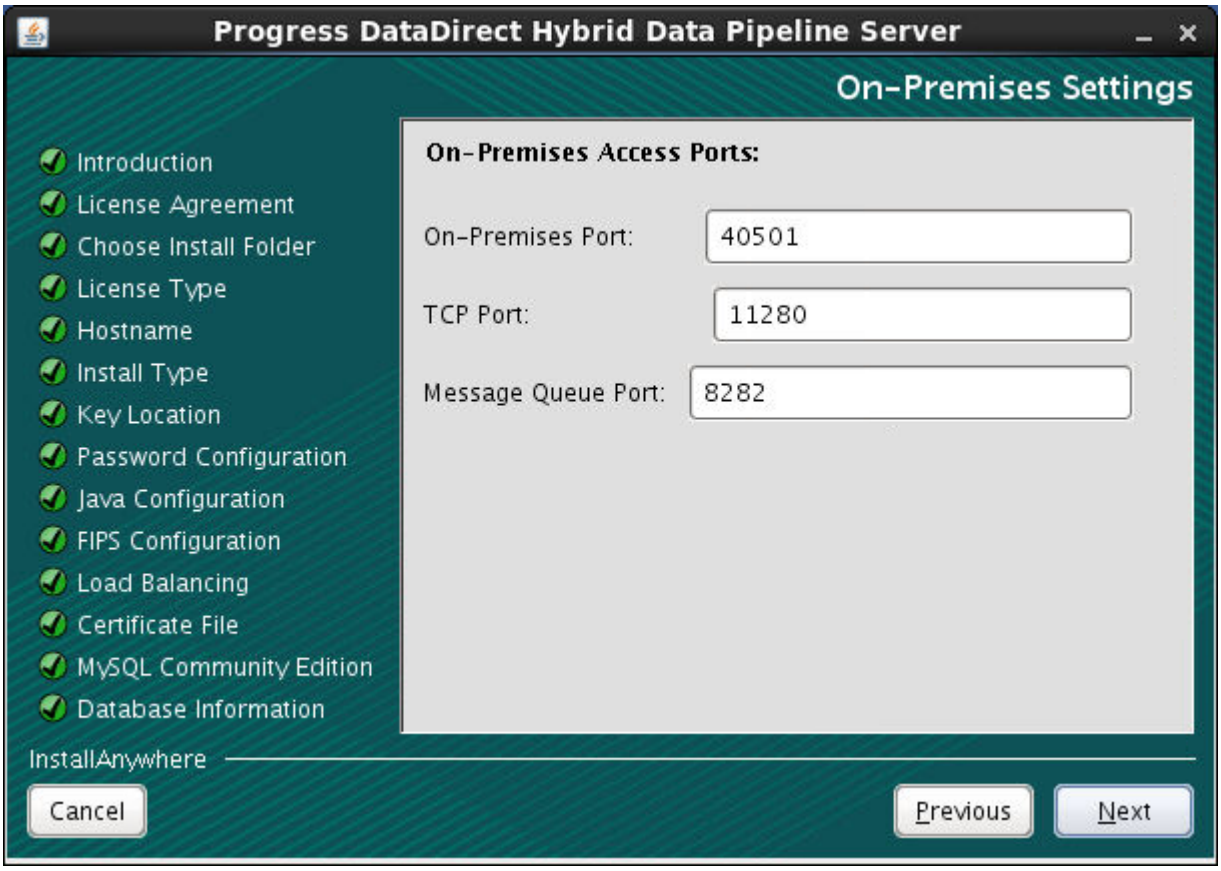


Table 4: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
Message Queue Port	8282	Port for the message queue

12. Review the Server Internal Ports. The Internal API Port and the Shutdown Port must be opened.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of any Hybrid Data Pipeline instance.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

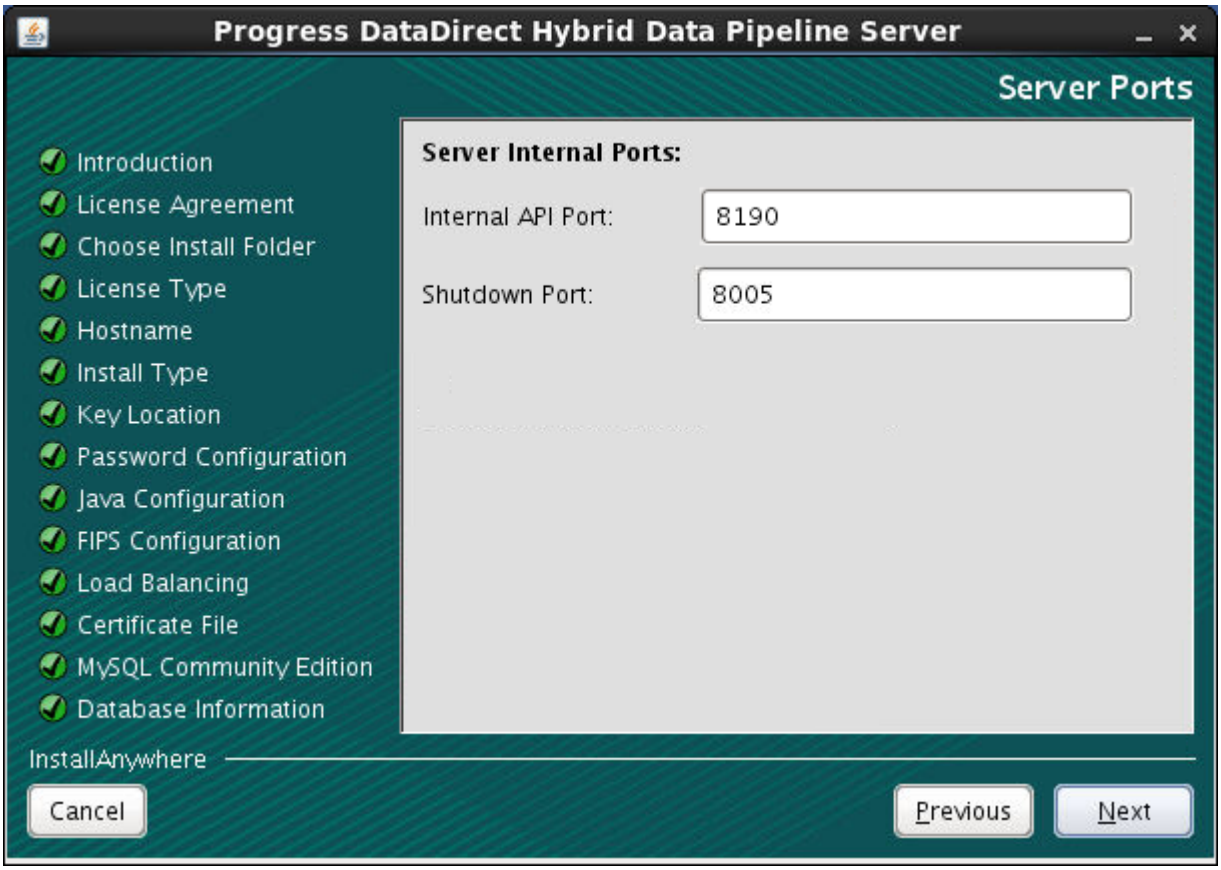


Table 5: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Shutdown Port	8005	Shutdown port

13. Review the installation summary. If you are satisfied with your choices, click **ENTER** to install.
14. After the installation has finished, press **ENTER** to exit the installer.
15. Verify the installation by accessing the Hybrid Data Pipeline user interface from a browser. The login page should appear. For example, type:

    `https://<myserver>/`

    where `<myserver>` is the fully qualified hostname or IP address of the load balancer.

    After logging in, administrators can verify product version information by selecting **About** from the question mark drop-down menu. For more information on retrieving version information, refer to "Get Version Information" in the *Progress DataDirect Hybrid Data Pipeline User's Guide*.

Refer to installation log files for a record of any problems that may have occurred during the installation. See Server installation log files on page 166 for details.

What to do next

During installation, the installer generates four configuration and certificate files. These files will be located in the `redist` subdirectory of the key location you specified in Step 10 in "GUI mode installation." Before installing a component such as the ODBC driver, the JDBC driver, or the On-Premises Connector, these files must be copied to the installer directory of the component you are installing.

Note: If an SSL certificate was not specified in Step 1 on page 57, the installer will not generate the configuration and certificate files required for the installation of the On-Premises Connector and the ODBC and JDBC drivers.

The four configuration and certificate files are:

- config.properties
- ddcloud.pem
- ddcloudTrustStore.jks
- OnPremise.properties

Console mode installation

After copying the downloaded product file to a temporary directory, take the following steps to install the Hybrid Data Pipeline server with the installer in console mode.

1. From a command-line prompt, navigate to the directory where you saved the product file. Alternatively, place the product file directory on your path before proceeding to the next step.

   The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_`*`nn`*`_LINUX_64_INSTALL.bin`, where *`nn`* is the version of the product.

2. Make the file an executable using the `chmod` command. Then, press **ENTER**. For example:

   ```
   chmod +x ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

3. Run the executable by entering the product file path and pressing **ENTER**.

   a) Type the file name and path of the product file. For example:

   ```
   ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -i console
   ```

   b) Press **ENTER**.

   c) The **Introduction** step appears. Press **ENTER** to continue.

4. The License Agreement appears. Press **ENTER** multiple times to advance through the license agreement. Make sure that you read and understand the license agreement.

   - To accept the terms in the License Agreement and continue with the installation, type `Y`.
   - To end the installation, type `N` and press **ENTER**.

   Note: You can exit the installation program at any time by typing `Quit`.

5. You are prompted for the installation directory.

   - Press **ENTER** to accept the default installation directory.
   - Type the absolute path to the installation directory for the installation, and press **ENTER**.

   The default installation directory is:

`/opt/Progress/DataDirect/Hybrid_Data_Pipeline/Hybrid_Server`

If you do not have `/opt` directory permissions, the installer program installs the drivers to your home directory by default. For example:

`/home/users/<username>/Progress/DataDirect/Hybrid_Data_Pipeline/Hybrid_Server`

If the directory contains an existing Hybrid Data Pipeline deployment, you are prompted to specify a different directory or upgrade the existing installation.

6. Choose whether you want to install an evaluation or licensed version of the product. Licensed installations require a valid License Key.
   - Evaluation. Type `1` to proceed with installing an evaluation version of the product (functional for 30 days). Then, press **ENTER** to continue with the installation.
   - Licensed. Type `2` if you purchased a licensed version of the product. Then, press **ENTER**. Type the license key, including any dashes, and then press **ENTER**.
7. Accept or enter the fully qualified hostname for the Hybrid Data Pipeline server. By default, the installer suggests the name of the current machine. Then, press **ENTER**.

   Note: If the installer is unable to validate the hostname, you are prompted to reenter the hostname or skip validation. Skipping validation is often desired when performing a silent installation. See Silent installation process on page 72 for details.
8. Select the installation type.
   - To accept the default values for the remaining options, type `1` and press **ENTER** for a typical installation. Continue at Step 9 on page 63.
   - To customize installation options, type `2` and press **ENTER**. Then, skip to Step 10 on page 64.

   You will need to complete a custom installation if you plan to do any of the following:
   - Specify the key location. The key location serves as a location for shared files used in the installation and operation of the server. The key location should be secured on a system separate from the system that stores encrypted data, or encrypts or decrypts data.
   - Change the Java configuration to use an external JRE
   - Enable FIPS
   - Use a load balancer
   - Change an SSL configuration
   - Use MySQL Community Edition as a data store
   - Store system information in an external MySQL Community Edition, Oracle, or SQL Server database
   - Specify non-default values for ports used by the Hybrid Data Pipeline service
   - Use On-Premises Connectors for secure access to on-premises data sources from the cloud
9. Specify passwords for the *d2cadmin* and *d2cuser* user accounts. Continue at Step 15 in "Standalone installation (console mode)".

   Best practices recommend that you follow the Hybrid Data Pipeline default password policy when specifying these account passwords. When initially logging in to the Web UI or using the API, you must authenticate as one of these users.

10. Specify the key location. The key location serves as a location for shared files used in the installation and operation of the server. The key location should be secured on a system separate from the system that stores encrypted data, or encrypts or decrypts data.

    - Type `1` if you want to specify a location other than the default. You must specify a location for a load balancer installation. Press **ENTER** and continue to the next step.
    - Type `2` and press **ENTER** if you want to use the default location for a standalone installation. This option cannot be used for a load balancer. The default location is *`install_dir`*`/ddcloud/keystore`. Proceed to Standalone installation (console mode) on page 64.

11. Specify passwords for the *d2cadmin* and *d2cuser* user accounts.

    Best practices recommend that you follow the Hybrid Data Pipeline default password policy when specifying these account passwords. When initially logging in to the Web UI or using the API, you must authenticate as one of these users.

12. Specify the desired Java configuration.

    Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

    - Type `1` if you will be using an external JRE (a JRE not installed with the server).
    - Type `2` if you will be using the embedded JRE installed with the server.

13. Specify the fully qualified location of the Java home directory. This is the path to the external JRE. Press **ENTER**.
14. Specify whether you want to enable FIPS on the Hybrid Data Pipeline server.

    Important: To implement FIPS, your hardware must support secure random, or you must have a secure random daemon installed.

    - Type `1` if you want to enable FIPS. Press **ENTER** and continue to the next step.
    - Type `2` and press **ENTER** if you want to use the default setting which is FIPS disabled.

15. Specify if you are planning to use a load balancer.

    - Type `1` if you do not plan to use a load balancer.
    - Type `2` if you plan to use a network load balancer such as HAProxy.
    - Type `3` if you plan to use a cloud load balancer such as AWS Application Load Balancer.

Standalone installation (console mode)

1. Depending on your environment, provide the appropriate SSL certificate information.

    - Type `1` to specify a PEM file to be used by the server to establish SSL connections with ODBC and JDBC client applications. Type the full path of the PEM file. Then, press **ENTER**.

      Note: The PEM file must consist of a private key, a public key certificate issued by a certificate authority (CA), and additional certificates that make up the trust chain. See The PEM file on page 20 for more information.

    - Type `2` to use the self-signed certificate included with the installation. Then, press **ENTER**.

Note: The self-signed certificate may be used in a test environment. However, for production, a PEM file with required information should be specified. See The PEM file on page 20 for more information.

2. Choose the appropriate option depending on whether you are using MySQL Community Edition. MySQL Community Edition can be used as an external system database or as a data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. However, you can use the MySQL Connector/J driver to use MySQL Community Edition as an external system database or as a data source.
   - Type `1` and press **ENTER**, if you are using MySQL Community Edition. Type the name and location of the MySQL Connector/J jar file, and press **ENTER** again.
   - Type `2` and press **ENTER**, if you are not using MySQL Community Edition in your environment.

   Note: For more information on the MySQL Connector/J driver, visit the MySQL developer website at https://dev.mysql.com/.

3. Select the type of database you want to use to store system information.
   - Type `1` to store information on an internal database supplied by this installation. Continue at Step 5 on page 65.
   - Type `2` to store information on an external database. Proceed to the next step.

   Note: Users and data sources created in the internal database are specific to the internal database. They are not migrated to the external database if you subsequently modify the Hybrid Data Pipeline Server to use an external database.

4. Select the type of external system database you want to use to store system information.
   - Select **Oracle**, and continue at Step 6 on page 65.
   - Select **MySQLCommunity**, and continue at Step 7 on page 66.
   - Select **MSSQLServer**, and continue at Step 8 on page 66.
   - Select **PostgreSQL**, and continue at Step 9 on page 66.

5. Enter the database port for the internal database. If your environment has already defined a function for the default port, the installer alerts you with a message so that you can specify a different port. Press **ENTER** and continue at Step 11 on page 67.
6. Provide the Oracle connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Select the connection type. Do one of the following:
      - If you connect using the Oracle System Identifier (SID), type `1`, then type the SID.
      - If you connect using the Service Name, type `2`,then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name—a name that typically comprises the database name and domain name.

d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret;serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

e) Press **ENTER**, and continue at Step 10 on page 66.

7. Provide connection information for the MySQL Community Edition external database.
   a) Type the name of the Hostname.
   b) Type the port number.
   c) Type the database name.
   d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as a ampersand-separated list of *parameter=value*.
   e) Press **ENTER**, and continue at Step 10 on page 66.
8. Provide the SQL Server connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
   e) Press **ENTER**, and continue at Step 10 on page 66.
9. Provide the PostgreSQL connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Type the name of the schema.
   e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
   f) Press **ENTER**, and continue at Step 10 on page 66.
10. You are prompted to provide the database credential information for a user with administrator privileges and for a user without administrator privileges. After you enter the credential information, press **ENTER** to continue.

Note: Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.

Note: If the installer is unable to validate, you are prompted to reenter credentials or skip validation. Skipping validation is often desired when performing a silent installation. See Silent installation process on page 72 for details.

a) Type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.

b) You are prompted to provide the Admin Password. Type the password for a administrator account for the external database.

c) You are prompted to provide the username for a user who does *not* have administrator privileges. Type a user name. The standard user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.

d) You are prompted to provide the user password. Type the user password.

11. Review the Server Access Ports. A Server Access Port must be available to the end user across the firewall. Best security practices recommend using an HTTPS port.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

Table 6: Server Access Ports

Name	Default	Description
HTTP Port	8080	Port that exposes Hybrid Data Pipeline
HTTPS Port	8443	SSL port that exposes Hybrid Data Pipeline

12. Select whether you are using the On-Premises Connector.

- If using the On-Premises Connector, type `1` and press **ENTER**. Then continue to the next step.
- If not using the On-Premises Connector, type `2` and press **ENTER**. Continue at Step 14 on page 68.

13. Review the On-Premises Access Ports. The On-Premises Access Port and a Notification Server Port must be available across the firewall. Best security practices recommend using the SSL Notification Server Port.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

Table 7: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
SSL Port	11443	SSL port for the Notification Server
Message Queue Port	8282	Port for the message queue

14. Review the Server Internal Ports. A port for the internal API and the Shutdown Port must be opened. Best security practices recommend using the Internal API SSL Port.

    Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of the Hybrid Data Pipeline instance.

    Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

    Table 8: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Internal API SSL Port	8090	SSL port for the Internal API
Shutdown Port	8005	Shutdown port

15. Review the installation summary. If you are satisfied with your choices, press **ENTER** to install.
16. After the installation has finished, press **ENTER** to exit the installer.
17. Verify the installation by accessing the Hybrid Data Pipeline user interface from a browser. The login page should appear. For example:

    `https://<myserver>:8443/`

    where `<myserver>` is the fully qualified hostname of the machine where you installed Hybrid Data Pipeline.

    After logging in, administrators can verify product version information by selecting **About** from the question mark drop-down menu. For more information on retrieving version information, refer to "Get Version Information" in the *Progress DataDirect Hybrid Data Pipeline User's Guide*.

Refer to installation log files for a record of any problems that may have occurred during the installation. See Server installation log files on page 166 for details.

What to do next

During installation, the installer generates four configuration and certificate files. These files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. Before installing a component such as the ODBC driver, the JDBC driver, or the On-Premises Connector, these files must be copied to the installer directory of the component you are installing.

The four configuration and certificate files are:

- `config.properties`
- `OnPremise.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`

Load balancer installation (console mode)

1. Make the appropriate selection regarding SSL configuration based on your environment.

Important: If an SSL certificate is not specified, the installer will not generate the configuration and certificate files required for the installation of the On-Premises Connector and the ODBC and JDBC drivers.

- Type `1` to specify the SSL certificate file to be used with the Hybrid Data Pipeline server. The specified file must be the root certificate used to sign the certificate for the load balancer server. PEM, DER, and Base64 encodings are supported. Type the full path to the certificate file. Then, press **ENTER**.
- Type `2` if you do not want to specify an SSL certificate.

2. Choose the appropriate option depending on whether you are using MySQL Community Edition. MySQL Community Edition can be used as an external system database or as a data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. However, you can use the MySQL Connector/J driver to use MySQL Community Edition as an external system database or as a data source.
   - Type `1` and press **ENTER**, if you are using MySQL Community Edition. Type the name and location of the MySQL Connector/J jar file, and press **ENTER** again.
   - Type `2` and press **ENTER**, if you are not using MySQL Community Edition in your environment.

Note: To download the MySQL Connector/J driver, visit the MySQL developer website at https://dev.mysql.com/.

3. Select the type of external system database you want to use to store system information.
   - Select **Oracle**, and continue at Step 4 on page 69.
   - Select **MySQLCommunity**, and continue at Step 5 on page 69.
   - Select **MSSQLServer**, and continue at Step 6 on page 70.
   - Select **PostgreSQL**, and continue at Step 7 on page 70.
4. Provide the Oracle connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Select the connection type. Do one of the following:
      - If you connect using the Oracle System Identifier (SID), type `1` and then enter the SID.
      - If you connect using the Service Name, type `2`, then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name—a name that typically comprises the database name and domain name.
   d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as a semicolon-separated list of *`parameter=value`*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret; serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

   e) Press **ENTER**, and continue at Step 8 on page 70.
5. Provide connection information for the MySQL Community Edition external database.

a) Type the name of the Hostname.

b) Type the port number.

c) Type the database name.

d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as a ampersand-separated list of *parameter=value*.

e) Press **ENTER**, and continue at Step 8 on page 70.

6. Provide the SQL Server connection information.

a) Type the name of the host.

b) Type the port number.

c) Type the database name.

d) Type the name of the schema.

e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.

f) Press **ENTER**, and continue at Step 8 on page 70.

7. Provide the PostgreSQL connection information.

a) Type the name of the host.

b) Type the port number.

c) Type the database name.

d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.

e) Press **ENTER**, and continue at Step 8 on page 70.

8. You are prompted to provide the database credential information for a user with administrator privileges and for a user without administrator privileges. After you enter the credential information, press **ENTER** to continue.

Note: Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.

Note: If the installer is unable to validate, you are prompted to reenter credentials or skip validation. Skipping validation is often desired when performing a silent installation. See Silent installation process on page 72 for details.

---

a) Type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.

b) You are prompted to provide the Admin Password. Type the password for a administrator account for the external database.

c) You are prompted to provide the username for a user who does *not* have administrator privileges. Type a user name. The standard user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.

d) You are prompted to provide the user password. Type the user password.

9. Review the Server Access Port. The Server Access Port must be opened for the load balancer. The default is 8080.

Note: In most cases, the default port works without problems. However, your environment might have already defined a function for the port. If the default port is in use, the installer pops up a message so that you can make the necessary changes.

10. Select whether you are using the On-Premises Connector.

Note: An SSL certificate must be specified in Step 1 on page 68 to use the On-Premises Connector.

- If using the On-Premises Connector, type `1` and press **ENTER**. Then continue to the next step.
- If not using the On-Premises Connector, type `2` and press **ENTER**. Continue at Step 12 on page 71.

11. Review the On-Premises Access Ports. The On-Premises Access Port and the TCP Notification Server Port must be opened for the load balancer.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

Table 9: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
Message Queue Port	8282	Port for the message queue

12. Review the Server Internal Ports. The Internal API Port and the Shutdown Port must be opened.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

Table 10: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Shutdown Port	8005	Shutdown port

13. Review the installation summary. If you are satisfied with your choices, press **ENTER** to install.
14. After the installation has finished, press **ENTER** to exit the installer.
15. Verify the installation by accessing the Hybrid Data Pipeline user interface from a browser. The login page should appear. For example, type:

    `https://<myserver>/`

    where `<myserver>` is the fully qualified hostname or IP address of the load balancer.

    After logging in, administrators can verify product version information by selecting **About** from the question mark drop-down menu. For more information on retrieving version information, refer to "Get Version Information" in the *Progress DataDirect Hybrid Data Pipeline User's Guide*.

Refer to installation log files for a record of any problems that may have occurred during the installation. See Server installation log files on page 166 for details.

What to do next

During installation, the installer generates four configuration and certificate files. These files will be located in the `redist` subdirectory of the key location you specified in Step 10 in "Console mode installation." Before installing a component such as the ODBC driver, the JDBC driver, or the On-Premises Connector, these files must be copied to the installer directory of the component you are installing.

Note: If an SSL certificate was not specified in Step 1 on page 68, the installer will not generate the configuration and certificate files required for the installation of the On-Premises Connector and the ODBC and JDBC drivers.

The four configuration and certificate files are:

- config.properties
- ddcloud.pem
- ddcloudTrustStore.jks
- OnPremise.properties

Silent installation process

A silent installation may be preferred when automating the installation of one or more Hybrid Data Pipeline servers. The silent installation process hinges on the creation of a response file. The response file is a text file that you create (for example, `installer.properties`) with the product installer. You begin by generating a response file, you then tailor the response file to your environment, and you then perform the silent installation.

If you are using the silent installation process to deploy Hybrid Data Pipeline behind a load balancer, the response file generated during the initial installation must be modified to install the server on any additional nodes. For a GUI generated response file, you will need to designate the name of an additional node with the `D2C_HOSTNAME` option. For a console generated response file, you will need to designate the name of an additional node with the `D2C_HOSTNAME_CONSOLE` option.

A silent installation requires performing the following steps:

- You must create a response file using the installer as described in either of the following topics:
  - Creating a response file using the installer in GUI mode on page 73
  - Creating a response file using the installer in console mode on page 88

- You must edit the response file to suit your environment. Response files differ depending on whether you generate them using the installer in GUI mode or console mode. Editing the response file is described in the following topics:
  - Editing a GUI generated installation response file on page 86
  - Editing a console generated installation response file on page 99
- You must perform the silent installation using the response file as described in Performing a silent installation on page 102.

Creating a response file using the installer in GUI mode

After copying the downloaded product file to a temporary directory, take the following steps to generate a response file using the installer in GUI mode.

Important: After generating a response file, you must edit the response file according to the guidelines in Editing a GUI generated installation response file on page 86. In all scenarios, the response file must be edited to include passwords for the *d2cadmin* and *d2cuser* user accounts. Depending on your environment, the response file may require additional modification.

---

1. From a command-line prompt, navigate to the directory where you saved the product file. Alternatively, place the product file directory on your path before proceeding to the next step.

   The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin`, where *nn* is the version of the product.

2. Make the file an executable using the `chmod` command. Then, press **ENTER**. For example:

   ```
   chmod +x ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

3. At a command-line prompt, type the following command where *response_file* is the path and file name of the response file you want to create. You must specify an absolute path.

   ```
   ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -r response_file
   ```

   The following example creates a response file named `pipeline.response` in the `/home/users/johndoe` directory.

   ```
   PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -r
   /home/users/johndoe/pipeline.response
   ```

4. The License Agreement window appears. Make sure that you read and understand the license agreement. To continue with the installation, select the **I accept the terms in the License Agreement** option; then, click **Next**.

   Note: You can exit the installation program at any time by clicking Cancel or return to the previous window by clicking **Previous**.

   ---

5. Choose the destination directory for the installation. Click **Next** to accept the default installation directory, or select **Choose...** to browse to a different directory, then click **Next**.

   The default installation directory is:

   ```
   /opt/Progress/DataDirect/Hybrid_Data_Pipeline/Hybrid_Server
   ```

If you do not have `/opt` directory permissions, the installer program installs the drivers to your home directory by default. For example:

```
/home/users/<username>/Progress/DataDirect/Hybrid_Data_Pipeline/Hybrid_Server
```

If the directory contains an existing Hybrid Data Pipeline deployment, you can select a different directory or upgrade the existing installation. To restore the installation directory to its default setting, click **Restore Default Folder**.

6. Choose whether you want to install an evaluation or licensed version of the product. Licensed installations require a valid License Key.
   - Evaluation. Select this option to install an evaluation version that is fully functional for 30 days. Click **Next** to continue with the installation.
   - Licensed. Select this option if you purchased a licensed version of the product. Type the license key, including any dashes, and then click **Next** to continue with the installation.
7. Accept or enter the fully qualified hostname of the machine that will host the Hybrid Data Pipeline server. By default, the installer suggests the name of the current machine.

   Note the following important information. Then, click **Next** to continue.
   - If you enter a hostname different than the hostname of the current machine, the installer will fail to validate the hostname. You are then prompted to reenter the hostname or skip validation. If you are planning on using the response file to install the product on a different machine, you should opt to skip validation.
   - Before using the response file to install the product on another machine, the response file must have the `SKIP_HOSTNAME_VALIDATION` and `SKIP_PORT_VALIDATION` properties set to `true`. For example:

     ```
     SKIP_HOSTNAME_VALIDATION=true
     SKIP_PORT_VALIDATION=true
     ```

   - Running an installation in silent mode with a response file containing these settings allows the silent installation to continue even if hostname or port validation fail. When the validation fails during the silent installation process, the installer generates the file `SilentInstallInfo.log` in the user's home directory but completes a full installation.
8. Select the installation type.
   - To accept the default values for all remaining options, select **Typical (use existing settings)** and click **Next**. Continue at Step 9 on page 75.
   - To modify installation options, select **Custom (choose configuration values)** and click **Next**. Then, skip to Step 10 on page 75.

   You will need to complete a custom installation if you plan to do any of the following:
   - Specify the key location. The key location serves as a location for shared files used in the installation and operation of the server. The key location should be secured on a system separate from the system that stores encrypted data, or encrypts or decrypts data.
   - Change the Java configuration to use an external JRE
   - Enable FIPS
   - Use a load balancer
   - Change an SSL configuration
   - Use MySQL Community Edition as a data store
   - Store system information in an external MySQL Community Edition, Oracle, or SQL Server database

- Specify non-default values for ports used by the Hybrid Data Pipeline service
- Use On-Premises Connectors for secure access to on-premises data sources from the cloud

9. Specify passwords for the *d2cadmin* and *d2cuser* user accounts. Continue at Step 14 in "Creating a response file for a standalone installation (GUI mode)".

Important: Passwords for the *d2cadmin* and *d2cuser* user accounts are not persisted in the response file. These values must be specified in the response file with the `D2C_ADMIN_PASSWORD` and `D2C_USER_PASSWORD` options before running a silent install (see Editing a GUI generated installation response file on page 86). Best practices recommend that you follow the Hybrid Data Pipeline default password policy when specifying these account passwords. When initially logging in to the Web UI or using the API, you must authenticate as one of these users.

---

10. Specify the key location. The key location serves as a location for shared files used in the installation and operation of the server. The key location should be secured on a system separate from the system that stores encrypted data, or encrypts or decrypts data.
    - Select **Use default location** if you want to use the default location for a standalone installation. This option cannot be used for a load balancer installation. The default location is *`install_dir`*`/ddcloud/keystore`. Click **Next** and proceed to Creating a response file for a standalone installation (GUI mode) on page 76.
    - Select **Specify location** if you want to specify a location other than the default. You must specify a location for a load balancer installation. Click **Next** and continue to the next step.
11. Specify passwords for the *d2cadmin* and *d2cuser* user accounts.

    Best practices recommend that you follow the Hybrid Data Pipeline default password policy when specifying these account passwords. When initially logging in to the Web UI or using the API, you must authenticate as one of these users.
12. Select the desired Java configuration.

Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

    - Select **Use default Java** if you will be using the embedded JRE installed with the server.
    - Select **Java home directory** and provide the path to an external JRE if you will be using a JRE not installed with the server.
13. Select whether you want to enable FIPS on the Hybrid Data Pipeline server.

Important: To implement FIPS, your hardware must support secure random, or you must have a secure random daemon installed.

---

14. Select whether you will install the Hybrid Data Pipeline server behind a load balancer.
    - Select **Yes** for an installation that supports load balancing. Click **Next**. In the host name field, type the name or IP address of the server hosting your load balancer device; then, press **ENTER**. Continue at Creating a response file for a load balancer installation (GUI mode) on page 81.
    - Select **No** for standalone installation. Then, click **Next**. Continue at Creating a response file for a standalone installation (GUI mode) on page 76.

Creating a response file for a standalone installation (GUI mode)

1. Depending on your environment, provide the appropriate SSL certificate information.
   - Select **Certificate file** to specify a PEM file to be used by the server to establish SSL connections with ODBC and JDBC client applications. Type the full path to the PEM file, or click **Choose...** to browse to the location of the PEM file. Then, click **Next**.

     Note: The PEM file must consist of a private key, a public key certificate issued by a certificate authority (CA), and additional certificates that make up the trust chain. See The PEM file on page 20 for more information.
   - Select **Use existing Certificate** to use the self-signed certificate included with the installation. Then, click **Next**.

     Note: The self-signed certificate may be used in a test environment. However, for production, a PEM file with required information should be specified. See The PEM file on page 20 for more information.
2. Select MySQL Community Edition if you plan to use MySQL Community Edition as an external system database or as a data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. However, you can use the MySQL Connector/J driver to use MySQL Community Edition as an external system database or as a data source. If you select MySQL Community Edition, enter the name and location of the MySQL Connector/J jar file in the **Jar Path** field. Then, click **Next** to continue.

   For more information on the MySQL Connector/J driver, refer to the MySQL developer website at https://dev.mysql.com/.
3. Select the type of database you want to use to store system information.
   - Select **Internal Database (supplied by this install)** to use the default internal database. Click **Next** to continue. Proceed to the next step.
   - Select **External Database** to store the system information in an external database. Then, from the drop down box, choose your database vender. Then, click **Next**.
     - Select **Oracle**, and continue at Step 5 on page 76.
     - Select **MySQLCommunity**, and continue at Step 6 on page 77.
     - Select **MSSQLServer**, and continue at Step 7 on page 77.
     - Select **PostgreSQL**, and continue at Step 8 on page 77.

   Note: Users and data sources created in the internal database are specific to the internal database. They are not migrated to the external database if you subsequently modify the Hybrid Data Pipeline Server to use an external database.
4. Enter the database port for the internal database. If your environment has already defined a function for the default port, the installer displays a message so that you can specify a different port. Click **Next** and continue at Step 10 on page 78.
5. Provide the Oracle connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Select the connection type. Do one of the following:

- If you connect using the Oracle System Identifier (SID), select **Connect using SID**, then type the SID.
- Select **Connect using Service Name**, then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name. The global database name typically comprises the database name and domain name.

d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection url. Values should be entered as a semicolon-separated list of *parameter=value*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret;serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

e) Click **Next**, and continue at Step 9 on page 77.

6. Provide connection information for the MySQL Community Edition external database.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
   e) Click **Next**, and continue at Step 9 on page 77.
7. Provide the SQL Server connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Type the name of the schema.
   e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
   f) Click **Next**, and continue at Step 9 on page 77.
8. Provide the PostgreSQL connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
   e) Click **Next**, and continue at Step 9 on page 77.
9. Provide the external database credential information.

- In the **Admin Username** field, type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- In the **Admin Password** field, type the password for an database administrator account.
- In the **Username** field, type a user name. The standard user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- In the **Password** field, type the user password.

Important:

- Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.
- Passwords for an external database implementation are not persisted. These values must be specified in the response file with the `D2C_DB_ADMIN_PASSWORD` and `D2C_DB_USER_PASSWORD` options before running a silent install.
- The installer attempts to validate the database. If the installer is unable to validate, you are prompted to reenter credentials or skip validation. If you skip validation, the response file must have the `SKIP_DATABASE_VALIDATION` property set to `true`. During a silent installation, the installer will complete the installation even when the database validation fails.

10. Review the Server Access Ports. A Server Access Port must be available to the end user across the firewall. Best security practices recommend using an HTTPS port.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

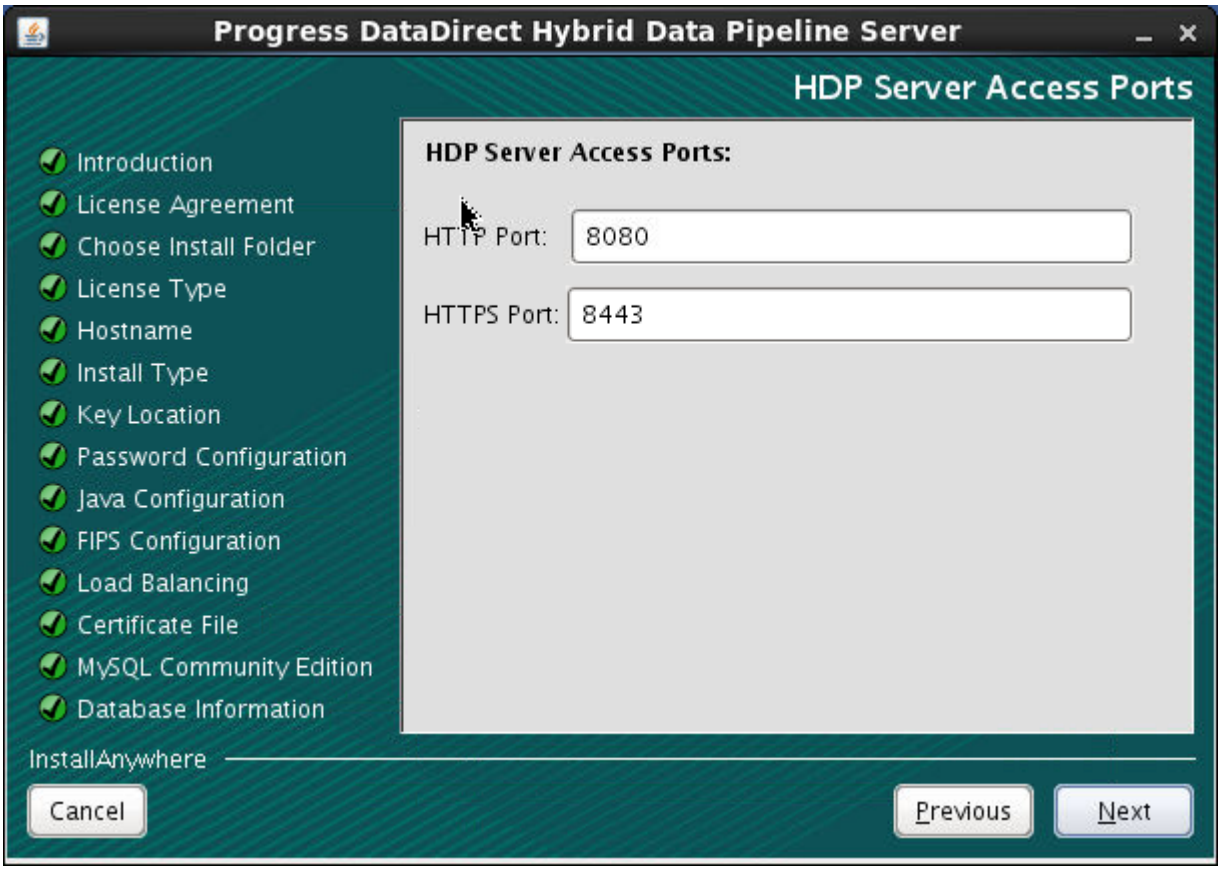


Table 11: Server Access Ports

Name	Default	Description
HTTP Port	8080	Port that exposes Hybrid Data Pipeline
HTTPS Port	8443	SSL port that exposes Hybrid Data Pipeline

11. Select whether you are using the On-Premises Connector.
    - If using the On-Premises Connector, select **Enable On-Premises Connector**. Click **Next** and continue to the next step.
    - If not using the On-Premises Connector, leave the check box empty and click **Next**. Continue at Step 13 on page 80.
12. Review the On-Premises Access Ports. The On-Premises Access Port and a Notification Server Port must be available across the firewall. Best security practices recommend using the SSL Notification Server Port.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

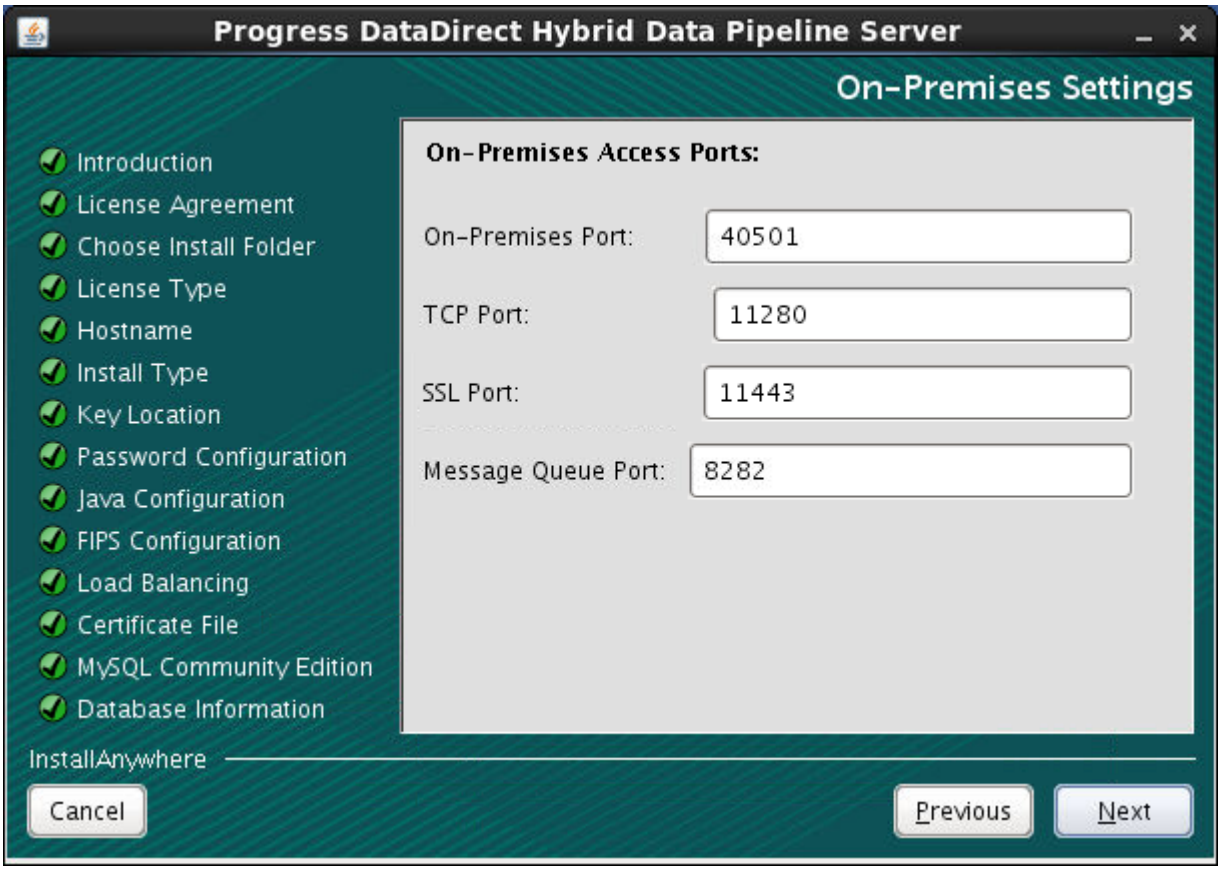


Table 12: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
SSL Port	11443	SSL port for the Notification Server
Message Queue Port	8282	Port for the message queue

13. Review the Server Internal Ports. A port for the internal API and the Shutdown Port must be opened. Best security practices recommend using the Internal API SSL Port.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of the Hybrid Data Pipeline instance.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

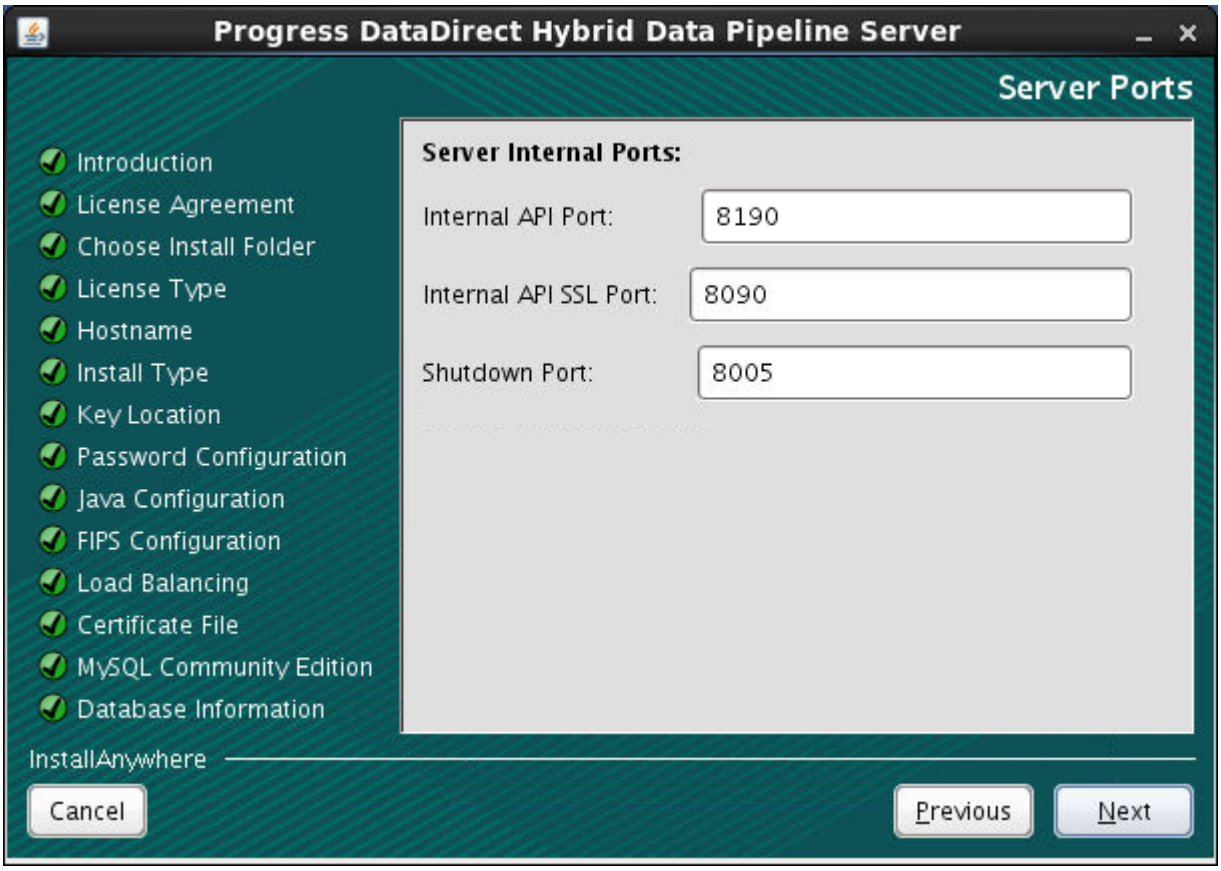


Table 13: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Internal API SSL Port	8090	SSL port for the Internal API
Shutdown Port	8005	Shutdown port

14. Review the installation summary. If you are satisfied with your choices, press **ENTER** to generate the response file.
15. After the response file has been generated, press **ENTER** to exit the installer.
16. Confirm that a response file has been generated by navigating to the response file directory you specified in Step 3 in "Creating a response file using the installer in GUI mode" and opening the response file.
17. You must now edit the response file according to the guidelines in Editing a GUI generated installation response file on page 86. In all scenarios, the response file must be edited to include passwords for the *d2cadmin* and *d2cuser* user accounts. Depending on your environment, the response file may require additional modification.

Creating a response file for a load balancer installation (GUI mode)

1. Make the appropriate selection regarding SSL configuration based on your environment.

Important: If an SSL certificate is not specified, the installer will not generate the configuration and certificate files required for the installation of the On-Premises Connector and the ODBC and JDBC drivers.

- Select **Yes** to specify the SSL certificate file to be used with the Hybrid Data Pipeline server. The specified file must be the root certificate used to sign the certificate for the load balancer server. PEM, DER, and Base64 encodings are supported. Type the full path to the certificate file, or click **Choose...** to browse to the location of the SSL certificate file. Then, click **Next**.
- Select **No** if you do not want to specify an SSL certificate.

2. Select whether you want to use the MySQL Community Edition data store for either a system database or data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition; however, it does support the MySQL Connector/J driver. If you choose **Yes**, in the **Jar Path** field, provide the name and location of the driver's jar file.

   For more information on the MySQL Connector/J driver, refer to the MySQL developer website at https://dev.mysql.com/.

3. Select the external database you want to use to store system information from the drop down menu.
   - Select **Oracle**, and continue at Step 4 on page 82.
   - Select **MySQLCommunity**, and continue at Step 5 on page 82.
   - Select **MSSQLServer**, and continue at Step 6 on page 83.
   - Select **PostgreSQL**, and continue at Step 7 on page 83.

4. Provide the Oracle connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Select the connection type. Do one of the following:
      - If you connect using the Oracle System Identifier (SID), select **Connect using SID**, then type the SID.
      - Select **Connect using Service Name**, then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name. The global database name typically comprises the database name and domain name.

   d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection url. Values should be entered as a semicolon-separated list of *parameter=value*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret; serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

   e) Click **Next**, and continue at Step 8 on page 83.

5. Provide connection information for the MySQL Community Edition external database.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.

d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection url. Values should be entered as a ampersand-separated list of *parameter=value*.

e) Click **Next**, and continue at Step 8 on page 83.

6. Provide the SQL Server connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Type the name of the schema.
   e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
   f) Click **Next**, and continue at Step 8 on page 83.

7. Provide the PostgreSQL connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
   e) Click **Next**, and continue at Step 8 on page 83.

8. Provide the database credential information for the external database.
   - In the **Admin Username** field, type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
   - In the **Admin Password** field, type the password for an database administrator account.
   - In the **Username** field, type a user name. For a list of required privileges, see External system databases on page 15.
   - In the **Password** field, type the user password.

   Important:

   - Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.
   - Passwords for an external database implementation are not persisted. These values must be specified in the response file with the `D2C_DB_ADMIN_PASSWORD` and `D2C_DB_USER_PASSWORD` options before running a silent install.
   - The installer attempts to validate the database. If the installer is unable to validate, you are prompted to reenter credentials or skip validation. If you skip validation, the response file must have the `SKIP_DATABASE_VALIDATION` property set to `true`. During a silent installation, the installer will complete the installation even when the database validation fails.

9. Review the Server Access Port. The Server Access Port must be opened for the load balancer. The default is 8080.

   Note: In most cases, the default port works without problems. However, your environment might have already defined a function for the port. If the default port is in use, the installer pops up a message so that you can make the necessary changes.

10. Select whether you are using the On-Premises Connector.

    Note: An SSL certificate must be specified in Step 1 on page 81 to use the On-Premises Connector.

    - If using the On-Premises Connector, select **Enable On-Premises Connector**. Click **Next** and continue to the next step.
    - If not using the On-Premises Connector, leave the check box empty and click **Next**. Continue at Step 12 on page 85.

11. Review the On-Premises Access Ports. The On-Premises Access Port and the TCP Notification Server Port must be opened for the load balancer.

    Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

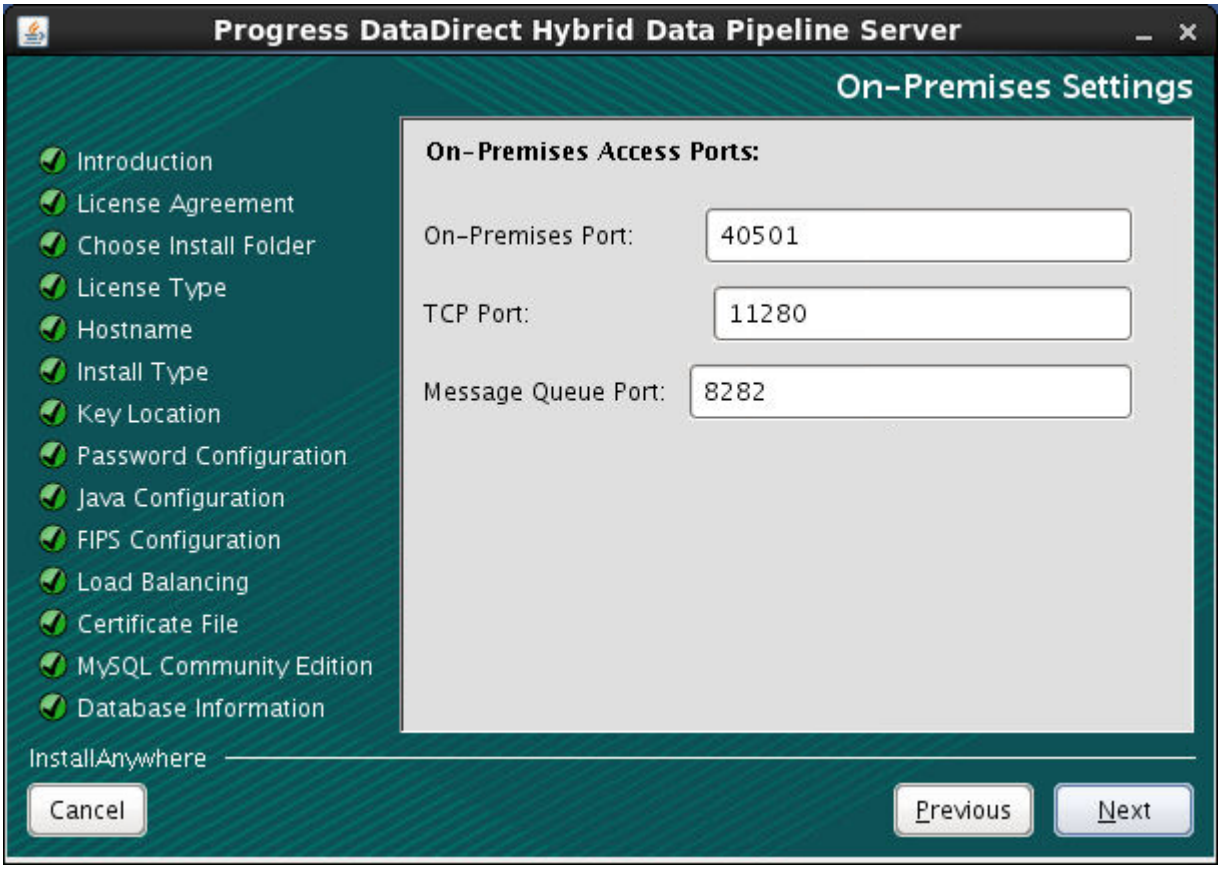


Table 14: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
Message Queue Port	8282	Port for the message queue

12. Review the Server Internal Ports. The Internal API Port and the Shutdown Port must be opened.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of any Hybrid Data Pipeline instance.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

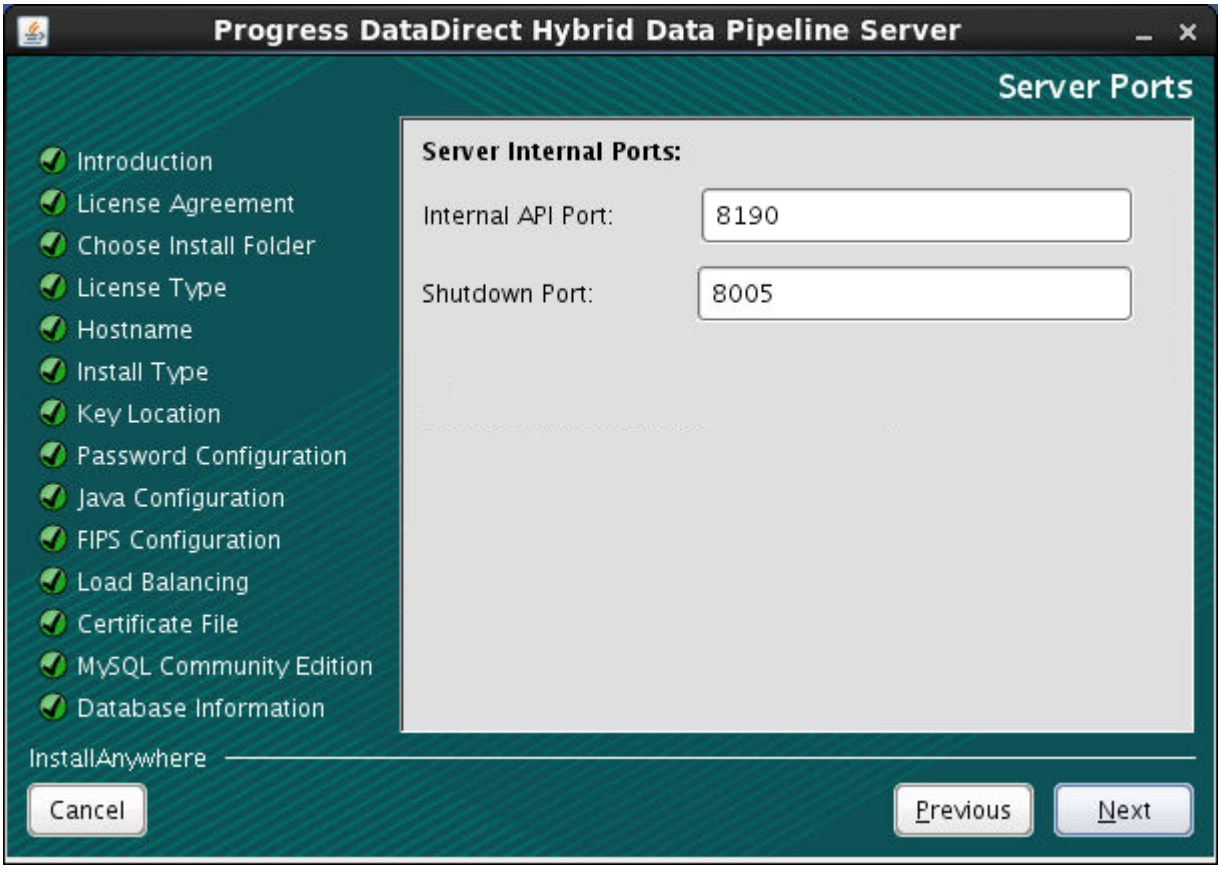


Table 15: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Shutdown Port	8005	Shutdown port

13. Review the installation summary. If you are satisfied with your choices, press **ENTER** to generate the response file.
14. After the response files has been generated, press **ENTER** to exit the installer.
15. Confirm that a response file has been generated by navigating to the response file directory you specified in Step 3 in "Creating a response file using the installer in GUI mode" and opening the response file.
16. You must now edit the response file according to the guidelines in Editing a GUI generated installation response file on page 86. In all scenarios, the response file must be edited to include passwords for the *d2cadmin* and *d2cuser* user accounts. Depending on your environment, the response file may require additional modification.

Editing a GUI generated installation response file

After you have generated a response file, you must edit the response file to suit your environment before you perform a silent installation. Use the following guidelines to edit your response file.

- You must specify passwords for the default *d2cadmin* and *d2cuser* accounts. Best practices recommend that you follow the Hybrid Data Pipeline default password policy when specifying these account passwords. When initially logging in to the Web UI or using the API, you must authenticate as one of these users. These settings take the following form.

```
D2C_ADMIN_PASSWORD=<admin_password>
D2C_USER_PASSWORD=<user_password>
```

- If you are installing the Hybrid Data Pipeline server on a system other than the one you used to generate the response file, you can designate the host machine with the `D2C_HOSTNAME` option.
- If you want to continue with an installation even though hostname, port, and load balancer hostname validations fail, then the validation settings should be set as follows. (Note that these properties are set to `false` by default.)

```
SKIP_HOSTNAME_VALIDATION=true
SKIP_PORT_VALIDATION=true
SKIP_LB_HOSTNAME_VALIDATION=true
```

- If you are storing user credentials on an external database, you must designate the administrator and user passwords of the external database with the `D2C_DB_ADMIN_PASSWORD` and `D2C_DB_USER_PASSWORD` options. However, you may skip database validation by setting the `SKIP_DATABASE_VALIDATION` property to `true`. If you skip database validation, the installer will complete the installation even when the database validation fails.

The following example response file includes the settings for a load balancer deployment using the On-Premises Connector, using a MySQL Community Edition external database. This type of response file would be generated with the GUI installer.

```
# Tue Nov 21 15:26:30 EST 2017
# Replay feature output
# ---------------------
```

```
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.



#Choose Install Folder
#---------------------
USER_INSTALL_DIR=<install_dir>

#Installation License Type
#-------------------------
D2C_EVAL_YES=1
D2C_LICENSED_YES=0
D2C_LICENSE_KEY=

#Enter Hostname
#--------------
D2C_HOSTNAME=<hybriddatapipelinehost>

#SKIP VALIDATION SETTINGS
#------------------------
SKIP_HOSTNAME_VALIDATION=true
SKIP_PORT_VALIDATION=true

#Install Type
#------------
D2C_INSTALL_TYPE_TYPICAL=0
D2C_INSTALL_TYPE_CUSTOM=1

#Key location
#------------
USER_INPUT_CHOOSE_KEY_LOCATION=1
USER_INPUT_KEY_LOCATION=/<keyfilepath>/
USER_INPUT_DEFAULT_KEY_LOCATION=0

#Password Configuration
#----------------------
D2C_ADMIN_PASSWORD=AdminSecret
D2C_USER_PASSWORD=UserSecret

#Java Configuration
#------------------
SPECIFY_JAVA_HOME_NO=1
SPECIFY_JAVA_HOME_YES=0

#FIPS Configuration
#------------------
D2C_USING_FIPS_CONFIG=0

#Load Balancing
#--------------
D2C_NO_LOAD_BALANCER=0
D2C_NETWORK_LOAD_BALANCER=0
D2C_CLOUD_LOAD_BALANCER=1
LOAD_BALANCING_HOST_NAME=<loadbalancerhost>

#SKIP VALIDATION SETTINGS
#------------------------
SKIP_LB_HOSTNAME_VALIDATION=true

#Certificate File
#----------------
D2C_CERT_FILE_YES=1
D2C_CERT_FILE=/<certificatepath>/<filename>
D2C_CERT_FILE_NO=0

#MySQL Community Edition
#-----------------------
D2C_DB_MYSQL_COMMUNITY_SUPPORT_YES=1
```

```
D2C_DB_MYSQL_JAR_PATH=/<mysqldriverpath>/<filename>.jar
D2C_DB_MYSQL_COMMUNITY_SUPPORT_NO=0

#Database Type
#--------------
D2C_DB_VENDOR_ORACLE=0
D2C_DB_VENDOR_MSSQLSERVER=0
D2C_DB_VENDOR_MYSQL=1
D2C_DB_VENDOR_POSTGRESQL=0

#MySQL Connection Information
#----------------------------
D2C_DB_HOSTNAME=mysqlserver1
D2C_DB_PORT=3306
D2C_DATABASE_NAME=<db_name>
D2C_DB_ADVANCED_OPTIONS=

#Database Credential Information
#-------------------------------
D2C_DB_ADMIN_USERNAME=<adminname>
D2C_DB_ADMIN_PASSWORD=<adminpassword>
D2C_DB_USER_USERNAME=<username>
D2C_DB_USER_PASSWORD=<userpassword>

#Database Connection Validation
#------------------------------
SKIP_DATABASE_VALIDATION=false

#HDP Server Access Ports
#-----------------------
D2C_API_PORT=8080

#On-Premises Settings
#--------------------
USER_INPUT_ENABLE_OPC=1
D2C_OPC_PORT=40501
D2C_NOTIFICATION_PORT=11280
D2C_MESSAGE_QUEUE_PORT=8282

#Server Ports
#------------
D2C_INTERNAL_API_PORT=8190
D2C_SHUTDOWN_PORT=8005
```

Creating a response file using the installer in console mode

After copying the downloaded product file to a temporary directory, take the following steps to generate a response file using the installer in console mode.

Important: After generating a response file, you must edit the response file according to the guidelines in Editing a console generated installation response file on page 99. In all scenarios, the response file must be edited to include passwords for the *d2cadmin* and *d2cuser* user accounts. Depending on your environment, the response file may require additional modification.

---

1. From a command-line prompt, navigate to the directory where you saved the product file. Alternatively, place the product file directory on your path before proceeding to the next step.

   The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin`, where *nn* is the version of the product.

2. Make the file an executable using the `chmod` command. Then, press **ENTER**. For example:

   ```
   chmod +x ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

3. At a command-line prompt, type the following command where *response_file* is the path and file name of the response file you want to create. You must specify an absolute path.

   ```
   ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -i console -r response_file
   ```

   The following example creates a response file named `pipeline.response` in the `/home/users/johndoe` directory.

   ```
   PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -i console -r /home/users/johndoe/pipeline.response
   ```

4. The License Agreement appears. Press **ENTER** multiple times to advance through the license agreement. Make sure that you read and understand the license agreement.

   - To accept the terms in the License Agreement and continue with the installation, type `Y`.
   - To end the installation, type `N` and press **ENTER**.

   Note: You can exit the installation program at any time by typing `Quit`.

5. You are prompted for the installation directory.

   - Press **ENTER** to accept the default installation directory.
   - Type the absolute path to the installation directory for the installation, and press **ENTER**.

   The default installation directory is:

   ```
   /opt/Progress/DataDirect/Hybrid_Data_Pipeline/Hybrid_Server
   ```

   If you do not have `/opt` directory permissions, the installer program installs the drivers to your home directory by default. For example:

   ```
   /home/users/<username>/Progress/DataDirect/Hybrid_Data_Pipeline/Hybrid_Server
   ```

   If the directory contains an existing Hybrid Data Pipeline deployment, you are prompted to specify a different directory or upgrade the existing installation.

6. Choose whether you want to install an evaluation or licensed version of the product. Licensed installations require a valid License Key.

   - Evaluation. Type `1` to proceed with installing an evaluation version of the product (functional for 30 days). Then, press **ENTER**.
   - Licensed. Type `2` if you purchased a licensed version of the product. Then, press **ENTER**. Type the license key, including any dashes, and then press **ENTER**.

7. Accept or enter the fully qualified hostname for your Progress DataDirect Hybrid Data Pipeline Server. By default, the installer suggests the name of the current machine. Then, press **ENTER**.

   Note the following important information. Then, click **ENTER** to continue.

   - If you enter a hostname different than the hostname of the current machine, the installer will fail to validate the hostname. You are then prompted to reenter the hostname or skip validation. If you are planning on using the response file to install the product on a different machine, you should opt to skip validation.

- Before using the response file to install the product on another machine, the response file must have the `SKIP_HOSTNAME_VALIDATION` and `SKIP_PORT_VALIDATION` validation properties set to `1`. For example:

  ```
  SKIP_HOSTNAME_VALIDATION=true
  SKIP_PORT_VALIDATION=true
  ```

- Running an installation in silent mode with a response file containing these settings allows the silent installation to continue even if hostname or port validation fail. When the validation fails during the silent installation process, the installer generates the file `SilentInstallInfo.log` in the user's home directory but completes a full installation.

8. Select your installation type.

   - To accept the default values for the remaining options, type `1` and press **ENTER** for a typical installation. Continue at Step 9 on page 90.
   - To customize installation options, type `2` and press **ENTER**. Then, skip to Step 10 on page 90.

   You will need to complete a custom installation if you plan to do any of the following:

   - Specify the key location. The key location serves as a location for shared files used in the installation and operation of the server. The key location should be secured on a system separate from the system that stores encrypted data, or encrypts or decrypts data.
   - Change the Java configuration to use an external JRE
   - Enable FIPS
   - Use a load balancer
   - Change an SSL configuration
   - Use MySQL Community Edition as a data store
   - Store system information in an external MySQL Community Edition, Oracle, or SQL Server database
   - Specify non-default values for ports used by the Hybrid Data Pipeline service
   - Use On-Premises Connectors for secure access to on-premises data sources from the cloud

9. Specify passwords for the *d2cadmin* and *d2cuser* user accounts. Continue at Step 15 in "Standalone installation (console mode)".

   Important: Passwords for the *d2cadmin* and *d2cuser* user accounts are not persisted in the response file. These values must be specified in the response file with the `D2C_ADMIN_PASSWORD_CONSOLE` and `D2C_USER_PASSWORD_CONSOLE` options before running a silent install (see Editing a console generated installation response file on page 99). Best practices recommend that you follow the Hybrid Data Pipeline default password policy when specifying these account passwords. When initially logging in to the Web UI or using the API, you must authenticate as one of these users.

10. Specify the key location. The key location serves as a location for shared files used in the installation and operation of the server. The key location should be secured on a system separate from the system that stores encrypted data, or encrypts or decrypts data.

    - Type `1` if you want to specify a location other than the default. You must specify a location for a load balancer installation. Press **ENTER** and continue to the next step.

- Type `2` and press **ENTER** if you want to use the default location for a standalone installation. This option cannot be used for a load balancer installation. The default location is *`install_dir`*`/ddcloud/keystore`. Proceed to Creating a response file for a standalone installation (console mode) on page 91.

11. Specify passwords for the *d2cadmin* and *d2cuser* user accounts.

    Best practices recommend that you follow the Hybrid Data Pipeline default password policy when specifying these account passwords. When initially logging in to the Web UI or using the API, you must authenticate as one of these users.

12. Specify the desired Java configuration.

    Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

    - Type `1` if you will be using an external JRE (a JRE not installed with the server).
    - Type `2` if you will be using the embedded JRE installed with the server.

13. Specify the fully qualified location of the Java home directory. This is the path to the external JRE. Press **ENTER**.
14. Specify whether you want to enable FIPS on the Hybrid Data Pipeline server.

    Important: To implement FIPS, your hardware must support secure random, or you must have a secure random daemon installed.

    - Type `1` if you want to enable FIPS. Press **ENTER** and continue to the next step.
    - Type `2` and press **ENTER** if you want to use the default setting which is FIPS disabled.

15. Specify if you are planning to use a load balancer.

    - Type `1` if you do not plan to use a load balancer. Continue at Creating a response file for a standalone installation (console mode) on page 91.
    - Type `2` if you plan to use a network load balancer such as HAProxy. Continue at Creating a response file for a load balancer installation (console mode) on page 95.
    - Type `3` if you plan to use a cloud load balancer such as AWS Application Load Balancer. Continue at Creating a response file for a load balancer installation (console mode) on page 95.

Creating a response file for a standalone installation (console mode)

1. Depending on your environment, provide the appropriate SSL certificate information.

    - Type `1` to specify a PEM file to be used by the server to establish SSL connections with ODBC and JDBC client applications. Type the full path of the PEM file. Then, press **ENTER**.

      Note: The PEM file must consist of a private key, a public key certificate issued by a certificate authority (CA), and additional certificates that make up the trust chain. See The PEM file on page 20 for more information.

    - Type `2` to use the self-signed certificate included with the installation. Then, press **ENTER**.

Note: The self-signed certificate may be used in a test environment. However, for production, a PEM file with required information should be specified. See The PEM file on page 20 for more information.

2. Choose the appropriate option depending on whether you are using MySQL Community Edition. MySQL Community Edition can be used as an external system database or as a data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. However, you can use the MySQL Connector/J driver to use MySQL Community Edition as an external system database or as a data source.
   - Type `1` and press **ENTER**, if you are using MySQL Community Edition. Type the name and location of the MySQL Connector/J jar file, and press **ENTER** again.
   - Type `2` and press **ENTER**, if you are not using MySQL Community Edition in your environment.

   Note: For more information on the MySQL Connector/J driver, visit the MySQL developer website at https://dev.mysql.com/.

3. Select the type of database you want to use to store system information.
   - Type `1` to use the default internal database (supplied by this installation). Continue at Step 5 on page 92.
   - Type `2` to use an external database. With this option, you store system information in an external database.

   Note: Users and data sources created in the internal database are specific to the internal database. They are not migrated to the external database if you subsequently modify the Hybrid Data Pipeline server to use an external database.

4. Select the type of external system database you want to use to store system information.
   - Select **Oracle**, and continue to the next Step 6 on page 92.
   - Select **MySQLCommunity**, and continue at Step 7 on page 93.
   - Select **MSSQLServer**, and continue at Step 8 on page 93.
   - Select **PostgreSQL**, and continue at Step 9 on page 93.

5. Enter the database port for the internal database. If your environment has already defined a function for the default port, the installer alerts you with a message so that you can specify a different port. Press **ENTER** and continue at Step 11 on page 94.
6. Provide the Oracle connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Select the connection type. Do one of the following:
      - If you connect using the Oracle System Identifier (SID), type `1`, then type the SID.
      - If you connect using the Service Name, type `2`,then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name—a name that typically comprises the database name and domain name.

d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as a semicolon-separated list of *parameter=value*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret;serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

e) Press **ENTER**, and continue at Step 10 on page 93.

7. Provide connection information for the MySQL Community Edition external database.
   a) Type the name of the Hostname.
   b) Type the port number.
   c) Type the database name.
   d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection URL. Values should be entered as a ampersand- separated list of *parameter=value*.
   e) Press **ENTER**, and continue at Step 10 on page 93.
8. Provide the SQL Server connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Type the name of the schema.
   e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
   f) Press **ENTER**, and continue at Step 10 on page 93.
9. Provide the PostgreSQL connection information.
   a) Type the name of the host.
   b) Type the port number.
   c) Type the database name.
   d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
   e) Press **ENTER**, and continue at Step 10 on page 93.
10. You are prompted to provide the external database credential information for a user with administrator privileges and for a user without administrator privileges. After you enter the credential information, press **ENTER** to continue.
    a) Type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
    b) You are prompted to provide the Admin Password. Type the password for an external database administrator account.

c) You are prompted to provide the username for a user who does *not* have administrator privileges. Type a user name. The standard user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.

d) You are prompted to provide the User Password. Type the user password.

Important:

- Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.
- Passwords for an external database implementation are not persisted. These values must be specified in the response file with the `D2C_DB_ADMIN_PASSWORD` and `D2C_DB_USER_PASSWORD` options before running a silent install.
- The installer attempts to validate the database. If the installer is unable to validate, you are prompted to reenter credentials or skip validation. If you skip validation, the response file must have the `SKIP_DATABASE_VALIDATION` property set to `true`. During a silent installation, the installer will complete the installation even when the database validation fails.

11. Review the Server Access Ports. A Server Access Port must be available to the end user across the firewall. Best security practices recommend using an HTTPS port.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

Table 16: Server Access Ports

Name	Default	Description
HTTP Port	8080	Port that exposes the Hybrid Data Pipeline service
HTTPS Port	8443	SSL port that exposes the Hybrid Data Pipeline service

12. Select whether you are using the On-Premises Connector.

- If using the On-Premises Connector, type `1` and press **ENTER**. Then continue to the next step.
- If not using the On-Premises Connector, type `2` and press **ENTER**. Continue at Step 14 on page 95.

13. Review the On-Premises Access Ports. The On-Premises Access Port and a Notification Server Port must be available across the firewall. Best security practices recommend using the SSL Notification Server Port.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

Table 17: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server

Name	Default	Description
SSL Port	11443	SSL port for the Notification Server
Message Queue Port	8282	Port for the message queue

14. Review the Server Internal Ports. A port for the internal API and the Shutdown Port must be opened. Best security practices recommend using the Internal API SSL Port.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of the Hybrid Data Pipeline instance.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

Table 18: Server Internal Ports

Name		Description
Internal API Port	8190	Non-SSL port for the Internal API
Internal API SSL Port	8090	SSL port for the Internal API
Shutdown Port	8005	Shutdown port

15. Review the installation summary. If you are satisfied with your choices, press **ENTER** to generate the response file.
16. After the response file has been generated, press **ENTER** to exit the installer.
17. Confirm that a response file has been generated by navigating to the response file directory you specified in Step 3 of "Creating a response file using the installer in console mode" and opening the response file.
18. You must now edit the response file according to the guidelines in Editing a console generated installation response file on page 99. In all scenarios, the response file must be edited to include passwords for the *d2cadmin* and *d2cuser* user accounts. Depending on your environment, the response file may require additional modification.

Creating a response file for a load balancer installation (console mode)

1. Make the appropriate selection regarding SSL configuration based on your environment.

Important: If an SSL certificate is not specified, the installer will not generate the configuration and certificate files required for the installation of the On-Premises Connector and the ODBC and JDBC drivers.

- Type `1` to specify the SSL certificate file to be used with the Hybrid Data Pipeline server. The specified file must be the root certificate used to sign the certificate for the load balancer server. PEM, DER, and Base64 encodings are supported. Type the full path to the certificate file. Then, press **ENTER**.

- Type `2` if you do not want to specify an SSL certificate.

2. Choose the appropriate option depending on whether you are using MySQL Community Edition. MySQL Community Edition can be used as an external system database or as a data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. However, you can use the MySQL Connector/J driver to use MySQL Community Edition as an external system database or as a data source.

   - Type `1` and press **ENTER**, if you are using MySQL Community Edition. Type the name and location of the MySQL Connector/J jar file, and press **ENTER** again.
   - Type `2` and press **ENTER**, if you are not using MySQL Community Edition in your environment.

   Note: To download the MySQL Connector/J driver, visit the MySQL developer website athttps://dev.mysql.com/.

3. Select the type of external system database you want to use to store system information.

   - Select **Oracle**, and continue at Step 4 on page 96.
   - Select **MySQLCommunity**, and continue at Step 5 on page 96.
   - Select **MSSQLServer**, and continue at Step 6 on page 97.
   - Select **PostgreSQL**, and continue at Step 7 on page 97.

4. Provide the Oracle connection information.

   a) Type the name of the host.

   b) Type the port number.

   c) Select the connection type. Do one of the following:

      - If you connect using the Oracle System Identifier (SID), type `1`, then type the SID.
      - If you connect using the Service Name, type `2`, then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name—a name that typically comprises the database name and domain name.

   d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as a semicolon-separated list of *`parameter=value`*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret; serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

   e) Press **ENTER**, and continue at Step 8 on page 97.

5. Provide connection information for the MySQL Community Edition external database.

   a) Type the name of the Hostname.

   b) Type the port number.

   c) Type the database name.

d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as a ampersand-separated list of *parameter=value*.

e) Press **ENTER**, and continue at Step 8 on page 97.

6. Provide the SQL Server connection information.

a) Type the name of the host.

b) Type the port number.

c) Type the database name.

d) Type the name of the schema.

e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.

f) Press **ENTER**, and continue at Step 8 on page 97.

7. Provide the PostgreSQL connection information.

a) Type the name of the host.

b) Type the port number.

c) Type the database name.

d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.

e) Press **ENTER**, and continue at Step 8 on page 97.

8. You are prompted to provide the database credential information for a user with administrator privileges and for a user without administrator privileges. After you enter the credential information, press **ENTER** to continue.

a) Type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.

b) You are prompted to provide the Admin Password. Type the password for a administrator account for the external database.

c) You are prompted to provide the username for a user who does *not* have administrator privileges. Type a user name. The standard user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.

d) You are prompted to provide the user password. Type the user password.

Important:

- Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.
- Passwords for an external database implementation are not persisted. These values must be specified in the response file with the `D2C_DB_ADMIN_PASSWORD` and `D2C_DB_USER_PASSWORD` options before running a silent install.
- The installer attempts to validate the database. If the installer is unable to validate, you are prompted to reenter credentials or skip validation. If you skip validation, the response file must have the `SKIP_DATABASE_VALIDATION` property set to `true`. During a silent installation, the installer will complete the installation even when the database validation fails.

9. Specify the desired Java configuration.

   Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

   - Type `1` if you will be using an external JRE (a JRE not installed with the server).
   - Type `2` if you will be using the embedded JRE installed with the server.

10. Specify the fully qualified location of the Java home directory. This is the path to the external JRE. Press **ENTER**.
11. Specify whether you want to enable FIPS on the Hybrid Data Pipeline server.

    Important: To implement FIPS, your hardware must support secure random, or you must have a secure random daemon installed.

    - Type `1` if you want to enable FIPS. Press **ENTER** and continue to the next step.
    - Type `2` and press **ENTER** if you want to use the default setting which is FIPS disabled.

12. Review the Server Access Port. The Server Access Port must be opened for the load balancer. The default is 8080.

    Note: In most cases, the default port works without problems. However, your environment might have already defined a function for the port. If the default port is in use, the installer pops up a message so that you can make the necessary changes.

13. Select whether you are using the On-Premises Connector.

    Note: An SSL certificate must be specified in Step 1 on page 95 to use the On-Premises Connector.

    - If using the On-Premises Connector, type `1` and press **ENTER**. Then continue to the next step.
    - If not using the On-Premises Connector, type `2` and press **ENTER**. Continue at Step 15 on page 99.

14. Review the On-Premises Access Ports. The On-Premises Access Port and the TCP Notification Server Port must be opened for the load balancer.

    Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

    Table 19: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
Message Queue Port	8282	Port for the message queue

15. Review the Server Internal Ports. The Internal API Port and the Shutdown Port must be opened.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of any Hybrid Data Pipeline instance.

Note: In most cases, the default ports work without problems. However, your environment might have already defined a function for one or more of the ports. If a default port is in use, the installer pops up a message so that you can make the necessary changes.

Table 20: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Shutdown Port	8005	Shutdown port

16. Review the installation summary. If you are satisfied with your choices, press **ENTER** to generate the response file.
17. After the response file has been generated, press **ENTER** to exit the installer.
18. Confirm that a response file has been generated by navigating to the response file directory you specified in Step 3 of "Creating a response file using the installer in console mode" and opening the response file.
19. You must now edit the response file according to the guidelines in Editing a console generated installation response file on page 99. In all scenarios, the response file must be edited to include passwords for the *d2cadmin* and *d2cuser* user accounts. Depending on your environment, the response file may require additional modification.

Editing a console generated installation response file

After you have generated a response file, you must edit the response file to suit your environment before you perform a silent installation. Use the following guidelines to edit your response file.

- You must specify passwords for the default *d2cadmin* and *d2cuser* accounts. Best practices recommend that you follow the Hybrid Data Pipeline default password policy when specifying these account passwords. When initially logging in to the Web UI or using the API, you must authenticate as one of these users. These settings take the following form.

```
D2C_ADMIN_PASSWORD_CONSOLE=\"<admin_password>\"
D2C_USER_PASSWORD_CONSOLE=\"<user_password>\"
```

- If you are installing the Hybrid Data Pipeline server on a system other than the one you used to generate the response file, you must designate the host machine with the `D2C_HOSTNAME_CONSOLE` option.
- If you want to continue with an installation even though hostname, port, load balancer hostname validations fail, then the validation settings should be set as follows. (Note that these properties are set to `false` by default.)

```
SKIP_HOSTNAME_VALIDATION=true
SKIP_PORT_VALIDATION=true
SKIP_LB_HOSTNAME_VALIDATION=true
```

- If you are storing user credentials on an external database, you must designate the administrator and user passwords of the external database with the `D2C_DB_ADMIN_PASSWORD` and `D2C_DB_USER_PASSWORD`

options. However, you may skip database validation by setting the `SKIP_DATABASE_VALIDATION` property to `true`. If you skip database validation, the installer will complete the installation even when the database validation fails.

The following example response file includes the settings for a load balancer deployment using the On-Premises Connector, using a MySQL Community Edition external database. This type of response file would be generated using the installer in console mode.

```
# Tue Nov 21 15:45:31 EST 2017
# Replay feature output
# ---------------------
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.



#Choose Install Folder
#---------------------
USER_INSTALL_DIR=<install_dir>

#Installation License Type
#-------------------------
D2C_LICENSE_TYPE_CONSOLE=\"Evaluation\",\"\"

#Enter Hostname
#--------------
D2C_HOSTNAME_CONSOLE=\"<hybriddatapipelinehost>\"

#SKIP VALIDATION SETTINGS
#--------------------------------
SKIP_HOSTNAME_VALIDATION=true
SKIP_PORT_VALIDATION=true

#Install Type
#------------
D2C_INSTALL_TYPE_CONSOLE=\"\",\"Custom\"

#Key Location
#------------
USER_INPUT_KEY_LOCATION_CONSOLE_OPTION=\"Specify location\",\"\"
USER_INPUT_KEY_LOCATION_CONSOLE=\"<keyfilepath>\"

#Password Configuration
#----------------------
D2C_ADMIN_PASSWORD_CONSOLE=\"AdminSecret\"
D2C_USER_PASSWORD_CONSOLE=\"UserSecret\"

#Java Configuration
#------------------
SPECIFY_JAVA_HOME_YESNO=\"No\",\"\"

#FIPS Configuration
#------------------
D2C_USING_FIPS_CONFIG_CONSOLE=\"No\",\"\"

#Load Balancing
#--------------
D2C_LOAD_BALANCER_CONSOLE=\"\",\"Network Load Balancer\",\"\"
LOAD_BALANCING_HOST_NAME_CONSOLE=\"<loadbalancerhost>\"

#SKIP VALIDATION SETTINGS
#------------------------
SKIP_LB_HOSTNAME_VALIDATION=true

#Certificate File
#----------------
D2C_CERT_FILE_YESNO=\"Yes\",\"\"
D2C_CERT_FILE_CONSOLE=\"/<sslcertficatepath>/<filename>\"
```

```
#MySQL Community Edition
#-----------------------
D2C_DB_MYSQL_COMMUNITY_SUPPORT_CONSOLE=\"Yes\",\"\"
D2C_DB_MYSQL_JAR_PATH_CONSOLE=\"/<mysqldriverpath>/<filename>.jar\"

#External Database Type
#----------------------
D2C_DB_VENDOR_CONSOLE=\"\",\"MySQLCommunity\"

#Database Connection Information - MySQLCommunity Hostname
#---------------------------------------------------------
D2C_DB_HOSTNAME_CONSOLE=\"<mysqlhost>\"

#Database Connection Information - MySQLCommunity Port
#----------------------------------------------------
D2C_DB_PORT_CONSOLE=\"3306\"

#Database Connection Information - MySQL Database Name
#----------------------------------------------------
D2C_DATABASE_NAME_CONSOLE=\"<mysqldbname>\"

#Database Connection Information - MySQL Connection Advanced Options
#------------------------------------------------------------------
D2C_DB_ADVANCED_OPTIONS_CONSOLE=\"\"

#Database Connection Information - Admin Username
#-----------------------------------------------
D2C_DB_ADMIN_USERNAME_CONSOLE=\"<adminname>\"

#Database Connection Information - Admin Password
#-----------------------------------------------
D2C_DB_ADMIN_PASSWORD_CONSOLE=\"<adminpassword>\"

#Database Connection Information - User Username
#----------------------------------------------
D2C_DB_USER_USERNAME_CONSOLE=\"<username>\"

#Database Connection Information - User Password
#----------------------------------------------
D2C_DB_USER_PASSWORD_CONSOLE=\"<userpassword>\"

#Database Connection Validation
#-----------------------------
SKIP_DATABASE_VALIDATION=false

#HDP Server Access Ports - HTTP Port
#----------------------------------
D2C_API_PORT_CONSOLE=\"8080\"

#On-Premises Settings
#--------------------
ENABLE_OPC_CONSOLE=\"Yes\",\"\"

#On-Premises Ports - On-Premises Port
#-----------------------------------
D2C_OPC_PORT_CONSOLE=\"40501\"

#On-Premises Ports - Notification TCP Port
#----------------------------------------
D2C_NOTIFICATION_PORT_CONSOLE=\"11280\"

#On-Premises Ports - Message Queue Port
#-------------------------------------
D2C_MESSAGE_QUEUE_PORT_CONSOLE=\"8282\"

#Server Internal Ports - Internal API Port
#----------------------------------------
D2C_INTERNAL_API_PORT_CONSOLE=\"8190\"
```

```
#Server Internal Ports - Shutdown Port
#-------------------------------------
D2C_SHUTDOWN_PORT_CONSOLE=\"8005\"
```

Performing a silent installation

After you have generated and edited your response file, you can perform a silent installation.

Take the following steps to perform a silent installation:

1. From a command-line prompt, navigate to the directory where you saved the product file. Alternatively, place the product file directory on your path before proceeding to the next step.

   The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin`, where *nn* is the version of the product.

2. Execute a silent installation by entering the following command and pressing **ENTER**.

   `PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -i silent -f response_file`

   where *response_file* is the full path of the response file you have created and edited. For example, if the response file is named `pipeline.response` and resides in the directory `/home/users/johndoe`, you would enter:

   `PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -i silent -f response_file`

3. The installation proceeds without any further user intervention unless you enter an incorrect value on the console or in the response file, in which case an error is displayed and installation stops.
4. Verify the installation by accessing the Hybrid Data Pipeline user interface from a browser. The login page should appear. For example:

   `https://<myserver>:8443/`

   where for a standalone installation:

   <myserver> is the fully qualified hostname of the machine where you installed Hybrid Data Pipeline.

   where for a load balancer installation:

   <myserver> is the fully qualified hostname or IP address of the load balancer.

   After logging in, administrators can verify product version information by selecting **About** from the question mark drop-down menu. For more information on retrieving version information, refer to "Get Version Information" in the *Progress DataDirect Hybrid Data Pipeline User's Guide*.

Refer to installation log files for a record of any problems that may have occurred during the installation. See Server installation log files on page 166 for details.

Note: Silent installation creates a file named "custom" in the installer launch directory. This file is a resource bundle properties file containing key value paired messages, and is created by the Third Party Software (InstallAnywhere) that is used to build the HDP server installer. Note that having this file created after silent installation is normal and this does not indicate any issue. Currently there is no way to avoid the creation of this file and it can be deleted once installation is completed.

What to do next

During installation of the Hybrid Data Pipeline server, four configuration and certificate files are generated. For a standalone deployment, these files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. For a load balancer deployment, these files are stored in a key location specified during installation. Before installing a component such as the ODBC driver, the JDBC driver, or the On-Premises Connector, these files must be copied to the installer directory of the component you are installing.

Note: If an SSL certificate is not specified in a load balancer response file, the installer will not generate the configuration and certificate files required for the installation of the On-Premises Connector and the ODBC and JDBC drivers.

The four configuration and certificate files are:

- `config.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`
- `OnPremise.properties`

Install using a Docker image

You can also install Hybrid Data Pipeline on a standalone node for a 30 day evaluation period using a Docker image. Installing Hybrid Data Pipeline with a Docker image minimizes the time it takes to set up a node and configure Hybrid Data Pipeline. The Hybrid Data Pipeline Docker image contains all the libraries and other dependencies needed for running Hybrid Data Pipeline. Installing with a Docker image is best suited for getting an instance of Hybrid Data Pipeline up and running for evaluation and testing purposes.

Note: An installation with a Docker image is for evaluation purposes. It cannot be upgraded to a licensed installation, and it cannot be migrated to a load balancer environment. If you want to move from a test environment to a production environment, you should begin by deploying Hybrid Data Pipeline on a single node behind a load balancer with the Hybrid Data Pipeline installation program. When deploying the service on a single node behind a load balancer, you can increase availability and scalability as demanded, and address security and recovery concerns as required.

Before you proceed with a Docker installation of Hybrid Data Pipeline, you must download and install Docker on your machine.

1. Download the Hybrid Data Pipeline Docker image.
   a) Visit the Progress DataDirect hybrid data integration page and click **TRY NOW**.
   b) Enter your information and click **DOWNLOAD**.
   c) Click the Docker Image **DOWNLOAD** button.
2. Run the following command to load the image into the Docker image repository.

   ```
   docker load -i hdp_eval_docker.tar.gz
   ```

3. Run the following command to confirm that the image has been loaded.

   ```
   docker images
   ```

   A list of Docker images is shown. The list includes details such as TAG, Image ID, time of image creation, and size of image. If the list of entries includes one titled `hdp_eval_<version_number>`, the Docker image has been successfully loaded into the image repository.

4. Run the Docker image with the following command.

Note: If you plan to spin up multiple Hybrid Data Pipeline containers, you must provide different Docker platform port numbers for each instance when mapping ports.

Note: The following command accepts the Hybrid Data Pipeline license agreement. See EULA for the license agreement.

Command syntax

```
docker run -dt --name <container_name>
   -p <docker_port_1>:8080 -p <docker_port_2>:8443
   -e "ACCEPT_EULA=true" -e "HDP_HOSTNAME=<docker_hostname>"
   -e "HDP_ADMIN_PASSWORD=<admin_password>"
   -e "HDP_USER_PASSWORD=<user_password>"
   <hdp_docker_image_name>:<docker_tag>
```

Where:

`container_name`

is an optional user specified name for the Docker container.

`docker_port_1`

maps a Docker port to a container port. Hybrid Data Pipeline will be accessible on the Docker host machine (`<docker_hostname>:<docker_port_1>`). Port 8080 is the default HTTP port that exposes Hybrid Data Pipeline.

`docker_port_2`

maps a Docker port to a container port. Hybrid Data Pipeline will be accessible on the Docker host machine (`<docker_hostname>:<docker_port_2>`). Port 8443 is the default HTTPS port that exposes Hybrid Data Pipeline.

`docker_hostname`

is the name of the machine hosting the Docker platform. Ensure that the valid hostname of the Docker platform is provided. The hostname will not be validated.

`admin_password`

is the password for the default Hybrid Data Pipeline administrator `d2cadmin`.

`user_password`

is the password for the default Hybrid Data Pipeline user `d2cuser`.

`hdp_docker_image_name`

is the name of the Hybrid Data Pipeline Docker image.

`docker_tag`

is the Docker TAG for the Hybrid Data Pipeline Docker image, as provided via the `docker images` command.

Example

```
docker run -dt --name my_hdp_eval
   -p 8080:8080 -p 8443:8443 -e "ACCEPT_EULA=true"
   -e "HDP_HOSTNAME=centos7264" -e "HDP_ADMIN_PASSWORD=d2cadmin"
   -e "HDP_USER_PASSWORD=d2cuser" hdp_eval_0.0.0:5
```

5. Take the following steps to deploy Hybrid Data Pipeline with an SSL certificate using a Docker image installation.

Note: The SSL certificate file must be in the PEM file format. See SSL certificates for standalone deployment on page 20 for details.

---

a) Copy the SSL certificate to a separate directory on the Docker host machine.

b) Run the Docker image with the following command. The `-v` option mounts the SSL certificate directory during the installation of the image. The mount point for mounted volume MUST be `/shared`. Note that if Docker is running in Windows, the drive that has the directory to be mounted must be marked as a shared driver in the Docker settings.

Command syntax

```
docker run -dt --name <container_name>
   -p <docker_port_1>:8080 -p <docker_port_2>:8443
   -e "ACCEPT_EULA=true" -e "HDP_HOSTNAME=<docker_hostname>"
   -e "HDP_ADMIN_PASSWORD=<admin_password>" -e "HDP_USER_PASSWORD=<user_password>"
   -e "HDP_CERT_FILE_NAME=<hdp_ssl_cert_file_name>"
   -v /<hdp_ssl_cert_file_directory>:/shared <hdp_docker_image_name>:<docker_tag>
```

Where:

`hdp_ssl_cert_file_name`

is the name of the Hybrid Data Pipeline SSL certificate file.

`hdp_ssl_cert_file_directory`

is the location of the Hybrid Data Pipeline SSL certificate on the Docker host machine.

Example

```
docker run -dt --name my_hdp_eval
   -p 8080:8080 -p 8443:8443 -e "ACCEPT_EULA=true"
   -e "HDP_HOSTNAME=centos7264" -e "HDP_ADMIN_PASSWORD=d2cadmin"
   -e "HDP_USER_PASSWORD=d2cuser"
   -e "HDP_CERT_FILE_NAME=ddcloud.bundle.pem"
   -v /shared_files:/shared hdp_eval_0.0.0:5
```

6. If you plan to install the On-Premises Connector, the ODBC driver, or the JDBC driver, you must expose additional ports as shown in the table below. (See also Access ports for standalone deployment on page 19.)

Table 21: Ports required for On-Premises Connector, the ODBC driver, and the JDBC driver

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector

Name	Default	Description
TCP Port	11280	Port for the Notification Server
SSL Port	11443	SSL port for the Notification Server

Note: If the Docker platform port numbers mapped are not the same as the container port numbers, you must update these port numbers in the `OnPremise.properties` file when installing the On-Premises Connector, the ODBC driver, or the JDBC driver. See What to do next for details.

Command syntax

```
docker run -dt --name <container_name>
   -p <docker_port_1>:8080 -p <docker_port_2>:8443
   -p <docker_port_3>:11443 -p <docker_port_4>:40501 -p <docker_port_5>:11235
   -p <docker_port_6>:11280 -e "ACCEPT_EULA=true" -e "HDP_HOSTNAME=<docker_hostname>"
   -e "HDP_ADMIN_PASSWORD=<admin_password>" -e "HDP_USER_PASSWORD=<user_password>"
   <hdp_docker_image_name>:<docker_tag>
```

Example

```
docker run -dt --name my_hdp_eval
   -p 8080:8080 -p 8443:8443 -p 11443:11443 -p 40501:40501
   -p 11235:11235 -p 11280:11280 -e "ACCEPT_EULA=true"
   -e "HDP_HOSTNAME=centos7264" -e "HDP_ADMIN_PASSWORD=d2cadmin"
   -e "HDP_USER_PASSWORD=d2cuser" hdp_eval_0.0.0:5
```

7. To obtain the status of the Hybrid Data Pipeline service running in the Docker container, execute the following command.

   Command syntax

   ```
   docker logs <container_name>
   ```

   Example

   ```
   docker logs my_hdp_eval
   Initializing Hybrid Data Pipeline container...
   Hybrid Data Pipeline services are up and running.
   ```

   Note: The `docker logs` command and other Docker commands can be run with the container ID as well as the container name. To obtain the container ID you can run the `docker ps` command.

8. Verify the installation by accessing the Hybrid Data Pipeline user interface from a browser. The server will be accessible via the Docker platform hostname and mapped port. For example, `http://centos7264:8080`.

   Note: The Hybrid Data Pipeline server is installed for a 30 day evaluation period.

What to do next

When you run the Hybrid Data Pipeline Docker image, four configuration and certificate files are generated. These files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. Before installing a component such as the ODBC driver, the JDBC driver, or the On-Premises Connector, these files must be copied to the installer directory of the component you are installing.

Note: If the Docker platform port numbers mapped in Step 6 on page 105 are not the same as the container port numbers, you must update these port numbers in the `OnPremise.properties` file when installing the On-Premises Connector, the ODBC driver, or the JDBC driver.

You can use the following command to copy the four configuration and certificate files from the Docker container to the directory from which the component installer will be run.

Syntax

```
docker cp
<container_name>:/opt/Progress/DataDirect/Hybrid_Data_Pipeline/Hybrid_Server/redist
/<destination_folder>
```

Example

```
docker cp my_hdp_eval:/opt/Progress/DataDirect/Hybrid_Data_Pipeline/Hybrid_Server/redist
 /jdbc_client_installer
```

The four configuration and certificate files are:

- `config.properties`
- `OnPremise.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`

Stopping and starting a Hybrid Data Pipeline Docker container

Hybrid Data Pipeline configurations are retained when stopping and starting the Hybrid Data Pipeline Docker container with the `docker stop` and `docker start` commands. The following examples show how to use these commands to stop and start the service.

Important: Hybrid Data Pipeline configurations are persisted in the Docker container. They are not mounted from an outside volume. Therefore, if the Docker container is deleted or disposed of, all configurations are lost.

Stop Hybrid Data Pipeline Docker container

The `docker stop` command results in a clean shutdown of the Hybrid Data Pipeline server.

- **Syntax**

  ```
  docker stop <container-name> | <container-id>
  ```

- **Example**

  ```
  docker stop my_hdp_eval
  ```

Start Hybrid Data Pipeline Docker container

The `docker start` command restarts the Hybrid Data Pipeline server.

- **Syntax**

  ```
  docker start <container-name> | <container-id>
  ```

- **Example**

```
docker start my_hdp_eval
```

Accessing the Hybrid Data Pipeline Docker container terminal

The following Docker command can be used to access the Hybrid Data Pipeline Docker container terminal. Access to the container terminal allows you to view system logs and otherwise inspect folders and files included in the Hybrid Data Pipeline installation.

Syntax

```
docker exec -it <hdp_container_name> /bin/bash
```

Example

```
docker exec -it my_hdp_eval /bin/bash
```

Upgrading Hybrid Data Pipeline server

The Hybrid Data Pipeline installer supports upgrading server installations in GUI or console mode.

Note: The installer does not support changing a standalone deployment to a load balancer deployment during an upgrade, or vice versa. To make such a change, you would need to uninstall the server and then reinstall it. See Uninstalling Hybrid Data Pipeline server on page 166 and Installing the Hybrid Data Pipeline server on page 47 for details.

If you deployed Hybrid Data Pipeline behind a load balancer, you must upgrade each node in the cluster. Any modifications you make to the configuration of the Hybrid Data Pipeline server during the upgrade of an initial node result in corresponding updates to internal files located in the key location. The installer uses these files when upgrading any additional nodes.

If you are using the silent installation process to upgrade cluster nodes, the response file generated during the initial upgrade must be modified to upgrade the server on any additional nodes. For a GUI generated response file, you will need to designate the name of an additional node with the `D2C_HOSTNAME` option. For a console generated response file, you will need to designate the name of an additional node with the `D2C_HOSTNAME_CONSOLE` option. See Silent upgrade process on page 134 for details.

Note: Before running the installer to perform an upgrade in a load balancer environment, the service must be shutdown on each node by running the `stop.sh` script. See Stopping and starting the Hybrid Data Pipeline service on page 165 for details.

Note: Before proceeding with an upgrade of the Hybrid Data Pipeline server, you must copy the product upgrade file to a temporary directory, for example, `/tmp`.

Depending on your preferred method for upgrading, proceed to the appropriate set of instructions:

- If you prefer to use a Graphical User Interface (GUI), see either of the following topics.
  - Standalone upgrade (GUI mode) on page 109
  - Load balancer upgrade (GUI mode) on page 116

- If you prefer to use the console, see either of the following topics.
  - Standalone upgrade (console mode) on page 123
  - Load balancer upgrade (console mode) on page 129
- If you prefer to use a silent installation, see Silent upgrade process on page 134.

Standalone upgrade (GUI mode)

Note: The installer does not support changing a standalone deployment to a load balancer deployment during an upgrade, or vice versa. To make such a change, you would need to uninstall the server and then reinstall it. See Uninstalling Hybrid Data Pipeline server on page 166 and Installing the Hybrid Data Pipeline server on page 47 for details.

After copying the product installation file to a temporary directory, take the following steps to upgrade a standalone deployment with the installer in GUI mode.

1. From a command-line prompt, navigate to the directory where you saved the product upgrade file. Alternatively, place the product upgrade file directory on your path before proceeding to the next step.

   The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin`, where *nn* is the version of the product.

2. Make the file an executable using the `chmod` command. Then, press **ENTER**. For example:

   ```
   chmod +x ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

3. Run the executable by entering the product file path and pressing **ENTER**.

   a) Type the file name and path of the product file. For example:

   ```
   ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

   b) Press **ENTER**.

   c) The **Introduction** window appears. Click **Next** to continue.

   Note: If the installer cannot continue with a GUI installation, a message is displayed, and the installation continues in console mode.

4. The License Agreement window appears. Make sure that you read and understand the license agreement. To continue with the installation, select the **I accept the terms in the License Agreement** option; then, click **Next**.

   Note: You can exit the installation program at any time by clicking **Cancel** or return to the previous window by clicking **Previous**.

5. Enter or choose the directory of the installation you want to upgrade; then, click **Next**. A pop-up dialog appears. Click **Upgrade** to continue.
6. Choose whether you want to upgrade with an evaluation or licensed version of the product. Licensed installations require a valid License Key.

- Evaluation. Select this option to upgrade with an evaluation version that is fully functional for 30 days. Then, click **Next**.
- Licensed. Select this option if you purchased a licensed version of the product. Type the license key, including any dashes, and then click **Next**.

7. Accept or enter the fully qualified hostname for the Hybrid Data Pipeline server. By default, the installer suggests the name of the current machine. Then, click **Next**.

Note: If the installer is unable to validate the hostname, you are prompted to reenter the hostname or skip validation. Skipping validation is often desired when performing a silent upgrade. See Silent upgrade process on page 134 for details.

---

8. Select how you want to continue the upgrade.

- Select **Express** to persist previously established values. Then, click **Next** and continue at Step 23 on page 116.
- Select **Modify settings** to change values for the following configurations. Then, click **Next**.
  - Change the location of the SSL certificate file
  - Change the Java configuration to use an external JRE
  - Enable or disable FIPS
  - Add MySQL Community Edition as a data store or external system database
  - Change the system database you are using
  - Update external system database credentials
  - Enable or disable the On-Premises Connector
  - Change Server Access Ports
  - Change On-Premises Connector Ports
  - Change Server Internal Access Ports

Note: The key location where the generated key and internal files are stored cannot be modified when performing an upgrade.

---

9. Select the desired Java configuration.

Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

- Select **Use default Java** if you will be using the embedded JRE installed with the server.
- Select **Java home directory** and provide the path to an external JRE if you will be using a JRE not installed with the server.

10. Select whether you want to enable FIPS on the Hybrid Data Pipeline server.

Important: To enable FIPS, your hardware must support secure random, or you must have a secure random daemon installed.

Important: When you enable FIPS during an upgrade, the environment uses the encryption key for the system database that was generated during the original installation of the server. This encryption key, while generated with a FIPS compliant algorithm, was not generated with a FIPS certified implementation of the algorithm.

11. Depending on your environment, provide the appropriate SSL certificate information.
    - Select **Certificate file** to specify a PEM file to be used by the server to establish SSL connections with ODBC and JDBC client applications. Type the full path to the PEM file, or click **Choose...** to browse to the location of the PEM file. Then, click **Next**.

      Note: The PEM file must consist of a private key, a public key certificate issued by a certificate authority (CA), and additional certificates that make up the trust chain. See The PEM file on page 20 for more information.
    - Select **Use existing Certificate** to use the SSL certificate specified in the previous installation or the self-signed certificate included with the installation. Then, click **Next**.

      Note: The self-signed certificate may be used in a test environment. However, for production, a PEM file with required information should be specified. See The PEM file on page 20 for more information.
12. Select whether you want to use MySQL Community Edition as a data source or external database. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition; however, it does support the MySQL Connector/J driver. If you choose **Yes**, in the **Jar Path** field, provide the name and location of the driver's jar file. Click **Next** to continue.

    Note: For more information on the MySQL Connector/J driver, refer to the MySQL developer website at https://dev.mysql.com/.

13. Select the type of database you want to use to store system information.
    - Select **Internal Database (supplied by this install)** to use the default internal database. Click **Next** and continue at Step 21 on page 114.
    - Select **External Database** to store the system information in an external database. Then, from the drop down box, choose your database vender. Then, click **Next**.
      - Select **Oracle**, and continue at Step 14 on page 111.
      - Select **MySQLCommunity**, and continue at Step 15 on page 112.
      - Select **MSSQLServer**, and continue at Step 16 on page 112.
      - Select **PostgreSQL**, and continue at Step 17 on page 112.

    Note: Users and data sources created in the internal database are specific to the internal database. They are not migrated to the external database if you subsequently modify the Hybrid Data Pipeline server to use an external database.

14. Provide the Oracle connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Select the connection type. Do one of the following:

- If you connect using the Oracle System Identifier (SID), select **Connect using SID**, then type the SID.
- Select **Connect using Service Name**, then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name. The global database name typically comprises the database name and domain name.

d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection url. Values should be entered as a semicolon-separated list of *parameter=value*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret;serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

e) Click **Next**, and continue at Step 18 on page 112.

15. Provide connection information for the MySQL Community Edition database.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection url. Values should be entered as a ampersand-separated list of *parameter=value*.
    e) Click **Next**, and continue at Step 18 on page 112.
16. Provide the SQL Server connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Type the name of the schema.
    e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
    f) Click **Next**, and continue at Step 18 on page 112.
17. Provide the PostgreSQL connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
    e) Click **Next**, and continue at Step 18 on page 112.
18. Provide the external database credential information.

Note: Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.

Note: If the installer is unable to validate, you are prompted to reenter credentials or skip validation. Skipping validation is often desired when performing a silent upgrade. See Silent upgrade process on page 134 for details.

- In the **Admin Username** field, type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- In the **Admin Password** field, type the password for an external database administrator account.
- In the **Username** field, type a user name. The standard user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- In the **Password** field, type the user password.

19. Review the Server Access Ports. A Server Access Port must be available to the end user across the firewall. Best security practices recommend using an HTTPS port.

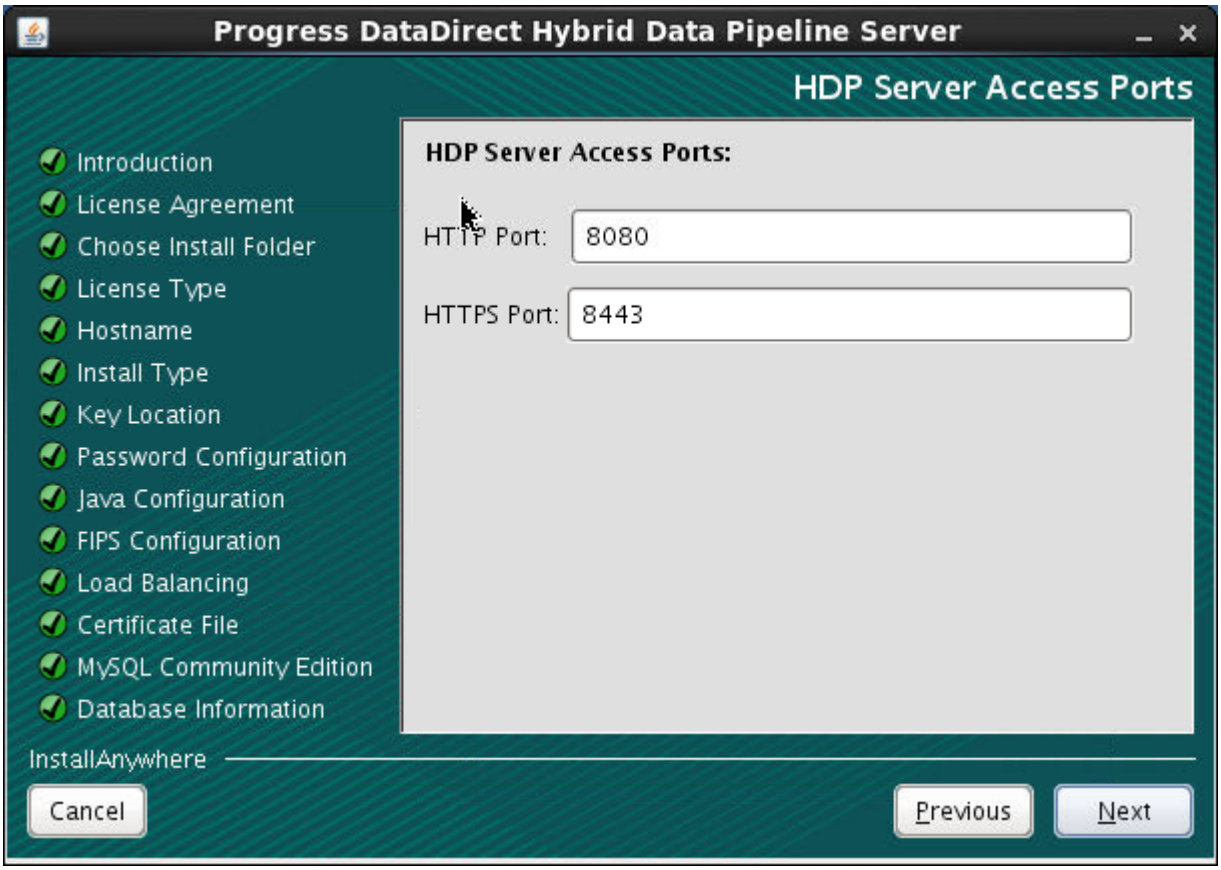


Table 22: Server Access Ports

Name	Default	Description
HTTP Port	8080	Port that exposes Hybrid Data Pipeline
HTTPS Port	8443	SSL port that exposes Hybrid Data Pipeline

20. Select whether you will continue to use the On-Premises Connector.
    - If using the On-Premises Connector, select **Enable On-Premises Connector**. Click **Next** and continue to the next step.
    - If not using the On-Premises Connector, leave the check box empty and click **Next**. Continue at Step 22 on page 115.
21. Review the On-Premises Access Ports. The On-Premises Access Port and a Notification Server Port must be available across the firewall. Best security practices recommend using the SSL Notification Server Port.

Important: If you change any values for On-Premises Access Ports during an upgrade, you will need to reinstall the On-Premises Connector with the updated distribution files in the `redist` subdirectory. See What to do next.

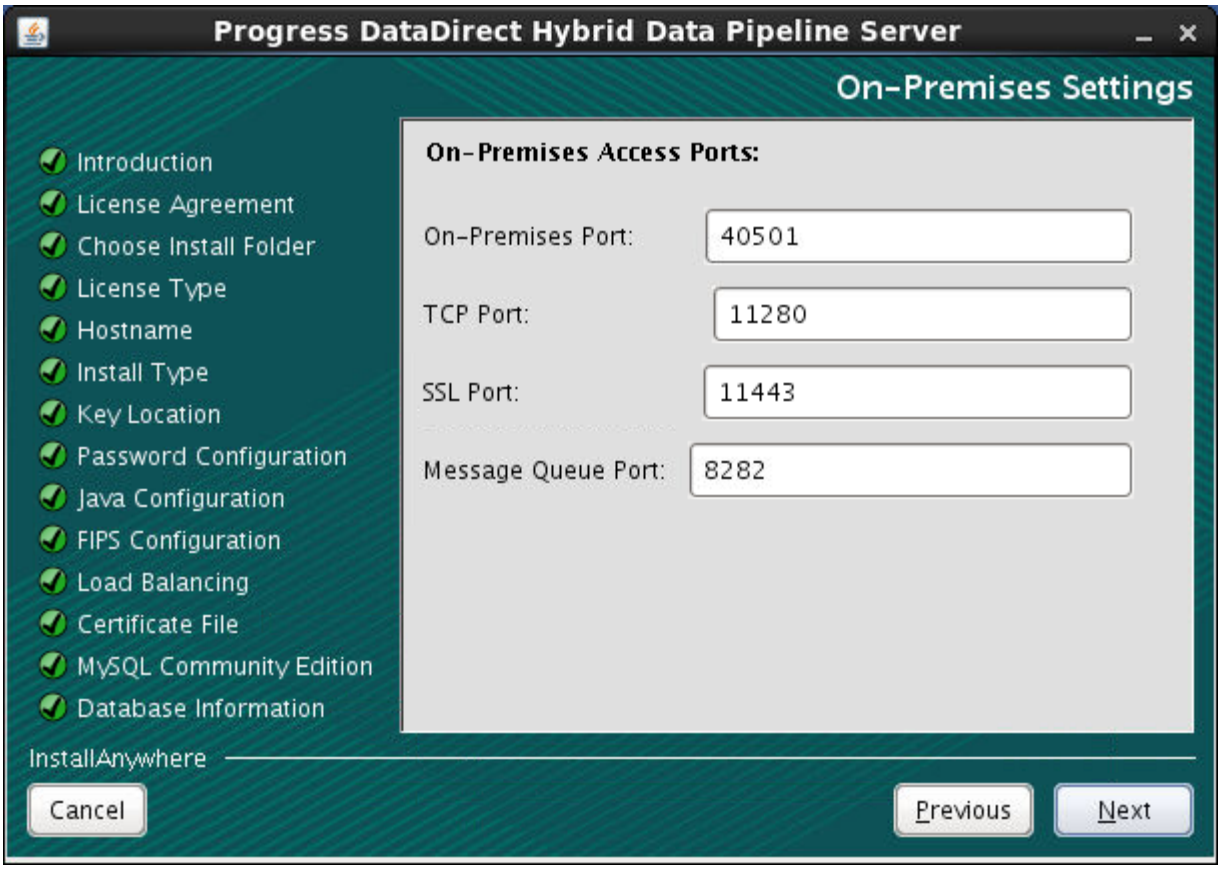


Table 23: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
SSL Port	11443	SSL port for the Notification Server
Message Queue Port	8282	Port for the message queue

22. Review the Server Internal Ports. A port for the internal API and the Shutdown Port must be opened. Best security practices recommend using the Internal API SSL Port.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of the Hybrid Data Pipeline instance.

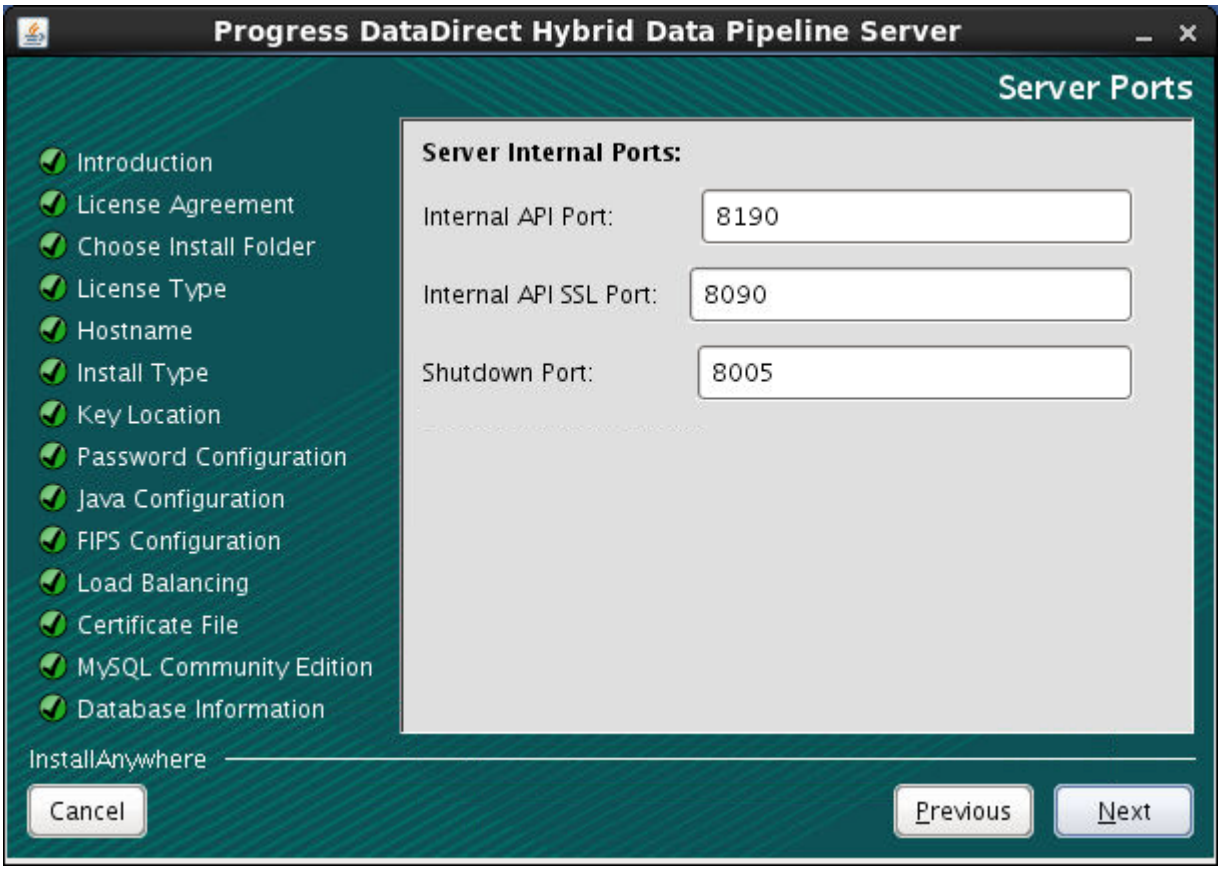


Table 24: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API

Name	Default	Description
Internal API SSL Port	8090	SSL port for the Internal API
Shutdown Port	8005	Shutdown port

23. Review the summary. If you are satisfied with your choices, press **ENTER** to upgrade.
24. After the upgrade has finished, press **ENTER** to exit the installer.
25. Verify the upgrade by accessing the Hybrid Data Pipeline user interface from a browser. The login page should appear. For example, type the following.

    `https://<myserver>:8443/`

    where `<myserver>` is the fully qualified hostname of the machine where you installed Hybrid Data Pipeline.

    After logging in, administrators can verify product version information by selecting **About** from the question mark drop-down menu. For more information on retrieving version information, refer to "Get Version Information" in the *Progress DataDirect Hybrid Data Pipeline User's Guide*.

Refer to installation log files for a record of any problems that may have occurred during the upgrade. See Server installation log files on page 166 for details.

What to do next

If you change any of the On-Premises Connector Ports, you will need to reinstall the On-Premises Connector with updated configuration and certificate files. These files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. These files must be copied to the directory of the On-Premises Connector installer before proceeding with the reinstallation of the On-Premises Connector.

The four configuration and certificate files are:

- `config.properties`
- `OnPremise.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`

See Installing the Hybrid Data Pipeline On-Premises Connector on page 191 for further details.

Load balancer upgrade (GUI mode)

Note: The installer does not support changing a standalone deployment to a load balancer deployment during an upgrade, or vice versa. To make such a change, you would need to uninstall the server and then reinstall it. See Uninstalling Hybrid Data Pipeline server on page 166 and Installing the Hybrid Data Pipeline server on page 47 for details.

After copying the product installation file to a temporary directory, take the following steps to upgrade a load balancer deployment with the installer in GUI mode.

1. From a command-line prompt, navigate to the directory where you saved the product upgrade file. Alternatively, place the product upgrade file directory on your path before proceeding to the next step.

The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin`, where *nn* is the version of the product.

2. Make the file an executable using the `chmod` command. Then, press **ENTER**. For example:

   ```
   chmod +x ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

3. Run the executable by entering the product file path and pressing **ENTER**.

   a) Type the file name and path of the product file. For example:

   ```
   ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

   b) Press **ENTER**.

   c) The **Introduction** window appears. Click **Next** to continue.

Note: If the installer cannot continue with a GUI installation, a message is displayed, and the installation continues in console mode.

---

4. The License Agreement window appears. Make sure that you read and understand the license agreement. To continue with the installation, select the **I accept the terms in the License Agreement** option; then, click **Next**.

Note: You can exit the installation program at any time by clicking **Cancel** or return to the previous window by clicking **Previous**.

---

5. Enter or choose the directory of the installation you want to upgrade; then, click **Next**. A pop-up dialog appears. Click **Upgrade** to continue.
6. Choose whether you want to upgrade with an evaluation or licensed version of the product. Licensed installations require a valid License Key.

   - Evaluation. Select this option to upgrade with an evaluation version that is fully functional for 30 days. Then, click **Next**.
   - Licensed. Select this option if you purchased a licensed version of the product. Type the license key, including any dashes, and then click **Next**.

7. Accept the fully qualified hostname for the Hybrid Data Pipeline server. By default, the installer suggests the name of the current machine. Then, click **Next**.

Note: If the installer is unable to validate the hostname, you are prompted to reenter the hostname or skip validation. Skipping validation is often desired when performing a silent upgrade. See Silent upgrade process on page 134 for details.

---

8. Select how you want to continue the upgrade.

   - Select **Express** to persist previously established values. Then, click **Next** and continue at Step 22 on page 122.
   - Select **Modify settings** to change values for the following configurations. Then, click **Next**.
     - Change the location of the SSL certificate file
     - Change the Java configuration to use an external JRE
     - Enable or disable FIPS

- Add MySQL Community Edition as a data store or external system database
- Change the system database you are using
- Update external system database credentials
- Change Server Access Ports
- Change On-Premises Connector Ports
- Change Server Internal Access Ports

Note: The following elements of an installation cannot be modified when performing an upgrade of a load balancer installation: key location, load balancer hostname, and On-Premises Connector enablement.

9. Select the desired Java configuration.

Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

- Select **Use default Java** if you will be using the embedded JRE installed with the server.
- Select **Java home directory** and provide the path to an external JRE if you will be using a JRE not installed with the server.

10. Select whether you want to enable FIPS on the Hybrid Data Pipeline server.

Important: To enable FIPS, your hardware must support secure random, or you must have a secure random daemon installed.

Important: When you enable FIPS during an upgrade, the environment uses the encryption key for the system database that was generated during the original installation of the server. This encryption key, while generated with a FIPS compliant algorithm, was not generated with a FIPS certified implementation of the algorithm.

11. Depending on your environment, provide the appropriate SSL certificate information.

- Select **Certificate file** to specify the SSL certificate file to be used with the Hybrid Data Pipeline server. The specified file must be the root certificate used to sign the certificate for the load balancer server. PEM, DER, and Base64 encodings are supported. Type the full path to the certificate file, or click **Choose...** to browse to the location of the SSL certificate file. Then, click **Next**.
- Select **Use existing Certificate** to use the SSL certificate specified in the previous installation or bypass the specification of an SSL certificate. Then, click **Next**.

12. Select MySQL Community Edition if you plan to use MySQL Community Edition as an external system database or as a data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. However, you can use the MySQL Connector/J driver to use MySQL Community Edition as an external system database or as a data source. If you select MySQL Community Edition, enter the name and location of the MySQL Connector/J jar file in the **Jar Path** field. Then, click **Next** to continue.

Note: For more information on the MySQL Connector/J driver, refer to the MySQL developer website at https://dev.mysql.com/.

13. Select the type of external database you want to use to store system information from the drop down box. Then, click **Next**.
    - Select **Oracle**, and continue at Step 14 on page 119.
    - Select **MySQLCommunity**, and continue at Step 15 on page 119.
    - Select **MSSQLServer**, and continue at Step 16 on page 119.
    - Select **PostgreSQL**, and continue at Step 17 on page 120.
14. Provide the Oracle connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Select the connection type. Do one of the following:
       - If you connect using the Oracle System Identifier (SID), select **Connect using SID**, then type the SID.
       - Select **Connect using Service Name**, then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name. The global database name typically comprises the database name and domain name.
    d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection url. Values should be entered as a semicolon-separated list of *parameter=value*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret;serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

    e) Click **Next**, and continue at Step 18 on page 120.
15. Provide connection information for the MySQL Community Edition database.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection url. Values should be entered as a ampersand-separated list of *parameter=value*.
    e) Click **Next**, and continue at Step 18 on page 120.
16. Provide the SQL Server connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Type the name of the schema.

e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.

f) Click **Next**, and continue at Step 18 on page 120.

17. Provide the PostgreSQL connection information.

a) Type the name of the host.

b) Type the port number.

c) Type the database name.

d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.

e) Click **Next**, and continue at Step 18 on page 120.

18. Provide the external database credential information.

Note: Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.

Note: If the installer is unable to validate, you are prompted to reenter credentials or skip validation. Skipping validation is often desired when performing a silent upgrade. See Silent upgrade process on page 134 for details.

- In the **Admin Username** field, type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- In the **Admin Password** field, type the password for an external database administrator account.
- In the **Username** field, type a user name. The standard user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- In the **Password** field, type the user password.

19. Review the Server Access Port. The Server Access Port must be opened for the load balancer. The default is 8080.
20. Take the appropriate action depending on whether you are using the On-Premises Connector.
    - If you are not using the On-Premises Connector, skip to the next step.
    - If you are using the On-Premises Connector, review the On-Premises Access Ports. The On-Premises Access Port and the TCP Notification Server Port must be opened for the load balancer.

Important: If you changed any values for On-Premises Access Ports during an upgrade, you will need to reconfigure the load balancer to use the new ports.

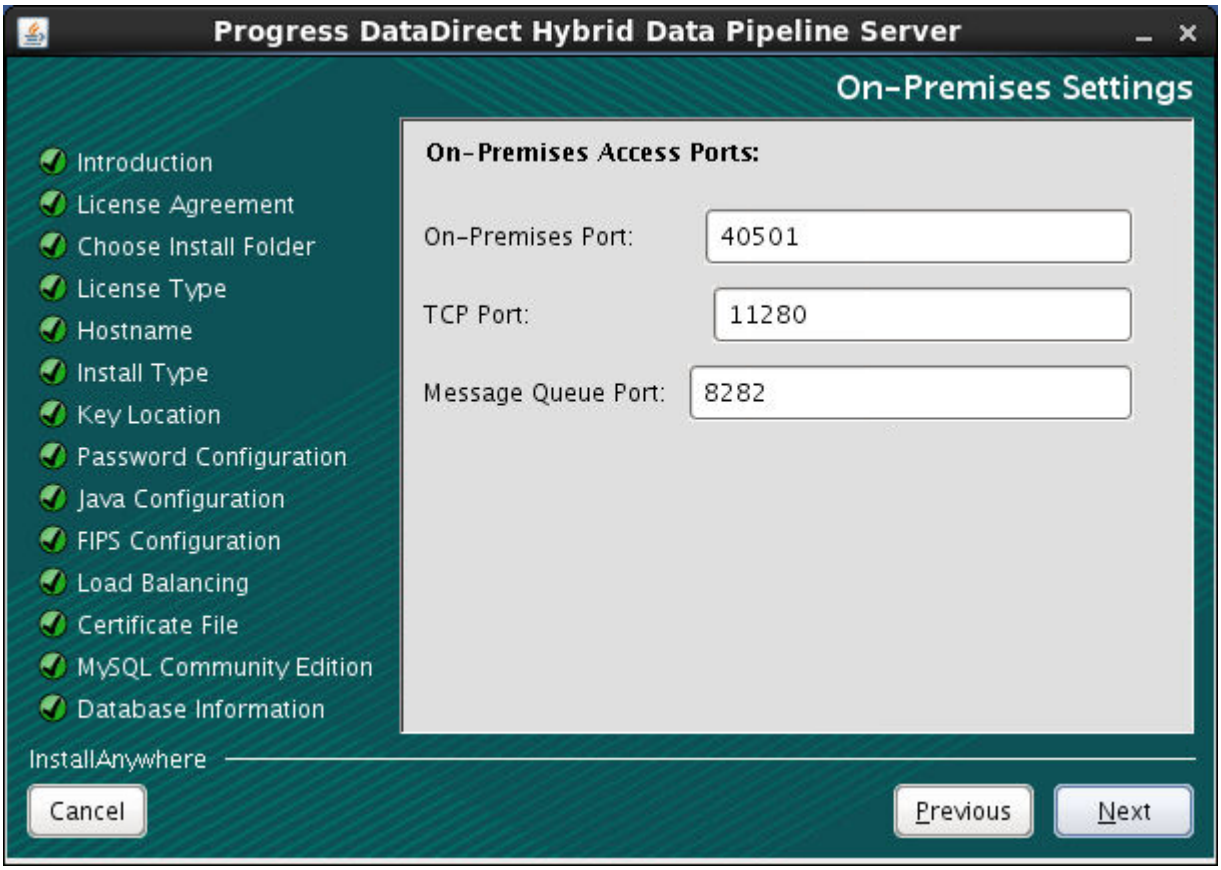


Table 25: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
Message Queue Port	8282	Port for the message queue

21. Review the Server Internal Ports. The Internal API Port and the Shutdown Port must be opened.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of any Hybrid Data Pipeline instance.

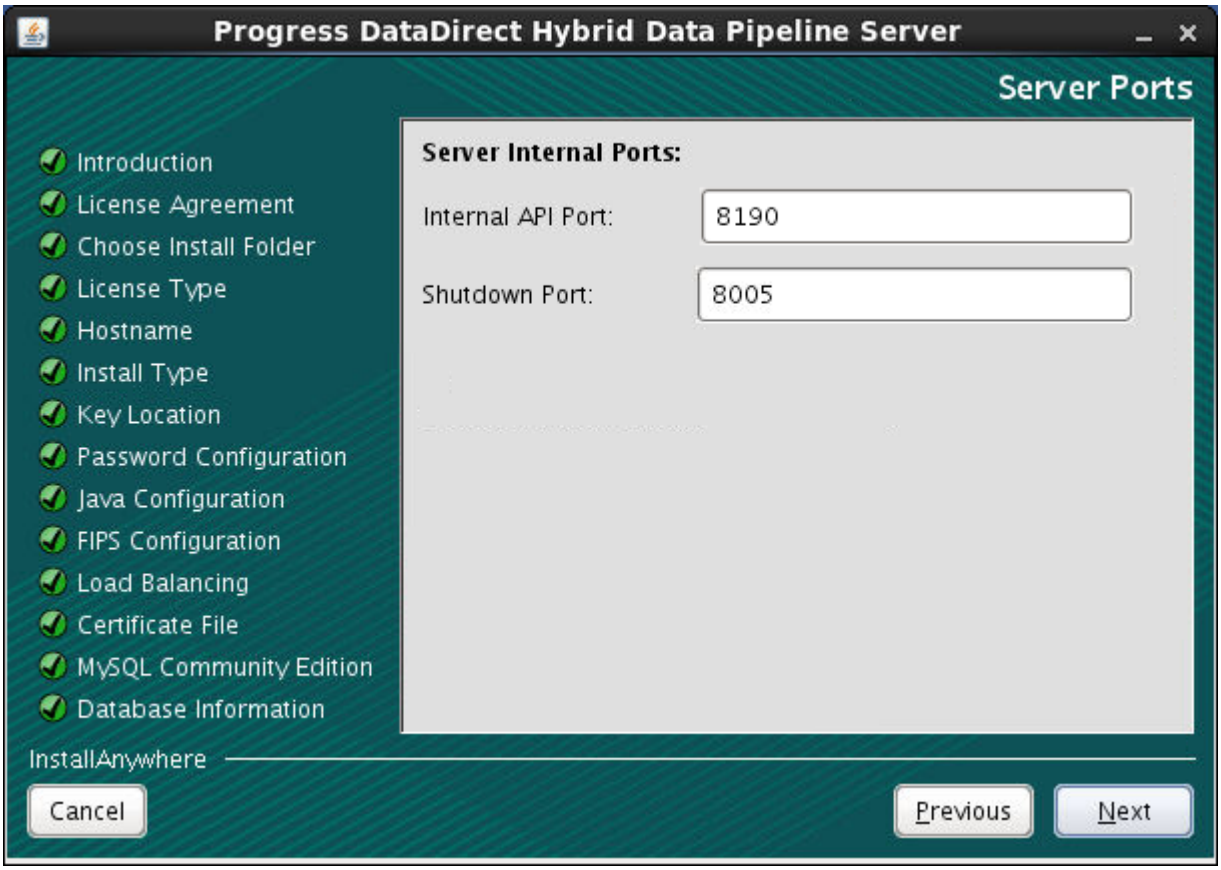


Table 26: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Shutdown Port	8005	Shutdown port

22. Review the installation summary. If you are satisfied with your choices, press **ENTER** to upgrade.
23. After the upgrade has finished, press **ENTER** to exit the installer.
24. Verify the upgrade by accessing the Hybrid Data Pipeline user interface from a browser. The login page should appear. For example:

    `https://<myserver>/`

    where `<myserver>` is the fully qualified hostname or IP address of the load balancer.

    After logging in, administrators can verify product version information by selecting **About** from the question mark drop-down menu. For more information on retrieving version information, refer to "Get Version Information" in the *Progress DataDirect Hybrid Data Pipeline User's Guide*.

Refer to installation log files for a record of any problems that may have occurred during the upgrade. See Server installation log files on page 166 for details.

What to do next

If you changed any values for On-Premises Access Ports during an upgrade, you will need to reconfigure the load balancer to use the new ports.

Standalone upgrade (console mode)

Note: The installer does not support changing a standalone deployment to a load balancer deployment during an upgrade, or vice versa. To make such a change, you would need to uninstall the server and then reinstall it. See Uninstalling Hybrid Data Pipeline server on page 166 and Installing the Hybrid Data Pipeline server on page 47 for details.

After copying the product installation file to a temporary directory, take the following steps to upgrade a standalone deployment with the installer in console mode.

1. From a command-line prompt, navigate to the directory where you saved the product file. Alternatively, place the product file directory on your path before proceeding to the next step.

   The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin`, where *nn* is the version of the product.

2. Make the file an executable using the `chmod` command. Then, press **ENTER**. For example:

   ```
   chmod +x ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

3. Run the executable by entering the product file path and pressing **ENTER**.

   a) Type the file name and path of the product file. For example:

   ```
   ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -i console
   ```

   b) Press **ENTER**.

   c) The **Introduction** step appears. Press **ENTER** to continue.

4. The License Agreement appears. Press **ENTER** multiple times to advance through the license agreement. Make sure that you read and understand the license agreement.

   - To accept the terms in the License Agreement and continue with the installation, type `Y`.
   - To end the installation, type `N` and press **ENTER**.

   Note: You can exit the installation program at any time by typing `Quit`.

5. You are prompted for the installation directory. Type the absolute path of the directory of the installation you want to upgrade. Then, press **ENTER**.
6. You are prompted to upgrade the existing installation or go back to enter a different installation directory. Type `1` to upgrade the existing installation. Then, press **ENTER**.
7. Choose whether you want to upgrade with an evaluation or licensed version of the product. Licensed installations require a valid License Key.

   - Evaluation. Type `1` to upgrade with an evaluation version of the product that is fully functional for 30 days. Then, press **ENTER**.
   - Licensed. Type `2` if you purchased a licensed version of the product. Then, press **ENTER**. Type the license key, including any dashes, and then press **ENTER**.

8. Accept or enter the fully qualified hostname for your Hybrid Data Pipeline server. By default, the installer suggests the name of the current machine. Then, press **ENTER**.

Note: If the installer is unable to validate the hostname, you are prompted to reenter the hostname or skip validation. Skipping validation is often desired when performing a silent upgrade. See Silent upgrade process on page 134 for details.

9. Select how you want to continue the upgrade.
   - Type `1` for an Express upgrade to persist previously established values. Then, press **ENTER** and continue at Step 27 on page 128.
   - Type `2` to change values for the following configurations. Then, press **ENTER** to continue.
     - Change the location of the SSL certificate file
     - Change the Java configuration to use an external JRE
     - Enable or disable FIPS
     - Add MySQL Community Edition as a data store or external system database
     - Change the system database you are using
     - Update external system database credentials
     - Change Server Access Ports
     - Change On-Premises Connector Ports
     - Change Server Internal Access Ports

Note: The key location where the generated key and internal files are stored cannot be modified when performing an upgrade.

10. Specify the desired Java configuration.

Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

- Type `1` if you will be using an external JRE (a JRE not installed with the server).
- Type `2` if you will be using the embedded JRE installed with the server.

11. Specify the fully qualified location of the Java home directory. This is the path to the external JRE. Press **ENTER**.
12. Specify whether you want to enable FIPS on the Hybrid Data Pipeline server.

Important: To enable FIPS, your hardware must support secure random, or you must have a secure random daemon installed.

Important: When you enable FIPS during an upgrade, the environment uses the encryption key for the system database that was generated during the original installation of the server. This encryption key, while generated with a FIPS compliant algorithm, was not generated with a FIPS certified implementation of the algorithm.

- Type `1` if you want to enable FIPS. Press **ENTER** and continue to the next step.

- Type 2 and press **ENTER** if you want to use the default setting which is FIPS disabled.

13. Depending on your environment, provide the appropriate SSL certificate information.

    - Type 1 to specify a PEM file to be used by the server to establish SSL connections with ODBC and JDBC client applications. Press **ENTER**. Type the full path to the PEM file. Press **ENTER** again, and proceed to the next step.

      Note: The PEM file must consist of a private key, a public key certificate issued by a certificate authority (CA), and additional certificates that make up the trust chain. See The PEM file on page 20 for more information.

    - Type 2 to use the SSL certificate specified in the previous installation or the self-signed certificate included with the previous installation. Then, press **ENTER**, and proceed to the next step.

      Note: The self-signed certificate may be used in a test environment. However, for production, a PEM file with required information should be specified. See The PEM file on page 20 for more information.

14. Choose the appropriate option depending on whether you are using MySQL Community Edition. MySQL Community Edition can be used as an external system database or as a data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. However, you can use the MySQL Connector/J driver to use MySQL Community Edition as an external system database or as a data source.

    - Type 1 and press **ENTER**, if you are using MySQL Community Edition. Type the name and location of the MySQL Connector/J jar file, and press **ENTER** again.
    - Type 2 and press **ENTER**, if you are not using MySQL Community Edition in your environment.

    Note: For more information on the MySQL Connector/J driver, visit the MySQL developer website at https://dev.mysql.com/.

    ---

15. Select the type of database you want to use to store system information.

    - Type 1 to store information on an internal database supplied by this installation. Continue at Step 17 on page 125.
    - Type 2 to store information on an external database. Proceed to the next step.

    Note: Users and data sources created in the internal database are specific to the internal database. They are not migrated to the external database if you subsequently modify the Hybrid Data Pipeline server to use an external database.

    ---

16. Select the type of external system database you want to use to store system information.

    - Select **Oracle**, and continue at Step 18 on page 125.
    - Select **MySQLCommunity**, and continue at Step 19 on page 126.
    - Select **MSSQLServer**, and continue at Step 20 on page 126.
    - Select **PostgreSQL**, and continue at Step 21 on page 126.

17. Enter the database port for the internal database. If your environment has already defined a function for the default port, the installer pops up a message so that you can specify a different port. Press **ENTER**, and continue at Step 23 on page 127.
18. Provide the Oracle connection information.

a) Type the name of the host.

b) Type the port number.

c) Select the connection type. Do one of the following:

- If you connect using the Oracle System Identifier (SID), type `1`, then type the SID.
- If you connect using the Service Name, type `2`, then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name—a name that typically comprises the database name and domain name.

d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as a semicolon-separated list of *`parameter=value`*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret;serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

e) Click **ENTER**, and continue at Step 22 on page 127.

19. Provide connection information for the MySQL Community Edition external database.

a) Type the name of the Hostname.

b) Type the port number.

c) Type the database name.

d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as a ampersand-separated list of *`parameter=value`*.

e) Click **ENTER**, and continue at Step 22 on page 127.

20. Provide the SQL Server connection information.

a) Type the name of the host.

b) Type the port number.

c) Type the database name.

d) Type the name of the schema.

e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *`parameter=value`*.

f) Click **ENTER**, and continue at Step 22 on page 127.

21. Provide the PostgreSQL connection information.

a) Type the name of the host.

b) Type the port number.

c) Type the database name.

d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of `parameter=value`.

e) Click **ENTER**, and continue at Step 22 on page 127.

22. You are prompted to provide the database credential information for a user with administrator privileges and for a user without administrator privileges.

Note: Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.

Note: If the installer is unable to validate, you are prompted to reenter credentials or skip validation. Skipping validation is often desired when performing a silent upgrade. See Silent upgrade process on page 134 for details.

- Type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- You are prompted to provide the Admin Password. Type the password for an external database administrator account.
- You are prompted to provide the username for a user who does *not* have administrator privileges. Type a user name. The standard user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- You are prompted to provide the User Password. Type the user password.
- The installer validates the connection. Press **ENTER** to continue.

23. Review the Server Access Ports. A Server Access Port must be available to the end user across the firewall. Best security practices recommend using an HTTPS port.

Table 27: Server Access Ports

Name	Default	Description
HTTP Port	8080	Port that exposes Hybrid Data Pipeline
HTTPS Port	8443	Port that exposes Hybrid Data Pipeline

24. Select whether you will continue to use the On-Premises Connector.

- If using the On-Premises Connector, type `1` and press **ENTER**. Then continue to the next step.
- If not using the On-Premises Connector, type `2` and press **ENTER**. Continue at Step 26 on page 128.

25. Review the On-Premises Access Ports. The On-Premises Access Port and a Notification Server Port must be available across the firewall. Best security practices recommend using the SSL Notification Server Port.

Important: If you change any values for On-Premises Access Ports during an upgrade, you will need to reinstall the On-Premises Connector with the updated distribution files in the `redist` subdirectory. See What to do next.

Table 28: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
SSL Port	11443	SSL port for the Notification Server
Message Queue Port	8282	Port for the message queue

26. Review the Server Internal Ports. A port for the internal API and the Shutdown Port must be opened. Best security practices recommend using the Internal API SSL Port.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of the Hybrid Data Pipeline instance.

Table 29: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Internal API SSL Port	8090	SSL port for the Internal API
Shutdown Port	8005	Shutdown port

27. Review the summary. If you are satisfied with your choices, press **ENTER** to upgrade.
28. After the upgrade has finished, press **ENTER** to exit the installer.
29. Verify the installation by accessing the Hybrid Data Pipeline user interface from a browser. The login page should appear. For example:

    `https://<myserver>:8443/`

    where `<myserver>` is the fully qualified hostname of the machine where you installed Hybrid Data Pipeline.

    After logging in, administrators can verify product version information by selecting **About** from the question mark drop-down menu. For more information on retrieving version information, refer to "Get Version Information" in the *Progress DataDirect Hybrid Data Pipeline User's Guide*.

Refer to installation log files for a record of any problems that may have occurred during the upgrade. See Server installation log files on page 166 for details.

What to do next

If you change any of the On-Premises Connector Ports, you will need to reinstall the On-Premises Connector with updated configuration and certificate files. These files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. These files must be copied to the directory of the On-Premises Connector installer before proceeding with the reinstallation of the On-Premises Connector.

The four configuration and certificate files are:

- `config.properties`
- `OnPremise.properties`

- `ddcloud.pem`
- `ddcloudTrustStore.jks`

See Installing the Hybrid Data Pipeline On-Premises Connector on page 191 for further details.

Load balancer upgrade (console mode)

Note: The installer does not support changing a standalone deployment to a load balancer deployment during an upgrade, or vice versa. To make such a change, you would need to uninstall the server and then reinstall it. See Uninstalling Hybrid Data Pipeline server on page 166 and Installing the Hybrid Data Pipeline server on page 47 for details.

After copying the product installation file to a temporary directory, take the following steps to upgrade a load balancer deployment with the installer in console mode.

1. From a command-line prompt, navigate to the directory where you saved the product file. Alternatively, place the product file directory on your path before proceeding to the next step.

   The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_`*`nn`*`_LINUX_64_INSTALL.bin`, where *`nn`* is the version of the product.

2. Make the file an executable using the `chmod` command. Then, press **ENTER**. For example:

   ```
   chmod +x ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

3. Run the executable by entering the product file path and pressing **ENTER**.

   a) Type the file name and path of the product file. For example:

   ```
   ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -i console
   ```

   b) Press **ENTER**.

   c) The **Introduction** step appears. Press **ENTER** to continue.

4. The License Agreement appears. Press **ENTER** multiple times to advance through the license agreement. Make sure that you read and understand the license agreement.

   - To accept the terms in the License Agreement and continue with the installation, type `Y`.
   - To end the installation, type `N` and press **ENTER**.

   Note: You can exit the installation program at any time by typing `Quit`.

5. You are prompted for the installation directory. Type the absolute path to the installation directory of the installation you want to upgrade. Then, press **ENTER**.
6. You are prompted to upgrade the existing installation or go back to enter a different installation directory. Type `1` to upgrade the existing installation. Then, press **ENTER**.
7. Choose whether you want to upgrade with an evaluation or licensed version of the product. Licensed installations require a valid License Key.

   - Evaluation. Type `1` to upgrade with an evaluation version of the product that is fully functional for 30 days. Then, press **ENTER**.

- Licensed. Type `2` if you purchased a licensed version of the product. Then, press **ENTER**. Type the license key, including any dashes, and then press **ENTER**.

8. Accept the fully qualified hostname for your Hybrid Data Pipeline Server. By default, the installer suggests the name of the current machine. Then, press **ENTER**.

Note: If the installer is unable to validate the hostname, you are prompted to reenter the hostname or skip validation. Skipping validation is often desired when performing a silent upgrade. See Silent upgrade process on page 134 for details.

---

9. Select how you want to continue the upgrade.

- Type `1` for an Express upgrade to persist previously established values. Then, press **ENTER** and continue at Step 24 on page 134.
- Type `2` to change values for the following configurations. Then, press **ENTER** to continue.
  - Change the location of the SSL certificate file
  - Change the Java configuration to use an external JRE
  - Enable or disable FIPS
  - Add MySQL Community Edition as a data store or external system database
  - Change the system database you are using
  - Update external system database credentials
  - Change Server Access Ports
  - Change On-Premises Connector Ports
  - Change Server Internal Access Ports

Note: The following elements of an installation cannot be modified when performing an upgrade of a load balancer installation: key location, load balancer hostname, and On-Premises Connector enablement.

---

10. Specify the desired Java configuration.

Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

- Type `1` if you will be using an external JRE (a JRE not installed with the server).
- Type `2` if you will be using the embedded JRE installed with the server.

11. Specify the fully qualified location of the Java home directory. This is the path to the external JRE. Press **ENTER**.
12. Specify whether you want to enable FIPS on the Hybrid Data Pipeline server.

Important: To enable FIPS, your hardware must support secure random, or you must have a secure random daemon installed.

Important: When you enable FIPS during an upgrade, the environment uses the encryption key for the system database that was generated during the original installation of the server. This encryption key, while generated with a FIPS compliant algorithm, was not generated with a FIPS certified implementation of the algorithm.

- Type `1` if you want to enable FIPS. Press **ENTER** and continue to the next step.
- Type `2` and press **ENTER** if you want to use the default setting which is FIPS disabled.

13. Depending on your environment, provide the appropriate SSL certificate information.
    - Type `1` to specify the SSL certificate file to be used with the Hybrid Data Pipeline server. The specified file must be the root certificate used to sign the certificate for the load balancer server. PEM, DER, and Base64 encodings are supported. Type the full path to the SSL certificate file. Then, press **ENTER**.
    - Type `2` to use the SSL certificate file that was specified during the previous installation or bypass the specification of an SSL certificate. Then, press **ENTER**.
14. Choose the appropriate option depending on whether you are using MySQL Community Edition. MySQL Community Edition can be used as an external system database or as a data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. However, you can use the MySQL Connector/J driver to use MySQL Community Edition as an external system database or as a data source.
    - Type `1` and press **ENTER**, if you are using MySQL Community Edition. Type the name and location of the MySQL Connector/J jar file, and press **ENTER** again.
    - Type `2` and press **ENTER**, if you are not using MySQL Community Edition in your environment.

    Note: For more information on the MySQL Connector/J driver, visit the MySQL developer website at https://dev.mysql.com/.
15. Select the type of external database you want to use to store system information.
    - Select **Oracle**, and continue at Step 16 on page 131.
    - Select **MySQLCommunity**, continue at Step 17 on page 132.
    - Select **MSSQLServer**, and continue at Step 18 on page 132.
    - Select **PostgreSQL**, and continue at Step 19 on page 132.
16. Provide the Oracle connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Select the connection type. Do one of the following:
        - If you connect using the Oracle System Identifier (SID), type `1`, then type the SID.
        - If you connect using the Service Name, type `2`, then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name—a name that typically comprises the database name and domain name.

d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as a semicolon-separated list of *parameter=value*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret;serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

e) Press **ENTER**, and continue at Step 20 on page 132.

17. Provide connection information for the MySQL Community Edition external database.
    a) Type the name of the Hostname.
    b) Type the port number.
    c) Type the database name.
    d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as a ampersand-separated list of *parameter=value*.
    e) Press **ENTER**, and continue at Step 20 on page 132.
18. Provide the SQL Server connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Type the name of the schema.
    e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
    f) Press **ENTER**, and continue at Step 20 on page 132.
19. Provide PostgreSQL connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
    e) Press **ENTER**, and continue at Step 20 on page 132.
20. You are prompted to provide the database credential information for a user with administrator privileges and for a user without administrator privileges.

Note: Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.

Note: If the installer is unable to validate, you are prompted to reenter credentials or skip validation. Skipping validation is often desired when performing a silent upgrade. See Silent upgrade process on page 134 for details.

- Type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- You are prompted to provide the Admin Password. Type the password for an external database administrator account.
- You are prompted to provide the username for a user who does *not* have administrator privileges. Type a user name. The standard user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- You are prompted to provide the User Password. Type the user password.
- The installer validates the connection. Press **ENTER** to continue.

21. Review the Server Access Port. The Server Access Port must be opened for the load balancer. The default is 8080.
22. Take the appropriate action depending on whether you are using the On-Premises Connector.
    - If you are not using the On-Premises Connector, skip to the next step.
    - If you are using the On-Premises Connector, review the On-Premises Access Ports. The On-Premises Access Port and the TCP Notification Server Port must be opened for the load balancer.

Important: If you changed any values for On-Premises Access Ports during an upgrade, you will need to reconfigure the load balancer to use the new ports.

Table 30: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
Message Queue Port	8282	Port for the message queue

23. Review the Server Internal Ports. The Internal API Port and the Shutdown Port must be opened.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of any Hybrid Data Pipeline instance.

Table 31: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Shutdown Port	8005	Shutdown port

24. Review the summary. If you are satisfied with your choices, press **ENTER** to upgrade.
25. After the upgrade has finished, press **ENTER** to exit the installer.
26. Verify the installation by accessing the Hybrid Data Pipeline user interface from a browser. The login page should appear. For example:

    `https://<myserver>/`

    where `<myserver>` is the name or IP address of the server hosting your load balancer device.

    After logging in, administrators can verify product version information by selecting **About** from the question mark drop-down menu. For more information on retrieving version information, refer to "Get Version Information" in the *Progress DataDirect Hybrid Data Pipeline User's Guide*.

Refer to installation log files for a record of any problems that may have occurred during the upgrade. See Server installation log files on page 166 for details.

What to do next

If you changed any values for On-Premises Access Ports during an upgrade, you will need to reconfigure the load balancer to use the new ports.

Silent upgrade process

A silent upgrade may be preferred when automating the upgrade of one or more Hybrid Data Pipeline servers. The silent upgrade process hinges on the creation of a response file. The response file is a text file that you create (for example, `pipeline.response`) with the product installer. You begin by generating a response file, you then tailor the response file to your environment, and you then perform the upgrade installation.

If you are using the silent installation process to upgrade cluster nodes, the response file generated during the initial upgrade must be modified to upgrade the server on any additional nodes. For a GUI generated response file, you will need to designate the name of an additional node with the `D2C_HOSTNAME` option. For a console generated response file, you will need to designate the name of an additional node with the `D2C_HOSTNAME_CONSOLE` option.

A silent upgrade requires performing the following steps:

1. You must create a response file using the installer as described in any of the following topics.
   - Creating a response file for a standalone upgrade (GUI mode) on page 135
   - Creating a response file for a load balancer upgrade (GUI mode) on page 142
   - Creating a response file for a standalone upgrade (console mode) on page 151
   - Creating a response file for a load balancer upgrade (console mode) on page 156
2. You must edit the response file to suit your environment. Response files differ depending on whether you generate them using the installer in GUI mode or console mode. Editing the response file is described in the following topics:
   - Editing a GUI generated upgrade response file on page 148
   - Editing a console generated upgrade response file on page 162
3. You must perform the silent upgrade using the response file as described in Performing a silent upgrade on page 164.

Creating a response file for a standalone upgrade (GUI mode)

Note: The installer does not support changing a standalone deployment to a load balancer deployment during an upgrade, or vice versa. To make such a change, you would need to uninstall the server and then reinstall it. See Uninstalling Hybrid Data Pipeline server on page 166 and Installing the Hybrid Data Pipeline server on page 47 for details.

After copying the product installation file to a temporary directory, take the following steps to generate a response file for a standalone upgrade using the GUI installer.

1. From a command-line prompt, navigate to the directory where you saved the product file. Alternatively, place the product file directory on your path before proceeding to the next step.

   The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin`, where *nn* is the version of the product.

2. Make the file an executable using the `chmod` command. Then, press **ENTER**. For example:

   ```
   chmod +x ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

3. At a command-line prompt, type the following command where *response_file* is the path and file name of the response file you want to create. You must specify an absolute path.

   ```
   PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -r response_file
   ```

   The following example creates a response file named `pipeline.response` in the `/home/users/johndoe` directory.

   ```
   PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -r
   /home/users/johndoe/pipeline.response
   ```

4. The License Agreement window appears. Make sure that you read and understand the license agreement. To continue with the installation, select the **I accept the terms in the License Agreement** option; then, click **Next**.

   Note: You can exit the installation program at any time by clicking Cancel or return to the previous window by clicking **Previous**.

5. Choose the destination directory for the installation. Click **Next** to accept the default installation directory, or select **Choose...** to browse to a different directory, then click **Next**.
6. Choose whether you want to upgrade with an evaluation or licensed version of the product. Licensed installations require a valid License Key.

   - Evaluation. Select this option to upgrade with an evaluation version that is fully functional for 30 days. Then, click **Next**.
   - Licensed. Select this option if you purchased a licensed version of the product. Type the license key, including any dashes, and then click **Next**.

7. Accept or enter the fully qualified hostname of the machine that will host the Hybrid Data Pipeline server. By default, the installer suggests the name of the current machine.

   Note the following important information. Then, click **Next** to continue.

   - If you enter a hostname different than the hostname of the current machine, the installer will fail to validate the hostname. You are then prompted to reenter the hostname or skip validation. If you are planning on using the response file to install the product on a different machine, you should opt to skip validation.

- Before using the response file to install the product on another machine, the response file must have the `SKIP_HOSTNAME_VALIDATION` and `SKIP_PORT_VALIDATION` properties set to `true`. For example:

```
SKIP_HOSTNAME_VALIDATION=true
SKIP_PORT_VALIDATION=true
```

- Running an installation in silent mode with a response file containing these settings allows the silent installation to continue even if hostname or port validation fail. When the validation fails during the silent installation process, the installer generates the file `SilentInstallInfo.log` in the user's home directory but completes a full installation.

8. Select how you want to continue the upgrade.
   - Select **Express** to persist previously established values. Then, click **Next** and continue at Step 23 on page 142.
   - Select **Modify settings** to change values for the following configurations. Then, click **Next**.
     - Change the location of the SSL certificate file
     - Change the Java configuration to use an external JRE
     - Enable or disable FIPS
     - Add MySQL Community Edition as a data store or external system database
     - Change the system database you are using
     - Update external system database credentials
     - Change Server Access Ports
     - Change On-Premises Connector Ports
     - Change Server Internal Access Ports

Note: The key location where the generated key and internal files are stored cannot be modified when performing an upgrade.

9. Select the desired Java configuration.

Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

- Select **Use default Java** if you will be using the embedded JRE installed with the server.
- Select **Java home directory** and provide the path to an external JRE if you will be using a JRE not installed with the server.

10. Select whether you want to enable FIPS on the Hybrid Data Pipeline server.

Important: To enable FIPS, your hardware must support secure random, or you must have a secure random daemon installed.

Important: When you enable FIPS during an upgrade, the environment uses the encryption key for the system database that was generated during the original installation of the server. This encryption key, while generated with a FIPS compliant algorithm, was not generated with a FIPS certified implementation of the algorithm.

11. Depending on your environment, provide the appropriate SSL certificate information.
    - Select **Certificate file** to specify a PEM file to be used by the server to establish SSL connections with ODBC and JDBC client applications. Type the full path to the PEM file, or click **Choose...** to browse to the location of the PEM file. Then, click **Next**.

      Note: The PEM file must consist of a private key, a public key certificate issued by a certificate authority (CA), and additional certificates that make up the trust chain. See The PEM file on page 20 for more information.
    - Select **Use existing Certificate** to use the SSL certificate specified in the previous installation or the self-signed certificate included with the installation. Then, click **Next**.

      Note: The self-signed certificate may be used in a test environment. However, for production, a PEM file with required information should be specified. See The PEM file on page 20 for more information.
12. Select whether you want to use MySQL Community Edition as a data source or external database. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition; however, it does support the MySQL Connector/J driver. If you choose **Yes**, in the **Jar Path** field, provide the name and location of the driver's jar file. Click **Next** to continue.

    Note: For more information on the MySQL Connector/J driver, refer to the MySQL developer website at https://dev.mysql.com/.

13. Select the type of database you want to use to store system information.
    - Select **Internal Database (supplied by this install)** to use the default internal database. Click **Next** to continue. Continue at Step 21 on page 140
    - Select **External Database** to store the system information in an external database. Then, from the drop down box, choose your database vender. Then, click **Next**.
      - Select **Oracle**, and continue at Step 14 on page 137.
      - Select **MySQLCommunity**, and continue at Step 15 on page 138.
      - Select **MSSQLServer**, and continue at Step 16 on page 138.
      - Select **PostgreSQL**, and continue at Step 17 on page 138.

    Note: Users and data sources created in the internal database are specific to the internal database. They are not migrated to the external database if you subsequently modify the Hybrid Data Pipeline Server to use an external database.

14. Provide the Oracle connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Select the connection type. Do one of the following:

- If you connect using the Oracle System Identifier (SID), select **Connect using SID**, then type the SID.
- Select **Connect using Service Name**, then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name. The global database name typically comprises the database name and domain name.

d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection url. Values should be entered as a semicolon-separated list of *parameter=value*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret; serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

e) Click **Next**, and continue at Step 18 on page 138.

15. Provide connection information for the MySQL Community Edition external database.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection url. Values should be entered as an ampersand-separated list of *parameter=value*.
    e) Click **Next**, and continue at Step 18 on page 138.
16. Provide the SQL Server connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Type the name of the schema.
    e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
    f) Click **Next**, and continue at Step 18 on page 138.
17. Provide the PostgreSQL connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
    e) Click **Next**, and continue at Step 18 on page 138.
18. Provide the external database credential information.

- In the **Admin Username** field, type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- In the **Admin Password** field, type the password for an external database administrator account.
- In the **Username** field, type a user name. For a list of required privileges, see External system databases on page 15.
- In the **Password** field, type the user password.

Important:

- Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.
- Passwords for an external database implementation are not persisted. These values must be specified in the response file with the `D2C_DB_ADMIN_PASSWORD` and `D2C_DB_USER_PASSWORD` options before running a silent install.
- The installer attempts to validate the database. If the installer is unable to validate, you are prompted to reenter credentials or skip validation. If you skip validation, the response file must have the `SKIP_DATABASE_VALIDATION` property set to `true`. During a silent upgrade, the installer will complete the upgrade even when the database validation fails.

19. Review the Server Access Ports. A Server Access Port must be available to the end user across the firewall. Best security practices recommend using an HTTPS port.

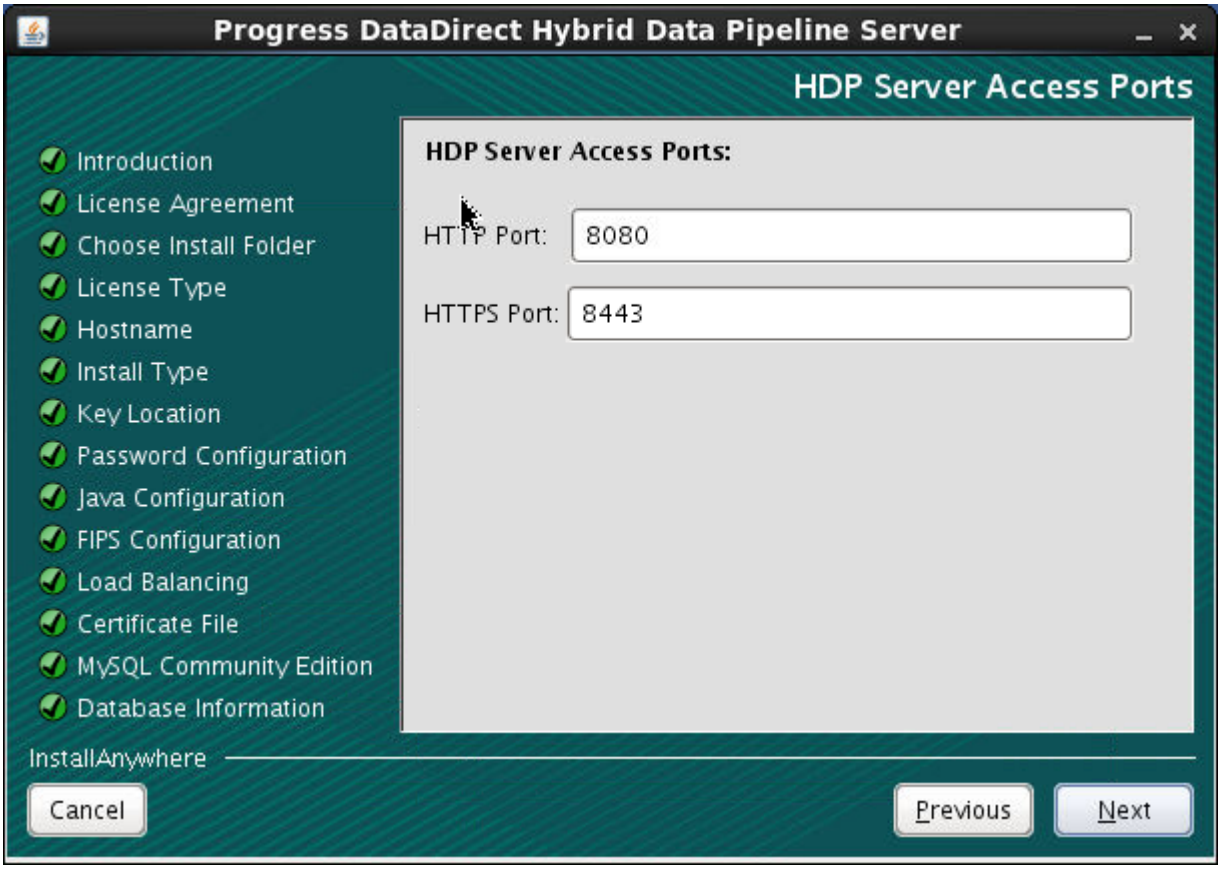


Table 32: Server Access Ports

Name	Default	Description
HTTP Port	8080	Port that exposes Hybrid Data Pipeline
HTTPS Port	8443	SSL port that exposes Hybrid Data Pipeline

20. Select whether you are using the On-Premises Connector.
    - If using the On-Premises Connector, select **Enable On-Premises Connector**. Click **Next** and continue to the next step.
    - If not using the On-Premises Connector, leave the check box empty and click **Next**. Continue at Step 22 on page 141.

21. Review the On-Premises Access Ports. The On-Premises Access Port and a Notification Server Port must be available across the firewall. Best security practices recommend using the SSL Notification Server Port.

Important: If you change any values for On-Premises Access Ports during an upgrade, you will need to reinstall the On-Premises Connector with the updated distribution files in the `redist` subdirectory. See "What to do next" in Performing a silent upgrade on page 164.

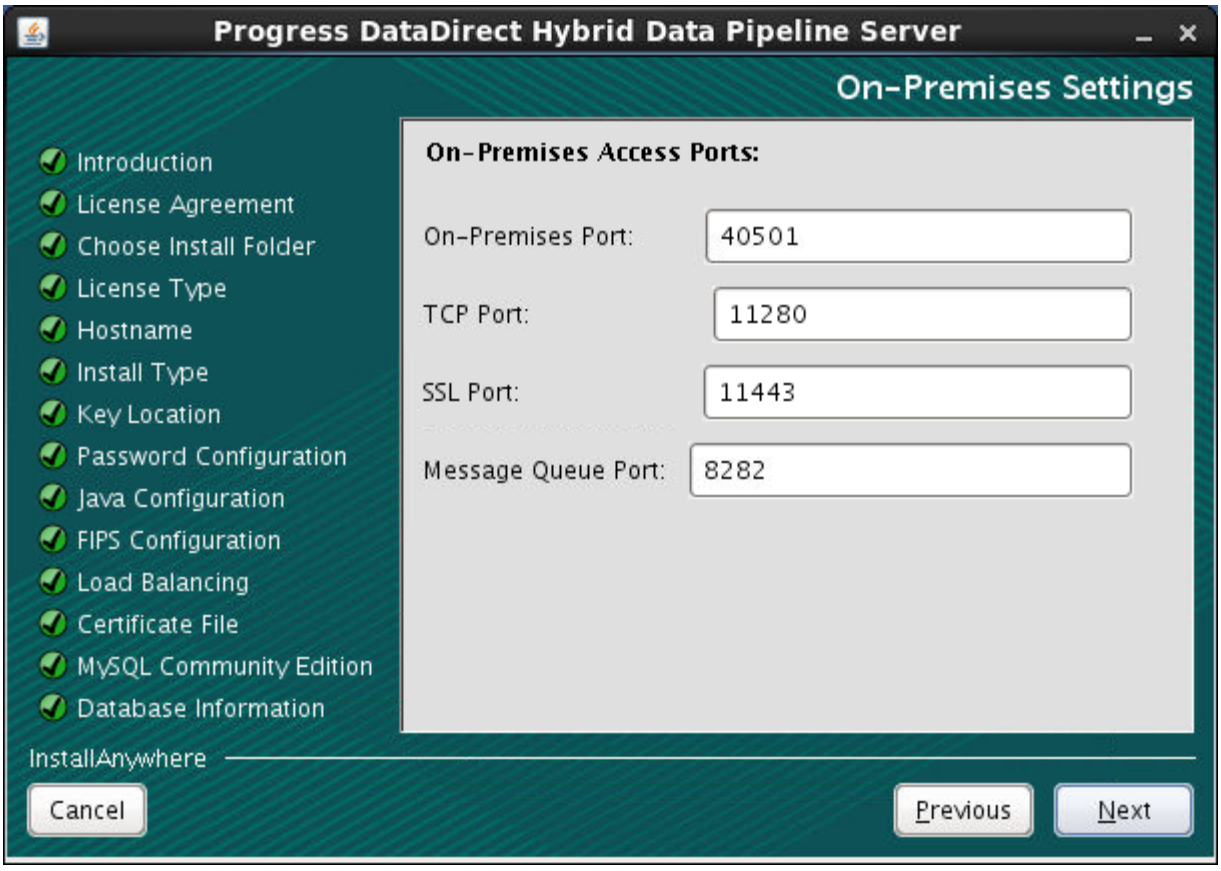


Table 33: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
SSL Port	11443	SSL port for the Notification Server
Message Queue Port	8282	Port for the message queue

22. Review the Server Internal Ports. A port for the internal API and the Shutdown Port must be opened. Best security practices recommend using the Internal API SSL Port.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of the Hybrid Data Pipeline instance.

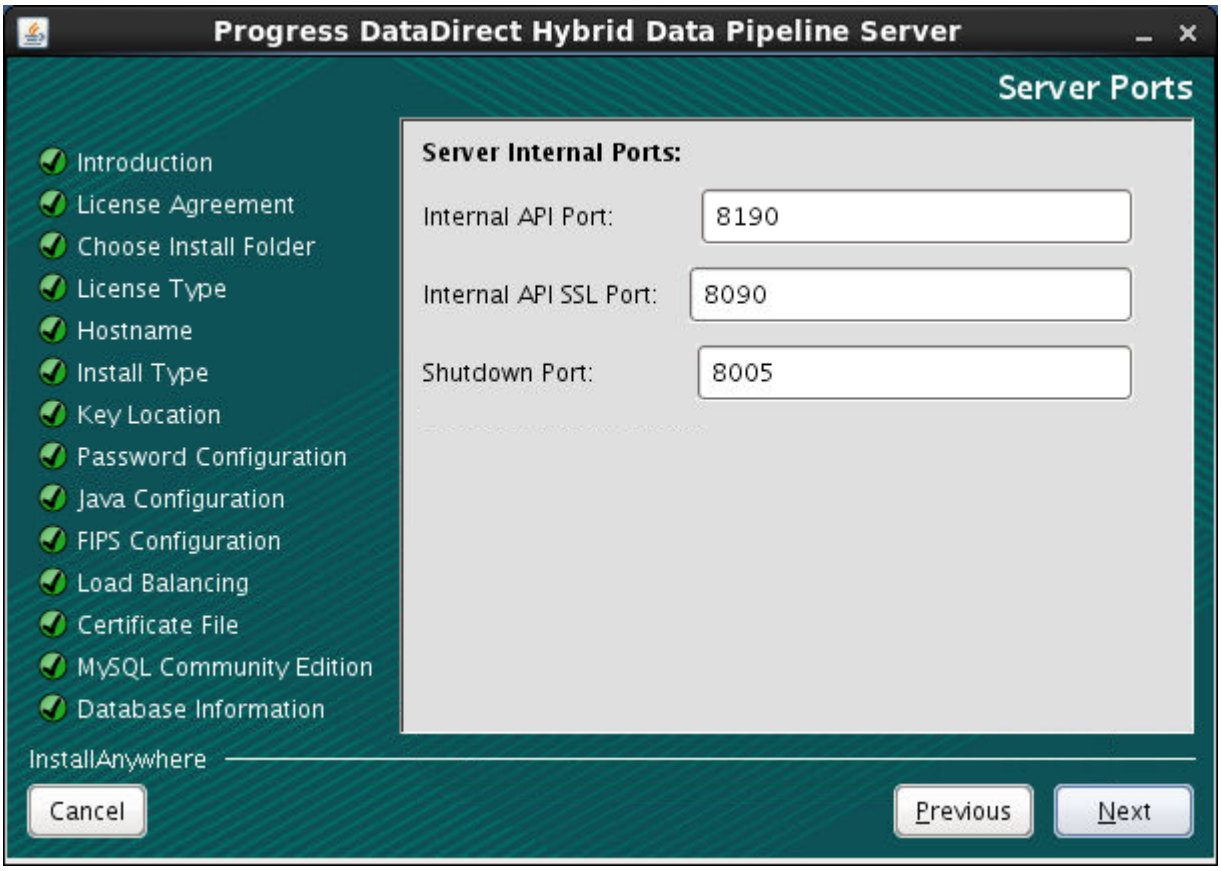


Table 34: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API

Name	Default	Description
Internal API SSL Port	8090	SSL port for the Internal API
Shutdown Port	8005	Shutdown port

23. Review the upgrade summary. If you are satisfied with your choices, press **ENTER** to generate the response file.
24. After the response file has been generated, press **ENTER** to exit the installer.
25. Confirm that a response file has been generated by navigating to the response file directory you specified in Step 3 on page 135 and opening the response file.
26. Proceed to Editing a GUI generated upgrade response file on page 148.

Creating a response file for a load balancer upgrade (GUI mode)

Note: The installer does not support changing a standalone deployment to a load balancer deployment during an upgrade, or vice versa. To make such a change, you would need to uninstall the server and then reinstall it. See Uninstalling Hybrid Data Pipeline server on page 166 and Installing the Hybrid Data Pipeline server on page 47 for details.

After copying the product installation file to a temporary directory, take the following steps to generate a response file for a load balancer upgrade using the GUI installer.

1. From a command-line prompt, navigate to the directory where you saved the product file. Alternatively, place the product file directory on your path before proceeding to the next step.

   The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin`, where *nn* is the version of the product.

2. Make the file an executable using the `chmod` command. Then, press **ENTER**. For example:

   ```
   chmod +x ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

3. At a command-line prompt, type the following command where *response_file* is the path and file name of the response file you want to create. You must specify an absolute path.

   ```
   PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -r response_file
   ```

   The following example creates a response file named `pipeline.response` in the `/home/users/johndoe` directory.

   ```
   PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -r
   /home/users/johndoe/pipeline.response
   ```

4. The License Agreement window appears. Make sure that you read and understand the license agreement. To continue with the installation, select the **I accept the terms in the License Agreement** option; then, click **Next**.

   Note: You can exit the installation program at any time by clicking Cancel or return to the previous window by clicking **Previous**.

5. Choose the destination directory for the installation. Click **Next** to accept the default installation directory, or select **Choose...** to browse to a different directory, then click **Next**.

6. Choose whether you want to upgrade with an evaluation or licensed version of the product. Licensed installations require a valid License Key.
   - Evaluation. Select this option to upgrade with an evaluation version that is fully functional for 30 days. Then, click **Next**.
   - Licensed. Select this option if you purchased a licensed version of the product. Type the license key, including any dashes, and then click **Next**.
7. Accept or enter the fully qualified hostname of the machine that will host the Hybrid Data Pipeline server. By default, the installer suggests the name of the current machine.

   Note the following important information. Then, click **Next** to continue.
   - If you enter a hostname different than the hostname of the current machine, the installer will fail to validate the hostname. You are then prompted to reenter the hostname or skip validation. If you are planning on using the response file to install the product on a different machine, you should opt to skip validation.
   - Before using the response file to install the product on another machine, the response file must have the `SKIP_HOSTNAME_VALIDATION` and `SKIP_PORT_VALIDATION` properties set to `true`. For example:

     ```
     SKIP_HOSTNAME_VALIDATION=true
     SKIP_PORT_VALIDATION=true
     ```

   - Running an installation in silent mode with a response file containing these settings allows the silent installation to continue even if hostname or port validation fail. When the validation fails during the silent installation process, the installer generates the file `SilentInstallInfo.log` in the user's home directory but completes a full installation.
8. Select how you want to continue the upgrade.
   - Select **Express** to persist previously established values. Then, click **Next** and continue at Step 22 on page 148.
   - Select **Modify settings** to change values for the following configurations. Then, click **Next**.
     - Change the location of the SSL certificate file
     - Change the Java configuration to use an external JRE
     - Enable or disable FIPS
     - Add MySQL Community Edition as a data store or external system database
     - Change the system database you are using
     - Update external system database credentials
     - Change Server Access Ports
     - Change On-Premises Connector Ports
     - Change Server Internal Access Ports

   Note: The following elements of an installation cannot be modified when performing an upgrade of a load balancer installation: key location, load balancer hostname, and On-Premises Connector enablement.
9. Select the desired Java configuration.

Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

- Select **Use default Java** if you will be using the embedded JRE installed with the server.
- Select **Java home directory** and provide the path to an external JRE if you will be using a JRE not installed with the server.

10. Select whether you want to enable FIPS on the Hybrid Data Pipeline server.

Important: To enable FIPS, your hardware must support secure random, or you must have a secure random daemon installed.

Important: When you enable FIPS during an upgrade, the environment uses the encryption key for the system database that was generated during the original installation of the server. This encryption key, while generated with a FIPS compliant algorithm, was not generated with a FIPS certified implementation of the algorithm.

11. Depending on your environment, provide the appropriate SSL certificate information.
    - Select **Certificate file** to specify the SSL certificate file to be used with the Hybrid Data Pipeline server. The specified file must be the root certificate used to sign the certificate for the load balancer server. PEM, DER, and Base64 encodings are supported. Type the full path to the certificate file, or click **Choose...** to browse to the location of the SSL certificate file. Then, click **Next**.
    - Select **Use existing Certificate** to use the SSL certificate specified in the previous installation or bypass the specification of an SSL certificate. Then, click **Next**.
12. Select MySQL Community Edition if you plan to use MySQL Community Edition as an external system database or as a data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. However, you can use the MySQL Connector/J driver to use MySQL Community Edition as an external system database or as a data source. If you select MySQL Community Edition, enter the name and location of the MySQL Connector/J jar file in the **Jar Path** field. Then, click **Next** to continue.

Note: For more information on the MySQL Connector/J driver, refer to the MySQL developer website at https://dev.mysql.com/.

13. Select the type of external database you want to use to store system information from the drop down box. Then, click **Next**.
    - Select **Oracle**, and continue at Step 14 on page 144.
    - Select **MySQLCommunity**, and continue at Step 15 on page 145.
    - Select **MSSQLServer**, and continue at Step 16 on page 145.
    - Select **PostgreSQL**, and continue at Step 17 on page 145.
14. Provide the Oracle connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Select the connection type. Do one of the following:

- If you connect using the Oracle System Identifier (SID), select **Connect using SID**, then type the SID.
- Select **Connect using Service Name**, then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name. The global database name typically comprises the database name and domain name.

d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection url. Values should be entered as a semicolon-separated list of *parameter=value*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret;serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

e) Click **Next**, continue at Step 18 on page 145.

15. Provide connection information for the MySQL Community Edition external database.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included the connection url. Values should be entered as an ampersand-separated list of *parameter=value*.
    e) Click **Next**, continue at Step 18 on page 145.
16. Provide the SQL Server connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Type the name of the schema.
    e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
    f) Click **Next**, continue at Step 18 on page 145.
17. Provide the PostgreSQL connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
    e) Click **Next**, continue at Step 18 on page 145.
18. Provide the external database credential information.

- In the **Admin Username** field, type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- In the **Admin Password** field, type the password for an external database administrator account.
- In the **Username** field, type a user name. For a list of required privileges, see External system databases on page 15.
- In the **Password** field, type the user password.

Important:

- Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.
- Passwords for an external database implementation are not persisted. These values must be specified in the response file with the `D2C_DB_ADMIN_PASSWORD` and `D2C_DB_USER_PASSWORD` options before running a silent install.
- The installer attempts to validate the database. If the installer is unable to validate, you are prompted to reenter credentials or skip validation. If you skip validation, the response file must have the `SKIP_DATABASE_VALIDATION` property set to `true`. During a silent upgrade, the installer will complete the upgrade even when the database validation fails.

19. Review the Server Access Port. The Server Access Port must be opened for the load balancer. The default is 8080.
20. Take the appropriate action depending on whether you are using the On-Premises Connector.
    - If you are not using the On-Premises Connector, skip to the next step.
    - If you are using the On-Premises Connector, review the On-Premises Access Ports. The On-Premises Access Port and the TCP Notification Server Port must be opened for the load balancer.

Important: If you changed any values for On-Premises Access Ports during an upgrade, you will need to reconfigure the load balancer to use the new ports.

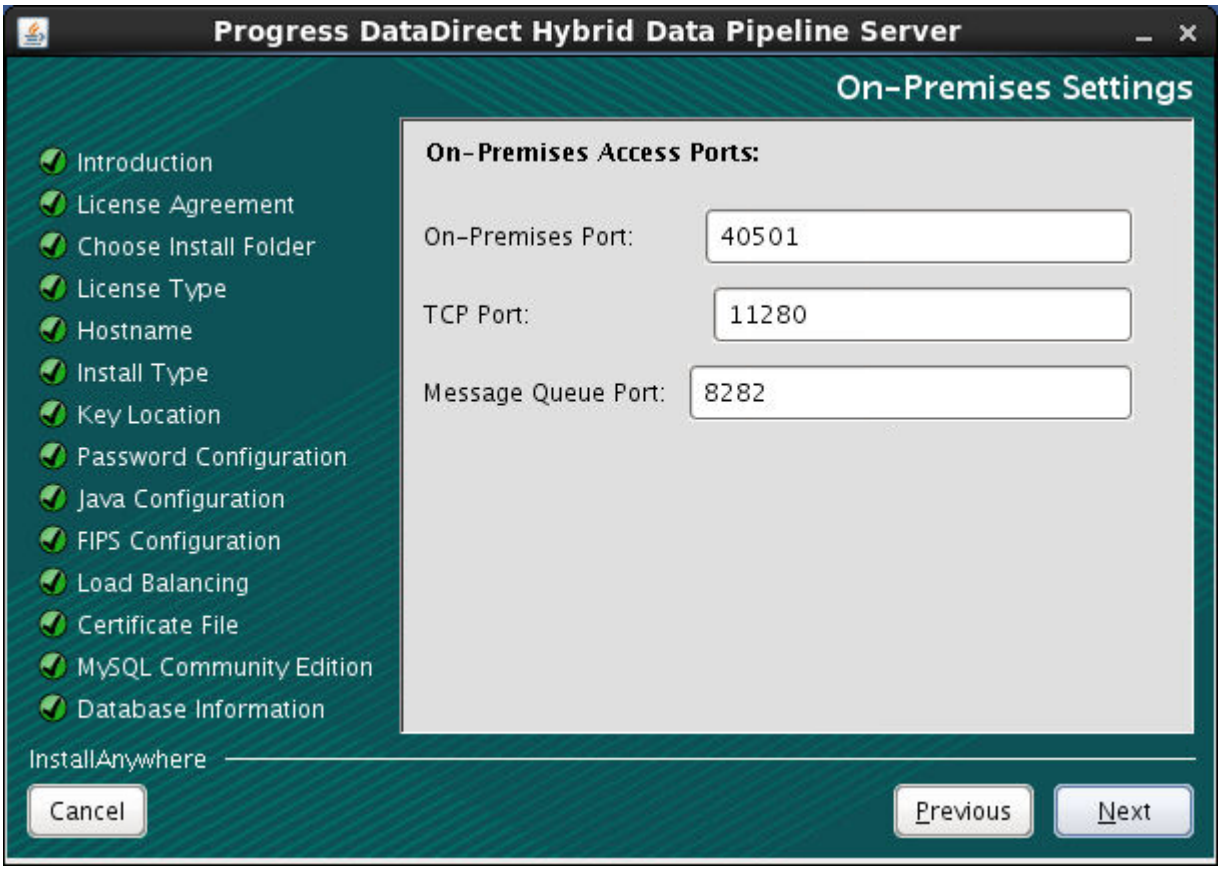


Table 35: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
Message Queue Port	8282	Port for the message queue

21. Review the Server Internal Ports. The Internal API Port and the Shutdown Port must be opened.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of any Hybrid Data Pipeline instance.

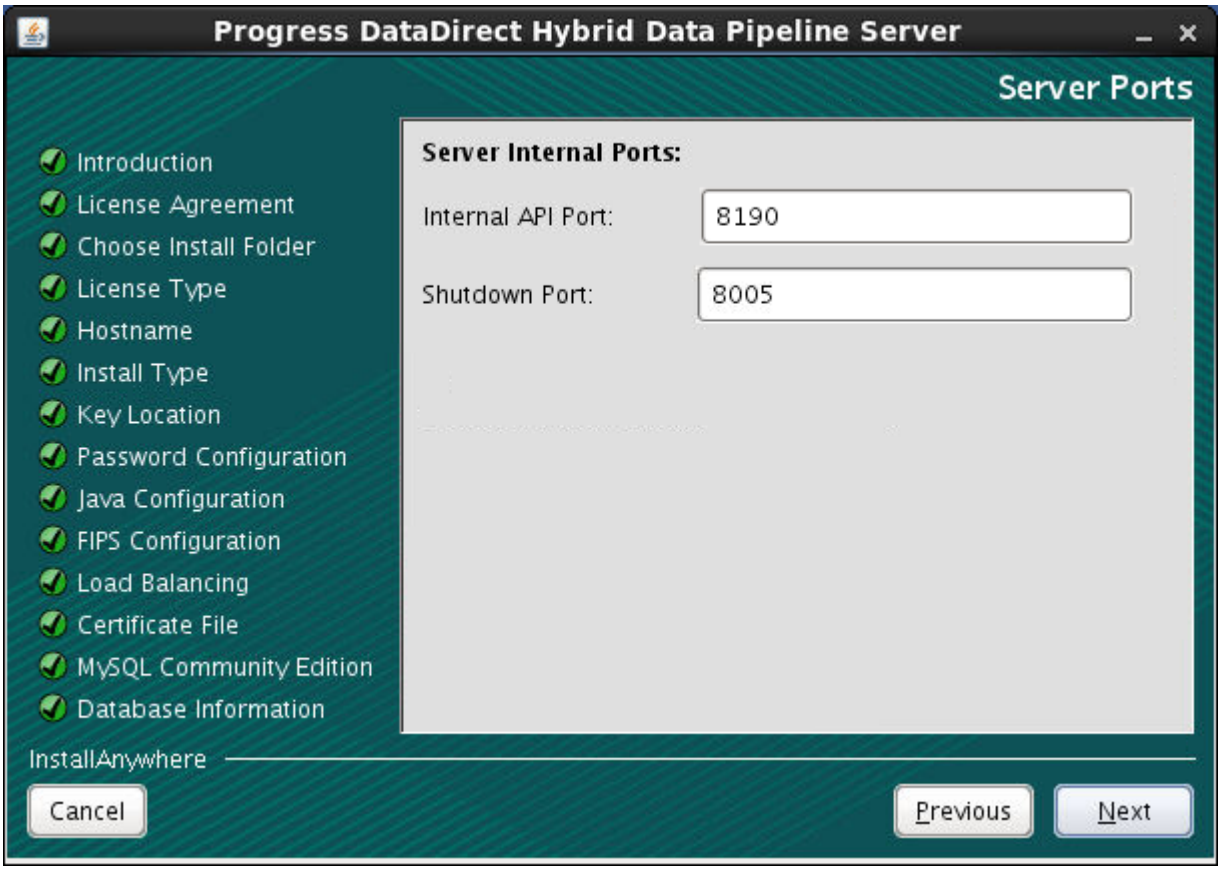


Table 36: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Shutdown Port	8005	Shutdown port

22. Review the upgrade summary. If you are satisfied with your choices, press **ENTER** to generate the response file.
23. After the response files has been generated, press **ENTER** to exit the installer.
24. Confirm that a response file has been generated by navigating to the response file directory you specified in Step 3 on page 142 and opening the response file.
25. Proceed to Editing a GUI generated upgrade response file on page 148.

Editing a GUI generated upgrade response file

After you have generated a response file, you must edit the response file to suit your environment before you perform a silent upgrade. Use the following guidelines to edit your response file.

- If you are installing the Hybrid Data Pipeline Server on a system other than the one you used to generate the response file, you must designate the host machine with the `D2C_HOSTNAME` option.

- If you want to continue with an upgrade even though hostname, port, and load balancer hostname validations fail, then the validation settings should be set as follows. (Note that these properties are set to `false` by default.)

  ```
  SKIP_HOSTNAME_VALIDATION=true
  SKIP_PORT_VALIDATION=true
  SKIP_LB_HOSTNAME_VALIDATION=true
  ```

- If you are storing user credentials on an external database, you must designate the administrator and user passwords of the external database with the `D2C_DB_ADMIN_PASSWORD` and `D2C_DB_USER_PASSWORD` options. However, you may skip database validation by setting the `SKIP_DATABASE_VALIDATION` property to `true`. If you skip database validation, the installer will complete the installation even when the database validation fails.

The following example response file includes the settings for a load balancer deployment using the On-Premises Connector, using a MySQL Community Edition external database. This type of response file would be generated with the GUI installer.

```
# Tue Nov 21 15:26:30 EST 2017
# Replay feature output
# ---------------------
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.



#Choose Install Folder
#---------------------
USER_INSTALL_DIR=<install_dir>

#Installation License Type
#-------------------------
D2C_EVAL_YES=1
D2C_LICENSED_YES=0
D2C_LICENSE_KEY=

#Enter Hostname
#--------------
D2C_HOSTNAME=<hybriddatapipelinehost>

#SKIP VALIDATION SETTINGS
#------------------------
SKIP_HOSTNAME_VALIDATION=true
SKIP_PORT_VALIDATION=true

#Install Type
#------------
D2C_INSTALL_TYPE_TYPICAL=0
D2C_INSTALL_TYPE_CUSTOM=1

#Key location
#------------
USER_INPUT_CHOOSE_KEY_LOCATION=1
USER_INPUT_KEY_LOCATION=/<keyfilepath>/
USER_INPUT_DEFAULT_KEY_LOCATION=0

#Java Configuration
#------------------
SPECIFY_JAVA_HOME_NO=1
SPECIFY_JAVA_HOME_YES=0
HDP_JAVA_HOME_DIR=<jrepath>

#FIPS Configuration
#------------------
D2C_USING_FIPS_CONFIG=0
```

```
#Load Balancing
#--------------
D2C_NO_LOAD_BALANCER=0
D2C_NETWORK_LOAD_BALANCER=0
D2C_CLOUD_LOAD_BALANCER=1
LOAD_BALANCING_HOST_NAME=<loadbalancerhost>


#SKIP VALIDATION SETTINGS
#------------------------
SKIP_LB_HOSTNAME_VALIDATION=true

#Certificate File
#----------------
D2C_CERT_FILE_YES=1
D2C_CERT_FILE=/<certificatepath>/<filename>
D2C_CERT_FILE_NO=0

#MySQL Community Edition
#-----------------------
D2C_DB_MYSQL_COMMUNITY_SUPPORT_YES=1
D2C_DB_MYSQL_JAR_PATH=/<mysqldriverpath>/<filename>.jar
D2C_DB_MYSQL_COMMUNITY_SUPPORT_NO=0

#Database Type
#--------------
D2C_DB_VENDOR_ORACLE=0
D2C_DB_VENDOR_MSSQLSERVER=0
D2C_DB_VENDOR_MYSQL=1
D2C_DB_VENDOR_POSTGRESQL=0

#MySQL Connection Information
#----------------------------
D2C_DB_HOSTNAME=mysqlserver1
D2C_DB_PORT=3306
D2C_DATABASE_NAME=<db_name>
D2C_DB_ADVANCED_OPTIONS=

#Database Credential Information
#-------------------------------
D2C_DB_ADMIN_USERNAME=<adminname>
D2C_DB_ADMIN_PASSWORD=<adminpassword>
D2C_DB_USER_USERNAME=<username>
D2C_DB_USER_PASSWORD=<userpassword>

#Database Connection Validation
#------------------------------
SKIP_DATABASE_VALIDATION=false

#HDP Server Access Ports
#-----------------------
D2C_API_PORT=8080

#On-Premises Settings
#--------------------
USER_INPUT_ENABLE OPC=1
D2C_OPC_PORT=40501
D2C_NOTIFICATION_PORT=11280
D2C_MESSAGE_QUEUE_PORT=8282

#Server Ports
#------------
D2C_INTERNAL_API_PORT=8190
D2C_SHUTDOWN_PORT=8005
```

Creating a response file for a standalone upgrade (console mode)

Note: The installer does not support changing a standalone deployment to a load balancer deployment during an upgrade, or vice versa. To make such a change, you would need to uninstall the server and then reinstall it. See Uninstalling Hybrid Data Pipeline server on page 166 and Installing the Hybrid Data Pipeline server on page 47 for details.

After copying the product installation file to a temporary directory, take the following steps to generate a response file for a standalone upgrade using the console installer.

1. From a command-line prompt, navigate to the directory where you saved the product file. Alternatively, place the product file directory on your path before proceeding to the next step.

   The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin`, where *nn* is the version of the product.

2. Make the file an executable using the `chmod` command. Then, press **ENTER**. For example:

   ```
   chmod +x ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

3. At a command-line prompt, type the following command where *response_file* is the path and file name of the response file you want to create. You must specify an absolute path.

   ```
   PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -i console -r
   response_file
   ```

   The following example creates a response file named `pipeline.response` in the `/home/users/johndoe` directory.

   ```
   PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -i console -r
   /home/users/johndoe/pipeline.response
   ```

4. The License Agreement appears. Press **ENTER** multiple times to advance through the license agreement. Make sure that you read and understand the license agreement.

   - To accept the terms in the License Agreement and continue with the installation, type `Y`.
   - To end the installation, type `N` and press **ENTER**.

   Note: You can exit the installation program at any time by typing `Quit`.

5. You are prompted for the installation directory. Type the absolute path to the installation directory of the installation you want to upgrade. Then, press **ENTER**.
6. You are prompted to upgrade the existing installation or go back to enter a different installation directory. Type `1` to upgrade the existing installation. Then, press **ENTER**.
7. Choose whether you want to upgrade with an evaluation or licensed version of the product. Licensed installations require a valid License Key.

   - Evaluation. Type `1` to upgrade with an evaluation version of the product that is fully functional for 30 days. Then, press **ENTER**.
   - Licensed. Type `2` if you purchased a licensed version of the product. Then, press **ENTER**. Type the license key, including any dashes, and then press **ENTER**.

8. Accept or enter the fully qualified hostname of the machine that will host the Hybrid Data Pipeline server. By default, the installer suggests the name of the current machine. Then, press **ENTER**.

Note the following important information. Then, press **ENTER** to continue.

- If you enter a hostname different than the hostname of the current machine, the installer will fail to validate the hostname. You are then prompted to reenter the hostname or skip validation. If you are planning on using the response file to install the product on a different machine, you should opt to skip validation.
- Before using the response file to install the product on another machine, the response file must have the `SKIP_HOSTNAME_VALIDATION` and `SKIP_PORT_VALIDATION` validation properties set to `1`. For example:

```
SKIP_HOSTNAME_VALIDATION=true
SKIP_PORT_VALIDATION=true
```

- Running an installation in silent mode with a response file containing these settings allows the silent installation to continue even if hostname or port validation fail. When the validation fails during the silent installation process, the installer generates the file `SilentInstallInfo.log` in the user's home directory but completes a full installation.

9. Select how you want to continue the upgrade.
   - Type `1` for an Express upgrade to persist previously established values. Then, press **ENTER** and continue at Step 27 on page 156.
   - Type `2` to change values for the following configurations. Then, press **ENTER** to continue.
     - Change the location of the SSL certificate file
     - Change the Java configuration to use an external JRE
     - Enable or disable FIPS
     - Add MySQL Community Edition as a data store or external system database
     - Change the system database you are using
     - Update external system database credentials
     - Change Server Access Ports
     - Change On-Premises Connector Ports
     - Change Server Internal Access Ports

Note: The key location where the generated key and internal files are stored cannot be modified when performing an upgrade.

---

10. Specify the desired Java configuration.

Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

- Type `1` if you will be using an external JRE (a JRE not installed with the server).
- Type `2` if you will be using the embedded JRE installed with the server.

11. Specify the fully qualified location of the Java home directory. This is the path to the external JRE. Press **ENTER**.
12. Specify whether you want to enable FIPS on the Hybrid Data Pipeline server.

Important: To enable FIPS, your hardware must support secure random, or you must have a secure random daemon installed.

Important: When you enable FIPS during an upgrade, the environment uses the encryption key for the system database that was generated during the original installation of the server. This encryption key, while generated with a FIPS compliant algorithm, was not generated with a FIPS certified implementation of the algorithm.

- Type `1` if you want to enable FIPS. Press **ENTER** and continue to the next step.
- Type `2` and press **ENTER** if you want to use the default setting which is FIPS disabled.

13. Depending on your environment, provide the appropriate SSL certificate information.

    - Type `1` to specify a PEM file to be used by the server to establish SSL connections with ODBC and JDBC client applications. Press **ENTER**. Type the full path to the PEM file. Press **ENTER** again, and proceed to the next step.

      Note: The PEM file must consist of a private key, a public key certificate issued by a certificate authority (CA), and additional certificates that make up the trust chain. See The PEM file on page 20 for more information.

    - Type `2` to use the SSL certificate specified in the previous installation or the self-signed certificate included with the previous installation. Then, press **ENTER**, and proceed to the next step.

      Note: The self-signed certificate may be used in a test environment. However, for production, a PEM file with required information should be specified. See The PEM file on page 20 for more information.

14. Choose the appropriate option depending on whether you are using MySQL Community Edition. MySQL Community Edition can be used as an external system database or as a data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. However, you can use the MySQL Connector/J driver to use MySQL Community Edition as an external system database or as a data source.

    - Type `1` and press **ENTER**, if you are using MySQL Community Edition. Type the name and location of the MySQL Connector/J jar file, and press **ENTER** again.
    - Type `2` and press **ENTER**, if you are not using MySQL Community Edition in your environment.

    Note: For more information on the MySQL Connector/J driver, visit the MySQL developer website at https://dev.mysql.com/.

15. Select the type of database you want to use to store system information.

    - Type `1` to use the default internal database supplied by this installation. Continue at Step 17 on page 154.
    - Type `2` to store information on an external database. Proceed to the next step.

    Note: Users and data sources created in the internal database are specific to the internal database. They are not migrated to the external database if you subsequently modify the Hybrid Data Pipeline Server to use an external database.

16. Select the type of external system database you want to use to store system information.

    - Select **Oracle**, and continue at Step 18 on page 154.

- Select **MySQLCommunity**, and continue at Step 19 on page 154.
- Select **MSSQLServer**, and continue at Step 20 on page 154.
- Select **PostgreSQL**, and continue at Step 21 on page 155.

17. Enter the database port for the internal database. If your environment has already defined a function for the default port, the installer pops up a message so that you can specify a different port. Press **ENTER**, and continue at Step 23 on page 155.
18. Provide the Oracle connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Select the connection type. Do one of the following:
       - If you connect using the Oracle System Identifier (SID), type `1`, then type the SID.
       - If you connect using the Service Name, type `2`,then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name—a name that typically comprises the database name and domain name.
    d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as a semicolon-separated list of *`parameter=value`*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret; serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

    e) Press **ENTER**, continue at Step 22 on page 155.
19. Provide connection information for the MySQL Community Edition external database.
    a) Type the name of the Hostname.
    b) Type the port number.
    c) Type the database name.
    d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as an ampersand-separated list of *`parameter=value`*.
    e) Press **ENTER**, continue at Step 22 on page 155.
20. Provide the SQL Server connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Type the name of the schema.
    e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *`parameter=value`*.
    f) Press **ENTER**, continue at Step 22 on page 155.

21. Provide the PostgreSQL connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of `parameter=value`.
    e) Press **ENTER**, continue at Step 22 on page 155.
22. You are prompted to provide the database credential information for a user with administrator privileges and for a user without administrator privileges.
    - Type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
    - You are prompted to provide the Admin Password. Type the password for an external database administrator account.
    - You are prompted to provide the username for a user who does *not* have administrator privileges. Type a user name. For a list of required privileges, see External system databases on page 15.
    - You are prompted to provide the User Password. Type the user password.
    - The installer validates the connection. Press **ENTER** to continue.

    Important:
    - Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.
    - Passwords for an external database implementation are not persisted. These values must be specified in the response file with the `D2C_DB_ADMIN_PASSWORD` and `D2C_DB_USER_PASSWORD` options before running a silent install.
    - The installer attempts to validate the database. If the installer is unable to validate, you are prompted to reenter credentials or skip validation. If you skip validation, the response file must have the `SKIP_DATABASE_VALIDATION` property set to `true`. During a silent upgrade, the installer will complete the upgrade even when the database validation fails.
23. Review the Server Access Ports. A Server Access Port must be available to the end user across the firewall. Best security practices recommend using an HTTPS port.

    Table 37: Server Access Ports

Name	Default	Description
HTTP Port	8080	Port that exposes Hybrid Data Pipeline
HTTPS Port	8443	SSL port that exposes Hybrid Data Pipeline

24. Select whether you will continue to use the On-Premises Connector.
    - If using the On-Premises Connector, type `1` and press **ENTER**. Then continue to the next step.
    - If not using the On-Premises Connector, type `2` and press **ENTER**. Continue at Step 26 on page 156.

25. Review the On-Premises Access Ports. The On-Premises Access Port and a Notification Server Port must be available across the firewall. Best security practices recommend using the SSL Notification Server Port.

Important: If you change any values for On-Premises Access Ports during an upgrade, you will need to reinstall the On-Premises Connector with the updated distribution files in the `redist` subdirectory. See "What to do next" in Performing a silent upgrade on page 164.

Table 38: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
SSL Port	11443	SSL port for the Notification Server
Message Queue Port	8282	Port for the message queue

26. Review the Server Internal Ports. A port for the internal API and the Shutdown Port must be opened. Best security practices recommend using the Internal API SSL Port.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of the Hybrid Data Pipeline instance.

Table 39: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Internal API SSL Port	8090	SSL port for the Internal API
Shutdown Port	8005	Shutdown port

27. Review the summary. If you are satisfied with your choices, press **ENTER** to generate the response file.
28. After the response file has been generated, press **ENTER** to exit the installer.
29. Confirm that a response file has been generated by navigating to the response file directory you specified in Step 3 on page 151 and opening the response file.
30. Proceed to Editing a console generated upgrade response file on page 162.

Creating a response file for a load balancer upgrade (console mode)

Note: The installer does not support changing a standalone deployment to a load balancer deployment during an upgrade, or vice versa. To make such a change, you would need to uninstall the server and then reinstall it. See Uninstalling Hybrid Data Pipeline server on page 166 and Installing the Hybrid Data Pipeline server on page 47 for details.

After copying the product installation file to a temporary directory, take the following steps to generate a response file for a load balancer upgrade using the console installer.

1. From a command-line prompt, navigate to the directory where you saved the product file. Alternatively, place the product file directory on your path before proceeding to the next step.

   The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin`, where *nn* is the version of the product.

2. Make the file an executable using the `chmod` command. Then, press **ENTER**. For example:

   ```
   chmod +x ./PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin
   ```

3. At a command-line prompt, type the following command where *response_file* is the path and file name of the response file you want to create. You must specify an absolute path.

   ```
   PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -i console -r
   response_file
   ```

   The following example creates a response file named `pipeline.response` in the `/home/users/johndoe` directory.

   ```
   PROGRESS_DATADIRECT_HDP_SERVER_nn_LINUX_64_INSTALL.bin -i console -r
   /home/users/johndoe/pipeline.response
   ```

4. The License Agreement appears. Press **ENTER** multiple times to advance through the license agreement. Make sure that you read and understand the license agreement.

   - To accept the terms in the License Agreement and continue with the installation, type `Y`.
   - To end the installation, type `N` and press **ENTER**.

   Note: You can exit the installation program at any time by typing `Quit`.

5. You are prompted for the installation directory. Type the absolute path to the installation directory of the installation you want to upgrade. Then, press **ENTER**.
6. You are prompted to upgrade the existing installation or go back to enter a different installation directory. Type `1` to upgrade the existing installation. Then, press **ENTER**.
7. Choose whether you want to upgrade with an evaluation or licensed version of the product. Licensed installations require a valid License Key.

   - Evaluation. Type `1` to upgrade with an evaluation version of the product that is fully functional for 30 days. Then, press **ENTER**.
   - Licensed. Type `2` if you purchased a licensed version of the product. Then, press **ENTER**. Type the license key, including any dashes, and then press **ENTER**.

8. Accept or enter the fully qualified hostname of the machine that will host the Hybrid Data Pipeline server. By default, the installer suggests the name of the current machine.

   Note the following important information. Then, click **Next** to continue.

   - If you enter a hostname different than the hostname of the current machine, the installer will fail to validate the hostname. You are then prompted to reenter the hostname or skip validation. If you are planning on using the response file to install the product on a different machine, you should opt to skip validation.

- Before using the response file to install the product on another machine, the response file must have the `SKIP_HOSTNAME_VALIDATION` and `SKIP_PORT_VALIDATION` properties set to `true`. For example:

```
SKIP_HOSTNAME_VALIDATION=true
SKIP_PORT_VALIDATION=true
```

- Running an installation in silent mode with a response file containing these settings allows the silent installation to continue even if hostname or port validation fail. When the validation fails during the silent installation process, the installer generates the file `SilentInstallInfo.log` in the user's home directory but completes a full installation.

9. Select how you want to continue the upgrade.
   - Type `1` for an Express upgrade to persist previously established values. Then, press **ENTER** and continue at Step 24 on page 162.
   - Type `2` to change values for the following configurations. Then, press **ENTER** to continue.
     - Change the location of the SSL certificate file
     - Change the Java configuration to use an external JRE
     - Enable or disable FIPS
     - Add MySQL Community Edition as a data store or external system database
     - Change the system database you are using
     - Update external system database credentials
     - Change Server Access Ports
     - Change On-Premises Connector Ports
     - Change Server Internal Access Ports

Note: The following elements of an installation cannot be modified when performing an upgrade of a load balancer installation: key location, load balancer hostname, and On-Premises Connector enablement.

10. Specify the desired Java configuration.

Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

- Type `1` if you will be using an external JRE (a JRE not installed with the server).
- Type `2` if you will be using the embedded JRE installed with the server.

11. Specify the fully qualified location of the Java home directory. This is the path to the external JRE. Press **ENTER**.
12. Specify whether you want to enable FIPS on the Hybrid Data Pipeline server.

Important: To enable FIPS, your hardware must support secure random, or you must have a secure random daemon installed.

Important: When you enable FIPS during an upgrade, the environment uses the encryption key for the system database that was generated during the original installation of the server. This encryption key, while generated with a FIPS compliant algorithm, was not generated with a FIPS certified implementation of the algorithm.

- Type `1` if you want to enable FIPS. Press **ENTER** and continue to the next step.
- Type `2` and press **ENTER** if you want to use the default setting which is FIPS disabled.

13. Depending on your environment, provide the appropriate SSL certificate information.
    - Type `1` to specify the SSL certificate file to be used with the Hybrid Data Pipeline server. The specified file must be the root certificate used to sign the certificate for the load balancer server. PEM, DER, and Base64 encodings are supported. Type the full path to the SSL certificate file. Then, click **Next**.
    - Type `2` to use the SSL certificate file that was specified during the previous installation or bypass the specification of an SSL certificate. Then, press **ENTER**.
14. Choose the appropriate option depending on whether you are using MySQL Community Edition. MySQL Community Edition can be used as an external system database or as a data source. Hybrid Data Pipeline does not provide a driver for MySQL Community Edition. However, you can use the MySQL Connector/J driver to use MySQL Community Edition as an external system database or as a data source.
    - Type `1` and press **ENTER**, if you are using MySQL Community Edition. Type the name and location of the MySQL Connector/J jar file, and press **ENTER** again.
    - Type `2` and press **ENTER**, if you are not using MySQL Community Edition in your environment.

Note: For more information on the MySQL Connector/J driver, visit the MySQL developer website at https://dev.mysql.com/.

15. Select the type of external database you want to use to store system information.
    - Select **Oracle**, and continue at Step 16 on page 159.
    - Select **MySQLCommunity**, and continue at Step 17 on page 160.
    - Select **MSSQLServer**, and continue at Step 18 on page 160.
    - Select **PostgreSQL**, and continue at Step 19 on page 160.
16. Provide the Oracle connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Select the connection type. Do one of the following:
        - If you connect using the Oracle System Identifier (SID), type `1`, then type the SID.
        - If you connect using the Service Name, type `2`,then type the database service name that specifies the database that is used for the connection. The service name is a string that is the global database name—a name that typically comprises the database name and domain name.

d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as a semicolon-separated list of *parameter=value*. For example, you may enter to following options to configure SSL:

```
encryptionLevel=Required;encryptionTypes=(AES256);
dataIntegrityLevel=Required;dataIntegrityTypes=(SHA1);
encryptionMethod=SSL;keyStore=/common/Oracle/trustStore.jks;
keyStorePassword=secret;serverType=dedicated;authenticationMethod=ntlm;
hostNameInCertificate=oracle;editionName=hybrid
```

e) Press **ENTER**, and continue at Step 20 on page 160.

17. Provide connection information for the MySQL Community Edition external database.
    a) Type the name of the Hostname.
    b) Type the port number.
    c) Type the database name.
    d) Optionally, when prompted for **Advanced Options**, specify additional connection parameters and their values to be included the connection url. Values should be entered as an ampersand-separated list of *parameter=value*.
    e) Press **ENTER**, and continue at Step 20 on page 160.
18. Provide the SQL Server connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Type the name of the schema.
    e) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
    f) Press **ENTER**, and continue at Step 20 on page 160.
19. Provide the PostgreSQL connection information.
    a) Type the name of the host.
    b) Type the port number.
    c) Type the database name.
    d) Optionally, in the **Advanced Options** field, specify additional connection parameters and their values to be included in the connection URL. Values should be entered as a semicolon-separated list of *parameter=value*.
    e) Press **ENTER**, and continue at Step 20 on page 160.
20. You are prompted to provide the database credential information for a user with administrator privileges and for a user without administrator privileges.
    - Type the administrator user name. The administrator user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
    - You are prompted to provide the Admin Password. Type the password for an external database administrator account.

- You are prompted to provide the username for a user who does *not* have administrator privileges. Type a user name. The standard user must have certain privileges that are specific to the database vendor. For a list of required privileges, see External system databases on page 15.
- You are prompted to provide the User Password. Type the user password.
- The installer validates the connection. Press **ENTER** to continue.

Important:

- Administrator credentials are only required at install time to create the database schema. Administrator credentials are not used by the product at run time.
- Passwords for an external database implementation are not persisted. These values must be specified in the response file with the `D2C_DB_ADMIN_PASSWORD` and `D2C_DB_USER_PASSWORD` options before running a silent install.
- The installer attempts to validate the database. If the installer is unable to validate, you are prompted to reenter credentials or skip validation. If you skip validation, the response file must have the `SKIP_DATABASE_VALIDATION` property set to `true`. During a silent upgrade, the installer will complete the upgrade even when the database validation fails.

21. Review the Server Access Port. The Server Access Port must be opened for the load balancer. The default is 8080.
22. Take the appropriate action depending on whether you are using the On-Premises Connector.
    - If you are not using the On-Premises Connector, skip to the next step.
    - If you are using the On-Premises Connector, review the On-Premises Access Ports. The On-Premises Access Port and the TCP Notification Server Port must be opened for the load balancer.

Important: If you changed any values for On-Premises Access Ports during an upgrade, you will need to reconfigure the load balancer to use the new ports.

Table 40: On-Premises Access Ports

Name	Default	Description
On-Premises Port	40501	Port for the On-Premises Connector
TCP Port	11280	Port for the Notification Server
Message Queue Port	8282	Port for the message queue

23. Review the Server Internal Ports. The Internal API Port and the Shutdown Port must be opened.

Important: As a matter of best practice, the Shutdown Port should not be available outside the firewall of any Hybrid Data Pipeline instance.

Table 41: Server Internal Ports

Name	Default	Description
Internal API Port	8190	Non-SSL port for the Internal API
Shutdown Port	8005	Shutdown port

24. Review the upgrade summary. If you are satisfied with your choices, press **ENTER** to generate the response file.
25. After the response file has been generated, press **ENTER** to exit the installer.
26. Confirm that a response file has been generated by navigating to the response file directory you specified in Step 3 on page 157 and opening the response file.
27. Proceed to Editing a console generated upgrade response file on page 162.

Editing a console generated upgrade response file

After you have generated a response file, you must edit the response file to suit your environment before you perform a silent upgrade. Use the following guidelines to edit your response file.

- If you are installing the Hybrid Data Pipeline server on a system other than the one you used to generate the response file, you must designate the host machine with the `D2C_HOSTNAME_CONSOLE` option.
- If you want to continue with an upgrade even though hostname, port, and load balancer hostname validations fail, then the validation settings should be set as follows. (Note that these properties are set to `false` by default.)

```
SKIP_HOSTNAME_VALIDATION=true
SKIP_PORT_VALIDATION=true
SKIP_LB_HOSTNAME_VALIDATION=true
```

- If you are storing user credentials on an external database, you must designate the administrator and user passwords of the external database with the `D2C_DB_ADMIN_PASSWORD` and `D2C_DB_USER_PASSWORD` options. However, you may skip database validation by setting the `SKIP_DATABASE_VALIDATION` property to `true`. If you skip database validation, the installer will complete the installation even when the database validation fails.

The following example response file includes the settings for a load balancer deployment using the On-Premises Connector, using a MySQL Community Edition external database. This type of response file would be generated using the installer in console mode.

```
# Tue Nov 21 15:45:31 EST 2017
# Replay feature output
# ---------------------
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.



#Choose Install Folder
#---------------------
USER_INSTALL_DIR=<install_dir>

#Installation License Type
#-------------------------
D2C_LICENSE_TYPE_CONSOLE=\"Evaluation\",\"\"
```

```
#Enter Hostname
#--------------
D2C_HOSTNAME_CONSOLE=\"<hybriddatapipelinehost>\"

#SKIP VALIDATION SETTINGS
#--------------------------------
SKIP_HOSTNAME_VALIDATION=true
SKIP_PORT_VALIDATION=true

#Install Type
#------------
D2C_INSTALL_TYPE_CONSOLE=\"\",\"Custom\"

#Key Location
#------------
USER_INPUT_KEY_LOCATION_CONSOLE_OPTION=\"Specify location\",\"\"
USER_INPUT_KEY_LOCATION_CONSOLE=\"<keyfilepath>\"

#Java Configuration
#------------------
SPECIFY_JAVA_HOME_YESNO=\"No\",\"\"
HDP_JAVA_HOME_DIR_CONSOLE=\"<jrepath>\"

#FIPS Configuration
#------------------
D2C_USING_FIPS_CONFIG_CONSOLE=\"No\",\"\"

#Load Balancing
#--------------
D2C_LOAD_BALANCER_CONSOLE=\"\",\"Network Load Balancer\",\"\"
LOAD_BALANCING_HOST_NAME_CONSOLE=\"<loadbalancerhost>\"

#SKIP VALIDATION SETTINGS
#------------------------
SKIP_LB_HOSTNAME_VALIDATION=true

#Certificate File
#----------------
D2C_CERT_FILE_YESNO=\"Yes\",\"\"
D2C_CERT_FILE_CONSOLE=\"/<sslcertficatepath>/<filename>\"

#MySQL Community Edition
#-----------------------
D2C_DB_MYSQL_COMMUNITY_SUPPORT_CONSOLE=\"Yes\",\"\"
D2C_DB_MYSQL_JAR_PATH_CONSOLE=\"/<mysqldriverpath>/<filename>.jar\"

#External Database Type
#----------------------
D2C_DB_VENDOR_CONSOLE=\"\",\"MySQLCommunity\"

#Database Connection Information - MySQLCommunity Hostname
#---------------------------------------------------------
D2C_DB_HOSTNAME_CONSOLE=\"<mysqlhost>\"

#Database Connection Information - MySQLCommunity Port
#-----------------------------------------------------
D2C_DB_PORT_CONSOLE=\"3306\"

#Database Connection Information - MySQL Database Name
#-----------------------------------------------------
D2C_DATABASE_NAME_CONSOLE=\"<mysqldbname>\"

#Database Connection Information - MySQL Connection Advanced Options
#-------------------------------------------------------------------
D2C_DB_ADVANCED_OPTIONS_CONSOLE=\"\"

#Database Connection Information - Admin Username
#------------------------------------------------
D2C_DB_ADMIN_USERNAME_CONSOLE=\"<adminname>\"
```

```
#Database Connection Information - Admin Password
#------------------------------------------------
D2C_DB_ADMIN_PASSWORD_CONSOLE=\"<adminpassword>\"

#Database Connection Information - User Username
#-----------------------------------------------
D2C_DB_USER_USERNAME_CONSOLE=\"<username>\"

#Database Connection Information - User Password
#-----------------------------------------------
D2C_DB_USER_PASSWORD_CONSOLE=\"<userpassword>\"

#Database Connection Validation
#------------------------------
SKIP_DATABASE_VALIDATION=false

#HDP Server Access Ports - HTTP Port
#-----------------------------------
D2C_API_PORT_CONSOLE=\"8080\"

#On-Premises Settings
#--------------------
ENABLE_OPC_CONSOLE=\"Yes\",\"\"

#On-Premises Ports - On-Premises Port
#------------------------------------
D2C_OPC_PORT_CONSOLE=\"40501\"

#On-Premises Ports - Notification TCP Port
#----------------------------------------
D2C_NOTIFICATION_PORT_CONSOLE=\"11280\"

#On-Premises Ports - Message Queue Port
#--------------------------------------
D2C_MESSAGE_QUEUE_PORT_CONSOLE=\"8282\"

#Server Internal Ports - Internal API Port
#----------------------------------------
D2C_INTERNAL_API_PORT_CONSOLE=\"8190\"

#Server Internal Ports - Shutdown Port
#------------------------------------
D2C_SHUTDOWN_PORT_CONSOLE=\"8005\"
```

Performing a silent upgrade

After you have generated and edited your response file, you can perform a silent upgrade.

Take the following steps to perform a silent upgrade:

1. From a command-line prompt, navigate to the directory where you saved the product file. Alternatively, place the product file directory on your path before proceeding to the next step.

   The product file has the format `PROGRESS_DATADIRECT_HDP_SERVER_`*`nn`*`_LINUX_64_INSTALL.bin`, where *`nn`* is the version of the product.

2. Execute a silent upgrade by entering the following command and pressing **ENTER**.

   `PROGRESS_DATADIRECT_HDP_SERVER_`*`nn`*`_LINUX_64_INSTALL.bin -i silent -f `*`response_file`*

   where *`response_file`* is the full path of the response file you have created and edited. For example, if the response file is named `pipeline.response` and resides in the directory `/home/users/`*`johndoe`*, you would enter:

   `PROGRESS_DATADIRECT_HDP_SERVER_`*`nn`*`_LINUX_64_INSTALL.bin -i silent -f `*`response_file`*

3. The upgrade proceeds without any further user intervention unless you enter an incorrect value on the console or in the response file, in which case an error is displayed and installation stops.
4. Verify the installation by accessing the Hybrid Data Pipeline user interface from a browser. The login page should appear. For example:

   `https://<myserver>:8443/`

   where for a standalone installation:

   <myserver> is the fully qualified hostname of the machine where you installed Hybrid Data Pipeline.

   where for a load balancer installation:

   <myserver> is the fully qualified hostname or IP address of the load balancer.

   After logging in, administrators can verify product version information by selecting **About** from the question mark drop-down menu. For more information on retrieving version information, refer to "Get Version Information" in the *Progress DataDirect Hybrid Data Pipeline User's Guide*.

When a silent installation or upgrade fails, the installer writes a file named `SilentInstallerError.log` to the user's home directory. This file can be used to troubleshoot installation errors.

What to do next

For a load balancer deployment, if you changed any values for On-Premises Access Ports during an upgrade, you will need to reconfigure the load balancer to use the new ports.

For a standalone deployment, if you changed any of the On-Premises Connector Ports, you will need to reinstall the On-Premises Connector with updated configuration and certificate files. These files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. These files must be copied to the directory of the On-Premises Connector installer before proceeding with the reinstallation of the On-Premises Connector.

The four configuration and certificate files are:

- `config.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`
- `OnPremise.properties`

See Installing the Hybrid Data Pipeline On-Premises Connector on page 191 for further details.

Stopping and starting the Hybrid Data Pipeline service

You may need to stop and start the Hybrid Data Pipeline service. Stop and start scripts (`stop.sh` and `start.sh`) are installed with the server.

Stopping a Hybrid Data Pipeline service

To stop a Hybrid Data Pipeline service, run the stop service script (`stop.sh`) in the `ddcloud` subdirectory of the installation directory. For example:

`./install_dir/ddcloud/stop.sh`

Note: Shutting down Hybrid Data Pipeline can take up to 2.5 minutes. Wait until you see the `Shutdown complete` message displayed on the console before taking any additional actions.

Starting a Hybrid Data Pipeline service

To start a Hybrid Data Pipeline service that has been stopped, run the start service script (`start.sh`) in the `ddcloud` subdirectory of the installation directory. For example:

`./install_dir/ddcloud/start.sh`

Uninstalling Hybrid Data Pipeline server

To uninstall Hybrid Data Pipeline server:

1. Change the directory to the installation directory, for example,

   ```
   cd /Hybrid_Server
   ```

2. Type one of the following and then press **ENTER**.

   - For GUI environments: `./Uninstall_ProgressHDPServer`
   - For console mode: `./Uninstall_ProgressHDPServer -i console`

Server installation log files

Log files found in the installation directory

When the installer successfully creates an installation directory, the following log files are written to the installation directory.

`.../_ProgressHDPServer_installation/Logs/Progress_DataDirect_Hybrid_Data_Pipeline_Server_Install.log`

This log file is generated by the InstallAnywhere installer. It records user inputs, installation settings, and installer activity.

`.../ddcloud/deploy.log`

The `deploy.log` file contains deployment details. In particular, it includes the parameters used in the configuration of the server and the system database. This file does not include user credentials, database credentials, or other confidential information supplied during the installation process.

`.../ddcloud/error.log`

The `error.log` file records errors, exceptions, and warnings that occur during server deployment.

`.../ddcloud/final.log`

The `final.log` file provides the final status of the server deployment. If no errors have occurred, the status message will be "Hybrid Data Pipeline deployment complete." If an error has occurred, the status message will indicate where the deployment script encountered the error.

Log file produced when installer fails to create installation directory

When the installer fails to create an installation directory, the following file is written to the machine's default temporary directory.

`Progress_DataDirect_Hybrid_Data_Pipeline_Server_InstallFailed.txt`

This log file provides information about the failed installation.

Additional log files generated for silent installation

When performing a silent installation, the following logs may be written to the user's home directory.

`.../SilentInstallError.log`

The `SilentInstallError.log` is generated when a silent installation fails. It provides information on why the installation failed.

`.../SilentInstallInfo.log`

The `SilentInstallInfo.log` file is generated when hostname and port validation are skipped by specifying the following settings in the silent installation response file.

```
SKIP_HOSTNAME_VALIDATION=true
SKIP_PORT_VALIDATION=true
SKIP_LB_HOSTNAME_VALIDATION=true
```

If you need help interpreting these files, contact Progress DataDirect Technical Support.

3

Installing the Hybrid Data Pipeline Driver for ODBC

You should install the Progress DataDirect Hybrid Data Pipeline Server component before you install the ODBC driver.

For details, see the following topics:

- Installation on Windows Systems
- Installation on UNIX and Linux Systems
- ODBC driver installation log files

Installation on Windows Systems

Windows system requirements for the ODBC driver

Before you install the Progress® DataDirect® Hybrid Data Pipeline Driver *for* ODBC:

- Verify that your system meets the appropriate driver requirements:
  - 32-bit driver Windows system requirements on page 170
  - 64-bit driver Windows system requirements on page 170

- You must be a system administrator or have update privileges for the Registry key `[HKEY_LOCAL_MACHINE]`. These privileges are required to update the Registry with the new drivers being installed. See your system administrator if you are unsure.
- If the files are on a network, verify that you have write privileges. See your network administrator if you are unsure.

Important: You must have Microsoft Data Access Components (MDAC) installed. For 32-bit drivers, you must have version 2.6 or higher. For 64-bit drivers, you must have version 2.8 (64-bit) or higher. Depending on the version of your Windows operating system, these components may already be installed. You can download MDAC or a utility that determines whether MDAC is installed and its version from the following Microsoft site: http://msdn.microsoft.com/en-us/data/aa937730.aspx

---

32-bit driver Windows system requirements

If your application was built with 32-bit system libraries, you must use the 32-bit driver. If your application was built with 64-bit system libraries, you must use the 64-bit driver (see 64-bit driver Windows system requirements on page 170). For the latest information on supported environments, see the Hybrid Data Pipeline support matrix.

The following processors are supported:

- x86: Intel
- x64: Intel and AMD

The following 32-bit operating systems are supported for the ODBC driver. All editions are supported unless otherwise noted.

- Windows 10
- Windows 8, 8.1
- Windows 7
- Windows Vista
- Windows XP, Service Pack 2 and higher
- Windows Server 2008

Requirements for an application that will use the ODBC driver include:

- It must be compatible with components that were built using Microsoft Visual Studio 2010 compiler and the standard Win32 threading model.
- ODBC header files must be used to compile your application. For example, Microsoft Visual Studio includes these files.

64-bit driver Windows system requirements

If your application was built with 64-bit system libraries, you must use the 64-bit driver. If your application was built with 32-bit system libraries, you must use the 32-bit driver (see 32-bit driver Windows system requirements on page 170). For the latest information on supported environments, see the Hybrid Data Pipeline support matrix.

The following processors are supported:

- Intel
- AMD

The following 64-bit operating systems are supported for the ODBC driver. All editions are supported unless otherwise noted.

- Windows 10
- Windows 8, 8.1
- Windows 7
- Windows Vista
- Microsoft Windows XP, Service Pack 2 and higher
- Windows Server 2012, Service Pack 2
- Windows Server 2008

Requirements for a 64-bit application that will use the ODBC driver include:

- It must be compatible with components that were built using Microsoft C/C++ Optimizing Compiler Version 14.00.40310.41 and the standard Windows 64 threading model.
- ODBC header files must be used to compile your application. For example, Microsoft Visual Studio includes these files.

Installing the ODBC driver on Windows

Applications using ODBC to access the Progress DataDirect Hybrid Data Pipeline connectivity service require access to a properly configured Hybrid Data Pipeline Driver *for* ODBC.

During installation of the Hybrid Data Pipeline server, four configuration and certificate files are generated. For a standalone deployment, these files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. For a load balancer deployment, these files are stored in a key location specified during installation. These files must be copied to the directory from which the ODBC driver installation program will be run. The files are:

- `config.properties`
- `OnPremise.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`

Take the following steps to install the driver on your local drive.

1. Download the product installation file into a temporary directory. For example, on a 64-bit machine, the file name is `PROGRESS_DATADIRECT_HDP_ODBC_`*`nn`*`_WIN_64.exe` where *`nn`* is the version number of the ODBC driver.
2. Copy the four configuration and certificate files from the Hybrid Data Pipeline Server installation into the temporary directory with the installer file.
3. Double-click the installation file to start the installer.

   The **Introduction** window opens. Click **Next** to continue.

   Note: You can exit the installation program at any time by clicking **Cancel**, or return to the previous window by clicking **Previous**.

4. Choose the type of installation to perform. Select one of the following options:

- **Standard Installation**. Select this option to install the standard unbranded version of the driver. Click **Next** to continue with the installation. Continue at the next step.
- **OEM Installation**. Select this option if you have purchased a licensed version of the product. Refer to the *Progress DataDirect Hybrid Data Pipeline for ODBC Distribution Guide* for information on installing, branding, unlocking, and distributing your branded driver.

5. In the **Where Would You Like to Install?** field, type the path, including the drive letter, of the product installation directory or click the **Choose** button to browse to and select an installation directory. Then click **Next**.
   - For the 32-bit driver on a 64-bit machine, the default is:

     ```
     C:\Program Files (x86)\Progress\DataDirect\Hybrid_Data_Pipeline_for_ODBC
     ```

   - For all other installations, the default is:

     ```
     C:\Program Files\Progress\DataDirect\Hybrid_Data_Pipeline_for_ODBC
     ```

6. In the **Create Default Data Source** window, check the box if you want to create a default data source entry in `HKEY_CURRENT_USER\Software\ODBC\ODBC.INI`.

   Note: If you select **Create Default Data Sources**, the data source currently in your registry with the same DataDirect default name will be overwritten. To maintain your current DataDirect default data source, rename it before you continue.

7. Click **Next**. The **Pre-Installation Summary** window appears.
8. Review the **Pre-Installation Summary** window to confirm the installation setup. Click **Previous** to revise your choices. Click **Install** to proceed with the installation.
9. Click **Done** to exit the installer.

Results:

The installer creates a **Progress DataDirect Hybrid Driver for ODBC** program group, which provides the following shortcuts:

- **ODBC Administrator**
- **ODBC Driver Help**
- **Uninstall Progress DataDirect Hybrid Driver for ODBC**

What to do next:

Refer to the *Progress DataDirect Hybrid Data Pipeline User's Guide Release 4.6* for information on creating Hybrid Data Pipeline data sources.

Silent installation of ODBC driver on Windows

A silent installation is useful for system administrators who want to install Progress DataDirect Hybrid Data Pipeline Driver *for* ODBC on multiple machines using the same options.

A silent installation requires the following steps:

- Creating the response file as described in Creating the response file using the installer on page 173 or Creating a response file using a text editor on page 173
- Performing the silent installation as described in Performing the silent installation on page 174

Creating the response file using the installer

Applications using ODBC to access the Progress DataDirect Hybrid Data Pipeline connectivity service require access to a properly configured Hybrid Data Pipeline Driver *for* ODBC.

During installation of the Hybrid Data Pipeline server, four configuration and certificate files are generated. For a standalone deployment, these files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. For a load balancer deployment, these files are stored in a key location specified during installation. These files must be copied to the directory from which the ODBC driver installation program will be run. The files are:

- `config.properties`
- `OnPremise.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`

Take the following steps to create a response file using the installer.

1. Download the product installation file into a temporary directory. For example, on a 64-bit machine, the file name is `PROGRESS_DATADIRECT_HDP_ODBC_4.1_WIN_64.exe`.
2. Copy the four configuration and certificate files from the Hybrid Data Pipeline Server installation into the temporary directory with the installer file.
3. At a Windows command prompt, type the following command where *`response_file`* is the path and file name of the response file you want to create. You must specify an absolute path, with the path and file name enclosed in double quotation marks.

   ```
   PROGRESS_DATADIRECT_HDP_ODBC_4.1_WIN_32.exe -r response_file
   ```

   The following example creates a response file named `installer.properties` in the `C:\temp` directory.

   ```
   PROGRESS_DATADIRECT_HDP_ODBC_4.1_WIN_32.exe -r "C:\temp\installer.properties"
   ```

4. Continue the installation at Step 4 in Installing the ODBC driver on Windows on page 171.

See Performing the silent installation on page 174 for instructions on running the response file.

Creating a response file using a text editor

Use a text editor to create a response file with the following contents:

```
#Install Type
#------------
INSTALL_TYPE_STD=true
INSTALL_TYPE_OEM=false

#Install Directory
#-----------------
USER_INSTALL_DIR_GUI_INPUT=C:\\Program Files (x86)\\Progress\\DataDirect\\Hybrid_for_ODBC

#Install Options
#---------------

INSTALL_OPTIONS_CREATE=1

#Install
#-------
\\uninstall\\uninstall_Progress_DataDirect_Hybrid_Driver_for_ODBC=Yes
\\uninstall\\resource\\iawin32.dll=Yes
```

```
\\uninstall\\resource\\win64_32_x64.exe=Yes
\\uninstall\\resource\\remove.exe=Yes
\\install\\installed.properties=Yes
\\install\\tailor.manifest=Yes
\\install\\driver.properties=Yes
```

where:

`CREATEDEF_DS`

specifies whether to create default data sources. Type `1` if you want to create default data sources or `0` if you do not want to create default data sources.

`USER_INSTALL_DIR_GUI_INPUT`

specifies the product installation directory. Notice that the backslash (\) special character must be delimited with a backslash.

See Performing the silent installation on page 174 for instructions on running the response file.

Performing the silent installation

Applications using ODBC to access the Progress DataDirect Hybrid Data Pipeline connectivity service require access to a properly configured Hybrid Data Pipeline Driver *for* ODBC.

During installation of the Hybrid Data Pipeline server, four configuration and certificate files are generated. For a standalone deployment, these files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. For a load balancer deployment, these files are stored in a key location specified during installation. These files must be copied to the directory from which the ODBC driver installation program will be run. The files are:

- `config.properties`
- `OnPremise.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`

On each machine, take the following steps to install the driver.

1. Copy the installer and the response file you created to a temporary directory, for example:

   `C:\temp`

2. Copy the four configuration and certificate files from the Hybrid Data Pipeline Server installation into the temporary directory with the installer and response files.
3. At a command prompt, change to the directory containing the installer and supporting files.
4. Type the following command where *`response_file`* is the path and file name of the response file created in Creating the response file using the installer on page 173 or Creating a response file using a text editor on page 173. You must specify an absolute path, with the path and file name enclosed in double quotation marks.

   ```
   PROGRESS_DATADIRECT_HYBRID_ODBC_4.1_WIN_32.exe -i silent -f "response_file"
   ```

   <The following example performs a silent installation by running a response file named `installer.properties` from the `C:\temp` directory:

```
PROGRESS_DATADIRECT_HYBRID_ODBC_4.1_WIN_32.exe -i silent
-f "C:\temp\installer.properties"
```

5. The installation proceeds without any further intervention or notification.

If you have any problems during installation, refer to ODBC driver installation log files on page 181.

Configuring and Testing an ODBC Data Source on Windows Systems

On Windows systems, you can configure and modify data sources through the ODBC Data Source Administrator, which is available from the Hybrid Data Pipeline Driver *for* ODBC program group. You specify default connection values in the driver's setup dialog box. The ODBC Data Source Administrator stores the values as user or system data sources in the Windows Registry, or as file data sources in a specified location. See the *User's Guide* for detailed information.

Uninstalling the Driver

To uninstall from a Windows machine, select the **Uninstall DataDirect Hybrid Data Pipeline for ODBC** option in the program group. Follow the prompts to uninstall the product.

Installation on UNIX and Linux Systems

DataDirect Hybrid Data Pipeline Driver *for* ODBC is an ODBC API-compliant dynamic link library, referred to in UNIX and Linux as a shared object. The prefix for the 32-bit driver file name is iv. The prefix for the 64-bit driver file name is dd. The driver file names are lowercase and the extension is .so, the standard form for a shared object. For example, the 32-bit Hybrid Data Pipeline driver file name is ivhybrid*nn*.so, where *nn* is the revision number of the driver. On HP-UX PA-RISC only, the extension is .sl, for example, ivhybrid*nn*.sl.

The driver includes a setup program for installing on machines running AIX, HP-UX, Linux, and Oracle Solaris operating systems.

UNIX and Linux system requirements for the ODBC driver

Before you install the Progress® DataDirect® Hybrid Data Pipeline Driver *for* ODBC on a UNIX or Linux system:

- Verify that you have write privileges for the installation directory.
- Verify that your system meets the appropriate driver requirements:
  - 32-bit driver UNIX and Linux system requirements on page 176
  - 64-bit driver UNIX and Linux system requirements on page 177

If running UTF-16 applications in a UNIX or Linux environment, modify the applications as described in UTF-16 Applications on UNIX and Linux on page 178

32-bit driver UNIX and Linux system requirements

If your application was built with 32-bit system libraries, you must use the 32-bit driver. If your application was built with 64-bit system libraries, you must use the 64-bit driver (see 64-bit driver UNIX and Linux system requirements on page 177). For the latest information on supported environments, see the Hybrid Data Pipeline support matrix.

The following sections describe platform-specific requirements for the 32-bit driver.

AIX

- AIX 5L operating system, version 5.3 fixpack 5 and higher, 6.1, and 7.1
- Applications must be compatible with components that were built using Visual Age C++ 6.0.0.0 and the AIX native threading model

HP-UX

- The following processors are supported:
  - PA-RISC
  - Intel Itanium II (IPF)
- The following operating systems are supported:
  - For PA-RISC: HP-UX 11i Versions 2 and 3 (B.11.23 and B.11.31), 11i (B.11.11), and 11
  - For IPF: HP-UX IPF 11i Versions 2 and 3 (B.11.23 and B.11.31)
- For PA-RISC: applications must be compatible with components that were built using HP aC++ 3.30 and the HP-UX 11 native (kernel) threading model (posix draft 10 threads).

  All of the standard 32-bit UNIX drivers are supported on HP PA-RISC.
- For IPF: an application compatible with components that were built using HP aC++ 5.36 and the HP-UX 11 native (kernel) threading model (posix draft 10 threads)

Linux

- The following processors are supported:
  - x86: Intel
  - x64: Intel and AMD
- The following operating systems are supported:
  - CentOS Linux 4.*x*, 5.*x*, 6.*x*, and 7.*x*
  - Debian Linux 7.11, 8.5
  - Oracle Linux 4.*x*, 5.*x*, 6.*x*, and 7.*x*
  - Red Hat Enterprise Linux 4.*x*, 5.*x*, 6.*x*, and 7.*x*
  - SUSE Linux Enterprise Server 10.*x*, 11.*x*, and 12.*x*
  - Ubuntu Linux 14.04, 16.04
- Applications compatible with components that were built using g++ GNU project C++ Compiler version 3.4.6 and the Linux native pthread threading model (Linuxthreads).

Oracle Solaris

- The following processors are supported:
  - Oracle SPARC
  - x86: Intel
  - x64: Intel and AMD
- The following operating systems are supported:
  - For Oracle SPARC: Oracle Solaris 8, 9, and 10
  - For x86/x64: Oracle Solaris 10, Oracle Solaris 11
- For Oracle SPARC: an application compatible with components that were built using Oracle Workshop v. 6 update 2 and the Solaris native (kernel) threading model.
- For x86/x64: an application compatible with components that were built using Oracle C++ 5.8 and the Solaris native (kernel) threading model

64-bit driver UNIX and Linux system requirements

If your application was built with 64-bit system libraries, you must use the 64-bit driver. If your application was built with 32-bit system libraries, you must use the 32-bit driver (see 32-bit driver UNIX and Linux system requirements on page 176). For the latest information on supported environments, see the Hybrid Data Pipeline support matrix.

The following sections describe platform-specific requirements for the 64-bit driver.

AIX

- AIX 5L operating system, version 5.3 fixpack 5 and higher, 6.1, and 7.1
- Applications must be compatible with components that were built using Visual Age C++ version 6.0.0.0 and the AIX native threading model

HP-UX

- Intel Itanium II (IPF) processor
- HP-UX IPF 11i operating system, Versions 2 and 3 (B.11.23 and B.11.31)
- HP aC++ v. 5.36 and the HP-UX 11 native (kernel) threading model (posix draft 10 threads)

Linux

- The following processors are supported:
  - x64: Intel and AMD
- The following operating systems are supported:
  - CentOS Linux 4.x, 5.x, 6.x, and 7.x
  - Debian Linux 7.11, 8.5
  - Oracle Linux 4.x, 5.x, 6.x, and 7.x
  - Red Hat Enterprise Linux 4.x, 5.x, 6.x, and 7.x
  - SUSE Linux Enterprise Server 10.x, 11.x, and 12.x

  - Ubuntu Linux 14.04, 16.04

- Applications must be compatible with components that were built using g++ GNU project C++ Compiler version 3.4 and the Linux native pthread threading model (Linuxthreads)

Oracle Solaris

- The following processors are supported:
  - Oracle SPARC
  - x64: Intel and AMD
- The following operating systems are supported:
  - For Oracle SPARC: Oracle Solaris 8, 9, and 10
  - For x64: Oracle Solaris 10 and Oracle Solaris 11 Express
- For Oracle SPARC: Applications must be compatible with components that were built using Oracle Workshop v. 6 update 2 and the Solaris native (kernel) threading model
- For x64: Applications must be compatible with components that were built using Oracle C++ Compiler version 5.8 and the Solaris native (kernel) threading model

UTF-16 Applications on UNIX and Linux

Because the DataDirect Driver Manager allows applications to use either UTF-8 or UTF-16 Unicode encoding, applications written in UTF-16 for Windows platforms can also be used on UNIX and Linux platforms.

The Driver Manager assumes a default of UTF-8 applications; therefore, two things must occur for it to determine that the application is UTF-16:

- The definition of SQLWCHAR in the ODBC header files must be switched from "char *" to "short *." To do this, the application uses #define SQLWCHARSHORT.
- The application must set the ODBC environment attribute SQL_ATTR_APP_UNICODE_TYPE to a value of SQL_DD_CP_UTF16, for example:

```
rc = SQLSetEnvAttr(*henv, SQL_ATTR_APP_UNICODE_TYPE, (SQLPOINTER)SQL_DD_CP_UTF16,
SQL_IS_INTEGER);
```

Installing the ODBC driver on UNIX and Linux

Applications using ODBC to access the Hybrid Data Pipeline connectivity service require access to a properly configured Hybrid Data Pipeline Driver *for* ODBC.

During installation of the Hybrid Data Pipeline server, four configuration and certificate files are generated. For a standalone deployment, these files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. For a load balancer deployment, these files are stored in a key location specified during installation. These files must be copied to the directory from which the ODBC driver installation program will be run. The files are:

- `config.properties`
- `OnPremise.properties`
- `ddcloud.pem`

- `ddcloudTrustStore.jks`

Take the following steps to install the driver on a local drive.

1. Download the driver installation file to a temporary directory.
2. Copy the four configuration and certificate files from the Hybrid Data Pipeline server installation into the temporary directory with the installer file.
3. From a command-line prompt, navigate to the directory where you saved the driver installation file. Alternatively, place the directory on your path before proceeding to the next step.
4. Make the file an executable using the `chmod` command. Then press **ENTER**. For example:

   ```
   chmod +x ./PROGRESS_DATADIRECT_HDP_ODBC_4.6.0_AIX_64_INSTALL.bin
   ```

5. Run the installer from the command-line prompt. Then press **ENTER**. For example:

   ```
   ./PROGRESS_DATADIRECT_HDP_ODBC_4.6.0_AIX_64_INSTALL.bin
   ```

6. The **Introduction** window opens. Click **Next** to continue.

   Note: You can exit the installation program at any time by clicking **Cancel**, or return to the previous window by clicking **Previous**.

7. Choose the type of installation to perform. Select one of the following options:
   - **Standard Installation**. Select this option to install the standard unbranded version of the driver. Click **Next** to continue with the installation. Continue at the next step.
   - **OEM Installation**. Select this option if you have purchased a licensed version of the product. Refer to the *Progress DataDirect Hybrid Data Pipeline for ODBC Distribution Guide* for information on installing, branding, unlocking, and distributing your branded driver.
8. In the **Where Would You Like to Install?** field, type the path, including the drive letter, of the product installation directory or click the **Choose** button to browse to and select an installation directory. Then click **Next**.

   Verify that you have entered or selected the correct installation directory, and click **Next** to continue.
9. Click **Next**. The **Pre-Installation Summary** window appears.
10. Review the **Pre-Installation Summary** window to confirm the installation setup. Click **Previous** to revise your choices. Click **Install** to proceed with the installation.
11. Click **Done** to exit the installer.

What to do next:

Refer to the *Progress DataDirect Hybrid Data Pipeline User's Guide Release 4.6* for information on creating Hybrid Data Pipeline data sources.

Silent installation of ODBC driver on UNIX and Linux

A silent installation is useful for system administrators who want to install Progress DataDirect Hybrid Data Pipeline Driver *for* ODBC on multiple machines using the same options.

A silent installation requires the following steps:

- Creating the response file as described in Creating a response file on page 180

- Performing the silent installation as described in Performing a silent installation on page 180

Creating a response file

A silent installation response file is a text file that you create, for example, `installer.properties`. This file must contain the arguments described in the following table.

Table 42: Required Arguments for Silent Installations

Argument	Description
`INSTALL_TYPE_STD=true | false`	Specifies whether to perform a standard installation.
`INSTALL_TYPE_OEM=true | false`	Specifies whether the installation is standard or for a OEM installation.
`USER_INSTALL_DIR_GUI_INPUT=`*`installation directory`*	Specifies the full path to the directory where you want to install the drivers. This **cannot** be the same directory as the temporary installation directory. It also cannot be the directory of a previous version of another Progress DataDirect ODBC driver. If the directory you enter does not exist, Setup creates it.

For example, the following response file installs the product in the `/opt/hybridforodbc` directory:

```
INSTALL_TYPE_STD=true
USER_INSTALL_DIR_GUI_INPUT=/opt/hybridforodbc
```

Performing a silent installation

Applications using ODBC to access the Progress DataDirect Hybrid Data Pipeline connectivity service require access to a properly configured Hybrid Data Pipeline Driver *for* ODBC.

During installation of the Hybrid Data Pipeline server, four configuration and certificate files are generated. For a standalone deployment, these files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. For a load balancer deployment, these files are stored in a key location specified during installation. These files must be copied to the directory from which the ODBC driver installation program will be run. The files are:

- `config.properties`
- `OnPremise.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`

On each machine, take the following steps to install the driver.

1. Copy the installer and the response file you created to a temporary directory, for example:

   `/tmp`

2. Copy the four configuration and certificate files from the Hybrid Data Pipeline Server installation into the temporary directory with the installer and response files.
3. At a command prompt, change to the directory containing the installer and supporting files.
4. Execute the following command where *`response_file`* is the path and file name of the response file created in Creating a response file on page 180.

```
installer.bin -i silent -f response_file
```

The following example performs a silent installation by running a response file named `installer.properties` that resides in your home directory:

```
installer.bin -i silent -f /home/users/johndoe/installer.properties
```

5. The installation proceeds without any further user intervention unless you enter an incorrect value on the command line or in the response file, in which case an error is displayed and installation stops. You must correct the command line or silent installation response file and execute it again.

If you have any problems during installation, refer to ODBC driver installation log files on page 181.

Uninstalling the ODBC Driver

You can uninstall the ODBC driver using the graphical user interface.

To uninstall the driver on your local drive:

1. In a shell window, switch to the uninstall directory (`/INSTALLDIR/UNINSTALL`) and select the uninstall executable.
2. At the command line, enter the name of the uninstaller, including the file extension `.bin`. For example, for the 32-bit driver on AIX, enter the following:

   ```
   uninstall_PROGRESS_DATADIRECT_HYBRID_ODBC_-_32.bin
   ```

   The **Introduction** window appears.
3. Follow the prompts to uninstall the product.
4. The uninstall procedure may leave several files, such as your odbc.ini and odbcinst.ini files, in the `/INSTALLDIR` directory. Delete the files and the `/INSTALLDIR` directory.

ODBC driver installation log files

Installation Log Files

If the installer successfully creates the ODBC driver installation directory, the installer writes a log file in the installation directory. Examine the log file for a record of any problems that may have occurred during the installation. The installation log file has the following name:

```
Progress_DataDirect_Hybrid_Data_Pipeline_for_ODBC.log
```

If the installation fails completely, the installer does not create the installation directory and writes a file named `Progress_DataDirect_Hybrid_for_ODBC__InstallFailed.txt` to the machine's default temporary directory (for example, on Windows systems, `%TEMP%`).

If you need help interpreting the contents of these files, contact Progress DataDirect customer support.

Installer Console Log

The installer records standard errors and standard output generated during installation to `HDP_ODBC_install_console.log`, which is created in the user profile directory.

Progress DataDirect customer support might ask for this log file to troubleshoot some installer problems.

4

Installing the Hybrid Data Pipeline Driver for JDBC

You should install the Progress DataDirect Hybrid Data Pipeline Server component before you install the JDBC driver.

For details, see the following topics:

Prerequisites for the JDBC Driver

Before installing the Hybrid Data Pipeline Driver *for* JDBC, the following requirements must be met.

- 21 MB of hard disk space
- A supported JVM must be defined on your system path. The following JVMs are supported.
  - Oracle Java 8 and 11
  - OpenJDK 8 and 11
- Standard installations of Java on some platforms do not include the jar file containing the extended encoding set that is required to support some of the less common database code pages. To verify whether your version of Java provides extended code page support, make sure that the `charsets.jar` file is installed in the `\lib` subdirectory of your Java installation directory. If you do not have the `charsets.jar` file, install the international version of Java.

Installing the JDBC Driver

Applications using JDBC to access the Progress DataDirect Hybrid Data Pipeline connectivity service require access to a properly configured Hybrid Data Pipeline Driver *for* JDBC.

During installation of the Hybrid Data Pipeline server, four configuration and certificate files are generated. For a standalone deployment, these files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. For a load balancer deployment, these files are stored in a key location specified during installation. These files must be copied to the directory from which the JDBC driver installation program will be run. The files are:

- `config.properties`
- `OnPremise.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`

Note: The Java installer can be run on any platform, including Windows; however, if you run the Java installer on Windows, turn off User Account Controls or select a non-system directory as the installation directory. The Windows installer allows you to install the Hybrid Data Pipeline Driver *for* JDBC in the `Program Files` system directory without turning off User Account Controls.

Take the following steps to install the driver.

1. Download the product installation file into a temporary directory.
   - **Windows**: `PROGRESS_DATADIRECT_HDP_JDBC_`*`version`*`_WIN.exe`
   - **Non-Windows**: `PROGRESS_DATADIRECT_HDP_JDBC_`*`version`*`.jar`
2. Copy the four configuration and certificate files from the Hybrid Data Pipeline Server installation into the temporary directory with the installer file.
3. Run the installer.

- **Windows**: Right-click `PROGRESS_DATADIRECT_HDP_JDBC_version_WIN.exe` and select **Run as administrator**.
- **Non-Windows**: Double-click `PROGRESS_DATADIRECT_HDP_JDBC_version.jar`

The **Introduction** window appears.

4. Click **Next**.

   The **Installation Type** window appears.

5. Choose the type of installation to perform. Select one of the following options:

   - **Standard Installation**. Select this option to install the standard unbranded version of the driver. Click `Next` to continue with the installation. Continue at the next step.
   - **OEM Installation**. Select this option if you have purchased a licensed version of the product. Enter your branding key. Then, click `Next` and continue with the next step.

   Note: OEM CUSTOMERS: Refer to the *Distribution Guide for Progress DataDirect Drivers for JDBC* for information on installing, branding, unlocking, and distributing your branded driver.

6. In the **Where Would You Like to Install?** field, click **Choose...** to browse to and select an installation directory or type the path, including the drive letter on Windows machines, of the appropriate directory.
7. Click **Next** to continue.

   Note: If you specify a directory that contains a previous installation of the driver, a warning message appears allowing you to overwrite your existing installation or specify a different installation directory.

8. A window appears allowing you to confirm your installation options. Click **Previous** to revise your choices, or click **Install** to continue with the installation.
9. Click **Done** to exit the installer.

To get started using the driver and for complete information about establishing connections and testing the driver, refer to Configuring Hybrid Data Pipeline for JDBC.

Installing from the command line on UNIX and Linux systems

Applications using JDBC to access the Progress DataDirect Hybrid Data Pipeline connectivity service require access to a properly configured Hybrid Data Pipeline Driver *for* JDBC.

During installation of the Hybrid Data Pipeline server, four configuration and certificate files are generated. For a standalone deployment, these files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. For a load balancer deployment, these files are stored in a key location specified during installation. These files must be copied to the directory from which the JDBC driver installation program will be run. The files are:

- `config.properties`
- `OnPremise.properties`
- `ddcloud.pem`

- ddcloudTrustStore.jks

Note: The Java installer can be run on any platform, including Windows; however, if you run the Java installer on Windows, turn off User Account Controls or select a non-system directory as the installation directory.

Take the following steps to install from a command line.

1. Download the product installation file into a temporary directory.

   Non-Windows installer: PROGRESS_DATADIRECT_HDP_JDBC_*version*.jar

2. Copy the four configuration and certificate files from the Hybrid Data Pipeline Server installation into the temporary directory with the installer file.
3. At a command prompt, type the installation command:

   java -jar PROGRESS_DATADIRECT_HDP_JDBC_*version*.jar -i console

   Press **ENTER**.

   The installer prompts you to answer questions regarding the installation. To accept the default value, press **ENTER**. To return to the previous step, type back and press **ENTER**.

4. The **Introduction** step appears. Press **ENTER**.
5. You are prompted for the installation directory. Enter the full path to the installation directory, or press **ENTER** to accept the default directory.
6. You are prompted to confirm the installation directory. If the installation directory is correct, type **y** and press **ENTER**.

   Note: If you specify a directory that contains a previous installation of the driver, a warning message appears allowing you to overwrite your existing installation or specify a different installation directory.

7. You are prompted to review the product name and installation directory. Press **ENTER** to continue.
8. If the product was successfully installed, a message appears confirming the installation. Press **ENTER** to exit the installer.

To get started using the driver and for complete information about establishing connections and testing the driver, refer to Testing the driver on page 190. If you encounter any issues with installation, see the User's Guide.

Silent installation of JDBC driver

A silent installation is useful for system administrators who want to install Progress DataDirect Hybrid Data Pipeline Driver *for* JDBC on multiple machines using the same options.

A silent installation requires performing the following steps:

- Creating the response file as described in Creating the response file using the installer on page 187 or Creating a response file using a text editor on page 188
- Performing the silent installation as described in Performing the silent installation on page 188

Creating the response file using the installer

Applications using JDBC to access the Progress DataDirect Hybrid Data Pipeline connectivity service require access to a properly configured Hybrid Data Pipeline Driver *for* JDBC.

During installation of the Hybrid Data Pipeline server, four configuration and certificate files are generated. For a standalone deployment, these files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. For a load balancer deployment, these files are stored in a key location specified during installation. These files must be copied to the directory from which the JDBC driver installation program will be run. The files are:

- `config.properties`
- `OnPremise.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`

Note: The Java installer can be run on any platform, including Windows; however, if you run the Java installer on Windows, turn off User Account Controls or select a non-system directory as the installation directory. The Windows installer allows you to install the Hybrid Data Pipeline Driver *for* JDBC in the `Program Files` system directory without turning off User Account Controls.

Take the following steps to create a response file using the installer.

1. Download the product installation file to a temporary directory.
   - **Windows**: `PROGRESS_DATADIRECT_HDP_JDBC_`*`version`*`_WIN.exe`
   - **Non-Windows**: `PROGRESS_DATADIRECT_HDP_JDBC_`*`version`*`.jar`
2. Copy the four configuration and certificate files from the Hybrid Data Pipeline Server installation into the temporary directory with the installer file.
3. At a command prompt, type the following command where *`response_file`* is the path and file name of the response file you want to create. Specify an absolute path. If the path is not specified, the specified file is created in the current working directory.

   ```
   java -jar PROGRESS_DATADIRECT_HDP_JDBC_version.jar -r response_file
   ```

   This example for Windows systems creates a response file named `installer.properties` in the `C:\temp` directory:

   ```
   java -jar PROGRESS_DATADIRECT_HDP_JDBC_version.jar
   -r C:\temp\installer.properties
   ```

   This example for UNIX/Linux systems creates a response file named `installer.properties` in the `/install` directory:

   ```
   java -jar PROGRESS_DATADIRECT_HDP_JDBC_version.jar
   -r ./install/installer.properties
   ```

4. The **Introduction** window appears. Click **Next**.
5. In the **Where Would You Like to Install?** field, type the path, including the drive letter on Windows machines, of the product installation directory or click **Choose (...)** to browse to and select an installation directory.

   Click **Next** to continue.

Note: If you specify a directory that contains a previous installation of the driver, a warning message appears allowing you to overwrite your existing installation or specify a different installation directory.

6. Click **Done** to exit the installer. The response file is created in the directory you specified in Step 3 on page 187.

   See Performing the silent installation on page 188 for instructions on running the response file.

Creating a response file using a text editor

Using a text editor, you can create a response file with the following contents:

```
#Install Folder
#--------------
USER_INSTALL_DIR=install_dir
```

where:

install_dir

is your product installation directory.

Note: If coding a path on Windows to an installation directory using the Universal Naming Convention (UNC), you must escape the double backslash (\\) and the single backslash with a Java escape character. For example: `\\\\server1\\Program Files\\Progress\\DataDirect\\Hybrid_for_JDBC`.

See Performing the silent installation on page 188 for instructions on running the response file.

Windows Example:

```
#Install Folder
#--------------
USER_INSTALL_DIR=C:\\Program Files\\Progress\\DataDirect
\\Hybrid_for_JDBC
```

UNIX/Linux Example:

```
#Install Folder
#--------------
USER_INSTALL_DIR=/opt/Progress/DataDirect/Hybrid_for_JDBC
```

Performing the silent installation

Applications using JDBC to access the Progress DataDirect Hybrid Data Pipeline connectivity service require access to a properly configured Hybrid Data Pipeline Driver *for* JDBC.

During installation of the Hybrid Data Pipeline server, four configuration and certificate files are generated. For a standalone deployment, these files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. For a load balancer deployment, these files are stored in a key location specified during installation. These files must be copied to the directory from which the JDBC driver installation program will be run. The files are:

- `config.properties`

- `OnPremise.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`

Note: The Java installer can be run on any platform, including Windows; however, if you run the Java installer on Windows, turn off User Account Controls or select a non-system directory as the installation directory. The Windows installer allows you to install the Hybrid Data Pipeline Driver *for* JDBC in the `Program Files` system directory without turning off User Account Controls.

On each machine, take the following steps to install the driver.

1. Copy the product installer and the response file you created to a temporary directory.
2. Copy the four configuration and certificate files from the Hybrid Data Pipeline Server installation into the temporary directory with the installer and response files.
3. At a command prompt, change to the directory containing the installer and supporting files.
4. Type the following command where *`response_file`* is the path and file name of the response file created in Creating the response file using the installer on page 187 or Creating a response file using a text editor on page 188.

   - **Windows**: `PROGRESS_DATADIRECT_HDP_JDBC_`*`version`*`_WIN.exe -f` *`response_file`* `-i silent`
   - **Non-Windows**: `java -jar PROGRESS_DATADIRECT_HDP_JDBC_`*`version`*`.jar -f` *`response_file`* `-i silent`

   Note: You can specify an absolute or relative path. If the path is not specified, the silent installation looks for the response file in the current working directory.

   Windows Example:

   This example performs a silent installation by running a response file named `installer.properties` in the `C:\temp` directory.

   ```
   PROGRESS_DATADIRECT_HDP_JDBC_version_WIN.exe -f C:\temp\installer.properties
   -i silent
   ```

   UNIX/Linux Example:

   This example performs a silent installation on AIX by running a response file named `installer.properties` in the `/install` directory, which is relative to the current working directory.

   ```
   java -jar PROGRESS_DATADIRECT_HDP_JDBC_version.jar
   -f /install/installer.properties -i silent
   ```

5. The installation proceeds without any further user intervention or notification.

Refer to the installation log file for a record of any problems that may have occurred during the installation. See JDBC driver installation log files on page 190 for details.

Uninstalling

The procedure for uninstalling depends on which installer you used to install Hybrid Data Pipeline Driver *for* JDBC:

- If you used the Windows installer: Use the Windows **Programs and Features** option to uninstall the product.
- If you used the Java installer: Delete the entire installation directory to uninstall the product.

Testing the driver

To get started using the driver and for complete information about establishing connections and testing the driver, refer to Getting started with the JDBC driver in the *User's Guide*.

JDBC driver installation log files

If the installer successfully creates the product installation directory, the installer writes a file named `Progress_DataDirect_HDP_Driver_for_JDBC.log` in the `install_dir/install/logs` directory. Examine the log file for a record of any problems that may have occurred during the installation.

If a product installation fails completely, the installer does not create the product installation directory and writes a `Progress_DataDirect_HDP_Driver_for_JDBCFailed.txt` file in the machine's default temporary directory.

If you need help interpreting the contents of these files, contact Progress DataDirect technical support.

5

Installing the Hybrid Data Pipeline On-Premises Connector

The Hybrid Data Pipeline On-Premises Connector can be used to access on-premises data stores behind separate firewalls on different networks without having to set up a VPN or other gateway.

To provide access to on-premises data stores, the On-Premises Connector must be installed on a Windows machine behind the firewall where the on-premises data stores are located. When data stores exist at multiple on-premise locations, multiple On-Premises Connectors can be installed and configured to enable access to data stores at each on-premise location.

During installation of the On-Premises Connector, a Hybrid Data Pipeline user ID and password must be provided. The Hybrid Data Pipeline On-Premises Connector uses these credentials to register the On-Premises Connector with Hybrid Data Pipeline.

A valid Hybrid Data Pipeline account must be used to access data stores with the On-Premises Connector. Data stores exposed by the On-Premises Connector are accessed, like any other type of Hybrid Data Pipeline data store, by creating a Hybrid Data Pipeline data source.

For details, see the following topics:

System requirements for the On-Premises Connector

The Hybrid Data Pipeline On-Premises Connector is supported on the following Windows 64-bit operating systems.

- Windows 10
- Windows 8
- Windows 7
- Windows Server 2012
- Windows Server 2008

Before installing the On-Premises Connector

The Hybrid Data Pipeline server must be installed *before* installing the On-Premises Connector.

Take the following steps before proceeding with an installation of the On-Premises Connector.

- Exit or close all applications to prevent file-locking conflicts.
- If you are upgrading an existing installation, stop the On-Premises Connector services before performing the upgrade. To stop the services, from the Windows Start Menu, select **Stop Services** in the On-Premises Connector program group.
- If you are deploying Hybrid Data Pipeline behind a load balancer, configure the load balancer according to the instructions in Load balancer configuration on page 28.
- During installation of the Hybrid Data Pipeline server, four configuration and certificate files are generated. For a standalone deployment, these files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. For a load balancer deployment, these files are stored in a key location specified during installation. These files must be copied to the directory from which the On-Premises Connector installation program will be run. The files are:
  - `config.properties`
  - `OnPremise.properties`
  - `ddcloud.pem`
  - `ddcloudTrustStore.jks`

Installing the On-Premises Connector

The Hybrid Data Pipeline server must be installed *before* the On-Premises Connector can be installed.

During installation of the Hybrid Data Pipeline server, four configuration and certificate files are generated. For a standalone deployment, these files are located in the Hybrid Data Pipeline installation directory `<install_dir>/redist`. For a load balancer deployment, these files are stored in a key location specified during installation. These files must be copied to the directory from which the On-Premises Connector installation program will be run. The files are:

- `config.properties`
- `OnPremise.properties`
- `ddcloud.pem`
- `ddcloudTrustStore.jks`

Note:

- The On-Premises Connector uses an embedded JRE at runtime. However, you can integrate an external JRE during the installation or upgrade of the connector. See also External JRE support and integration on page 42.
- By default, the installation program installs the On-Premises Connector in the `Program Files` system directory. If you are installing the On-Premises Connector in a system directory other than the `Program Files` directory, you must turn off User Account Controls to run the installation program.
- For Microsoft Dynamics CRM Kerberos configurations, see Configuring the Microsoft Dynamics CRM On-Premises data source for Kerberos on page 201.

Take the following steps to proceed with an installation of the Hybrid Data Pipeline On-Premises Connector.

1. Download the On-Premises Connector installation program to a temporary directory on the Windows machine on which you want to install it.
2. Copy the four configuration and certificate files generated during the installation of the Hybrid Data Pipeline server into the same directory from which you will run the On-Premises Connector installation program.
3. Run the installation program.
4. The Introduction window appears. Click **Next** to continue.

   If an existing installation is detected, you will be prompted to choose whether to install a new instance or upgrade an existing instance.

   - If you are installing a new instance of the connector, proceed to Step 5 on page 193.
   - If you are upgrading an instance of the connector, proceed to Step 6 on page 193.

5. In the **Where Would You Like to Install?** field, specify the installation directory. Then click **Next** and skip to Step 7 on page 194.
6. Take the following steps to upgrade a current installation. Then, proceed to Step 13 on page 195.
   a) From the drop down menu, select the installation that you want to upgrade. Then, click **Next**.
   b) Select the desired Java configuration.

   Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

   - Select **Use default Java** if you will be using the embedded JRE installed with the server.
   - Select **Java home directory** and provide the path to an external JRE if you will be using a JRE not installed with the server.

   c) Select whether you will be using a MySQL Community Edition data store.

   - If you are not using a MySQL Community Edition data store, click **Next** and proceed to Step 13 on page 195.

- If you are using a MySQL Community Edition data store, provide the name and location of the MySQL Community Edition driver jar file. Then, click **Next** and proceed to Step 13 on page 195.

Note: You will not be prompted to enter Microsoft CRM or proxy connection settings when performing an upgrade. If these settings need to be changed, you should change them with the On-Premises Configuration Tool.

---

7. Select the desired Java configuration.

Note: Further steps are required to integrate an external JRE. See External JRE support and integration on page 42 for details.

- Select **Use default Java** if you will be using the embedded JRE installed with the server.
- Select **Java home directory** and provide the path to an external JRE if you will be using a JRE not installed with the server.

8. Select the type of installation.
   - If your installation does not need modification, select **Standard** and continue at Step 12 on page 195.
   - If you need to customize the installation, select **Advanced Installation**, and then select one or more of the following options.
     - If you need to enable support for Microsoft Dynamics CRM, select **Microsoft Dynamics CRM**. Continue at Step 9 on page 194.
     - The On-Premises Connector must communicate with the Hybrid Data Pipeline service using the Internet. If your network environment requires a proxy to access the public Internet, select **Proxy Connection** and continue at Step 10 on page 194.
     - If you need to enable support for MySQL Community Edition, select **MySQL Community Edition**. Continue at Step 11 on page 195.

9. Type your user name and password for Microsoft Dynamics CRM. If required for your environment, select the check box and type the path to the Kerberos configuration files that you want to use (see also Configuring the Microsoft Dynamics CRM On-Premises data source for Kerberos on page 201.
   - If you need to configure a proxy connection, click **Next** and continue at Step 10 on page 194.
   - If you are not configuring a proxy connection but plan to connect to a MySQL Community Edition data store, click **Next** and continue at Step 11 on page 195.
   - If you are not configuring a proxy connection and do not plan to connect to a MySQL Community Edition data store, click **Next** and continue at Step 12 on page 195.

10. Provide your proxy connection information and the type of proxy authentication you want to use. (You can change this information later using the Hybrid Data Pipeline On-Premises Connector Configuration Tool.)

    a) Type the proxy connection information.

    Hostname specifies the Host name and, optionally, the domain of the proxy server. The value can be a host name, a fully qualified domain name, or an IPv4 or IPv6 address.

    Port Number specifies port number where the proxy server is listening.

    User Name specifies the user name needed to connect to the proxy server if you are using HTTP Basic or NTLM authentication. If NTLM Proxy Authentication is selected, the user name must be in the form `Domain\User`.

Password specifies the password needed to connect to the proxy server if you are using HTTP Basic or NTLM authentication.

b) From the **Proxy Authentication** drop-down list, select the type of proxy authentication needed in your environment.

- Select **No Proxy Authentication** if your proxy server does not require authentication.
- Select **HTTP Proxy Authentication** if the proxy server requires that all requests be authenticated using the HTTP Basic authentication protocol.
- Select **NTML Proxy Authentication** if the proxy server requires that all requests be authenticated using the NTLM authentication protocol.

c) Proceed to the next appropriate step.

- If you plan to connect to a MySQL Community Edition data store, click **Next** and continue at Step 11 on page 195.
- If you do not plan to connect to a MySQL Community Edition data store, click **Next** and continue at Step 12 on page 195.

11. In the jar path field, provide the name and location of the MySQL Community Edition driver jar file. Then, click **Next**.
12. Provide the user ID and password for your Hybrid Data Pipeline account. If desired, you can change the default connector label. Click **Next**.

    The installation program validates your Hybrid Data Pipeline account credentials.
13. Review the **Pre-Installation Summary** window. To install the connector, click **Install**.
14. Click **Done** to exit the installation program.
15. After the installation program closes, the On-Premises Connector Configuration Tool opens and verifies access to the Hybrid Data Pipeline service.

    - Close the Configuration Tool to complete the installation process.
    - Use the Configuration Tool to further configure the On-Premises Connector. For details, see Configuring the On-Premises Connector on page 195

Configuring the On-Premises Connector

You can use the On-Premises Configuration Tool to change settings you established during the installation process. You may use the Configuration Tool to change the user id and password used to register the On-Premises Connector with Hybrid Data Pipeline, and to change the label used to identify the Connector in the configuration dialogs. The Configuration Tool also allows you to see the Hybrid Data Pipeline Connector ID that is used to register the On-Premises Connector with Hybrid Data Pipeline.

1. Start the On-Premises Configuration Tool by selecting **Windows Start Menu > All Programs > Progress DataDirect Hybrid Data Pipeline On-Premises Connector**. Then select **Configuration Tool**.
2. Enter a name for your On-Premises Connector instance in the **Connector Label** field.
3. Enter your Hybrid Data Pipeline user id and password in their corresponding fields.

4. Click **Save**. This registers the On-Premises Connector to the Hybrid Data Pipeline service.
5. Select the Status tab and click **Test** to verify that the On-Premises Connector configuration is correct.

   All tests should all have a green check mark, showing the test was successful.

Restarting the On-Premises Connector

You must restart the On-Premises Connector whenever any configuration changes are made using the Configuration Tool. Follow these steps to start and restart On-Premises Connector services.

1. Select **Windows Start Menu > All Programs > Progress DataDirect Hybrid Data Pipeline On-Premises Connector**, and select **Stop Services**.
2. After the service is stopped, return to the **Progress DataDirect Hybrid Data Pipeline On-Premises Connector** program group and select **Start Services**.
3. From the **Progress DataDirect Hybrid Data Pipeline On-Premises Connector** program group, select the **Configuration Tool**.
4. Select the Status tab and click **Test** to verify that the On-Premises connector configuration is correct.

Each test should have a green check mark, showing the test was successful. If a red x appears next to any tests, you should reenter the information or see Troubleshooting the On-Premises Connector on page 202 to troubleshoot the issue.

Determining the Connector information

The On-Premises Configuration Tool allows you to see the Hybrid Data Pipeline Connector ID being used to register the On-Premises Connector with Hybrid Data Pipeline. You may also use the Configuration Tool to change the User ID and Password used to register the On-Premises Connector with Hybrid Data Pipeline, and to change the label used to identify the Connector in the configuration dialogs.

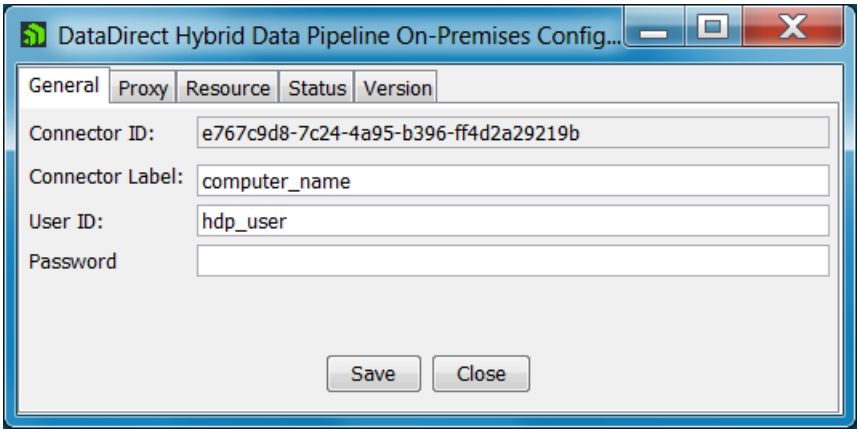
When you configure a Hybrid Data Pipeline data source to connect to an on-premises Data Store such as OpenEdge using the On-Premises Connector, you must select the Connector from a drop-down list.

Note: By default, only the owner of the On-Premises Connector can use the Connector to access data sources behind the firewall. The owner of the On-Premises Connector can grant other Hybrid Data Pipeline users permission to use the Connector. The User ID of the owner of the On-Premises Connector is shown in the User ID field of the General tab in the Configuration Tool. The Hybrid Data Pipeline Management API provides a set of REST calls that allow the owner to manage the list of users that can access the On-Premises Connector. Through the APIs, the owner can add and remove Hybrid Data Pipeline users to the list of users that can use the Connector. See the "Getting Started with Hybrid Data Pipeline" in the user's guide for more information.

---

1. Select **Configuration Tool** in the Hybrid Data Pipeline On-Premises Connector program group. Alternatively, navigate to the directory *`install_dir`*`\OPDH\config` and double-click the `opconfig.bat` file, or type `opconfig` from a command prompt.

   The General tab of the Hybrid Data Pipeline On-Premises Connector Configuration Tool displays the Connector ID and the User ID used when installing the On-Premises Connector.



2. Select the Connector ID string and copy it to a text file that you can refer to when you use the Hybrid Data Pipeline Management APIs.
3. If you want to change the label, which by default is the name of the computer, enter a unique descriptive name in the Connector Label field. The maximum length is 255 characters. This label appears in the Connector ID drop-down list on the configuration dialogs.

   If you have already used the label on another Connector, you are prompted to enter a different label. For example, you might change `Production` to `Production(West)`.
4. If you want to change the User ID and Password that was used to register the On-Premises Connector, enter a valid Progress Id and password in the User ID and Password fields.

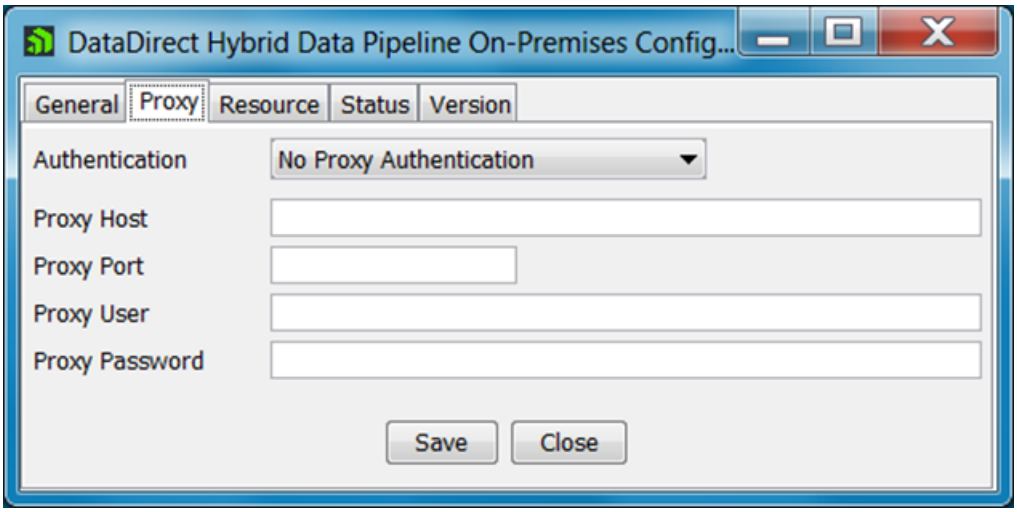
   If the User ID and Password are not valid, a message is returned.
5. Click **Save** to persist your settings, as well as changes on other Configuration Tool tabs. If you save your settings, then close and reopen the Configuration Tool, the saved settings are displayed automatically.
6. Click **Close** to exit the Configuration Tool.

Note: If you uninstall the On-Premises Connector and later re-install it, the Connector ID changes, even if you reuse the Connector label. In this case, you must update any data sources created with the original Connector ID. For each data source, select the label for the newer Connector. If you shared the Connector with other users, make sure that they update their data sources.

Defining the proxy server

The On-Premises Connector must communicate with the Hybrid Data Pipeline service using the Internet. If your network environment requires a proxy to access the public internet, you provide the proxy host name and port on the Proxy tab of the Configuration Tool and specify what type of proxy authentication to use. You might need to contact your network administrator to determine what proxy information you need to provide.

1. Open the Configuration Tool, and click the **Proxy** tab. If you provided the proxy connection information when you installed the Connector, the fields are automatically populated with that information.



2. Select the type of proxy authentication needed in your environment:

   Select **No Proxy Authentication** if the proxy server does not require authentication.

   Select **HTTP Proxy Authentication** if the proxy server requires that all requests be authenticated using the HTTP Basic authentication protocol.

   Select **NTML Proxy Authentication** if the proxy server requires that all requests be authenticated using the NTLM authentication protocol.

3. Provide the connection information for the proxy server. You may need to contact your network administrator for the proxy host name and port number, and if required, the proxy user name and password.

   Proxy Host specifies the Host name and, optionally, the domain of the proxy server. The value can be a host name, a fully qualified domain name, or an IPv4 or IPv6 address.

   Proxy Port specifies port number where the proxy server is listening.

   Proxy User specifies the user name needed to connect to the proxy server, if HTTP or NTLM authentication is specified. If NTLM authentication is specified, the user name must be in the form `domain\user`.

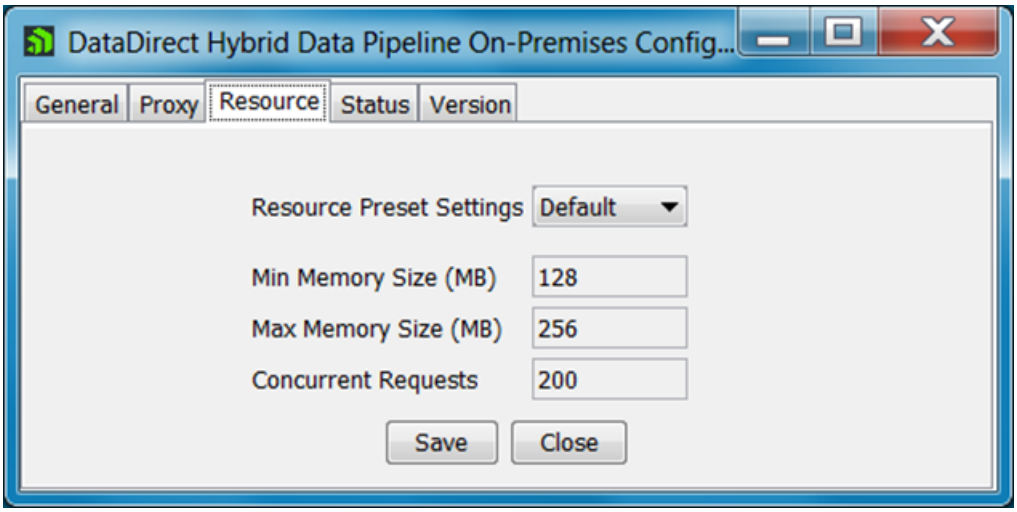
   Proxy Password specifies the password needed to connect to the proxy server, if you are using HTTP Basic or NTLM authentication.

4. Click **Save** to persist your Proxy settings, as well as changes you made on other Configuration Tool tabs. If you save your settings, then close and reopen the Configuration tool, the saved settings are automatically repopulated.
5. Click **Close** to exit the Configuration Tool.

Configuring On-Premises Connector memory resources

In most cases, the default memory allocated to the On-Premises Connector is sufficient, allowing for a small number of open connections and simultaneous requests. However, depending on the number and complexity of concurrent requests in your environment, you might need to increase the memory allocated to the On-Premises Connector, the number of concurrent request it can process, or both, to handle the query volume. If the memory allocation and concurrent request settings are at the high end of the range, you might want to consider using multiple On-Premises Connectors and configure load balancing to share the load between the Connectors.

1. Open the Configuration Tool, and click the **Resource** tab.



2. Select a preset memory load from the dropdown list, or specify custom values. The default resource settings are sufficient for most On-Premises Connector installations, allowing for a small number of open connections and simultaneous requests. Note that because the values for the High and Very High settings exceed the limits of a 32-bit Windows platform, they are not available when using the On-Premises Connector on a 32-bit inmachine.

   Min Memory Size (MB) specifies the minimum number of megabytes used by the On-Premises Connector's JVM. It must be less than or equal to the the Max Memory Size. The valid range is 128 to 16384.

   Max Memory Size (MB) specifies the maximum number of megabytes used by the On-Premises Connector's JVM. Be sure that your system has at least this much memory available for use by the Connector. The valid range is 256 to 16384.

   Concurrent Requests specifies the maximum number of concurrent requests, such as login and execute, that are supported. The valid range is 50 to 1000.

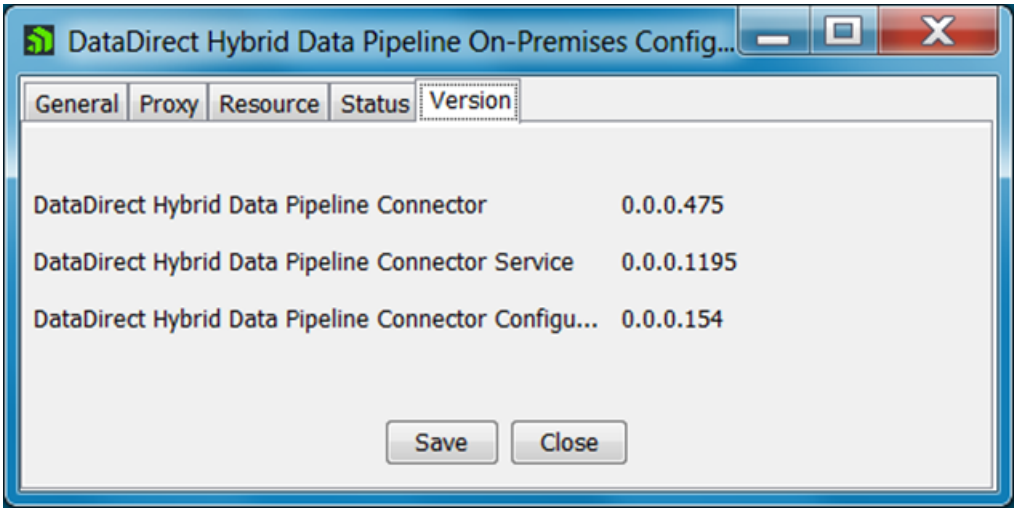
Memory Load	Minimum Memory Size (MB)	Maximum Memory Size (MB)	Concurrent Requests
Default	128	256	200
Moderate	2048	2048	500
High	4096	4096	800
Very High	8192	8192	1000
Custom	8192	8192	1000

3. Click **Save** to persist your settings on this and other Configuration Tool tabs. If you save your settings, then close and reopen the Configuration tool, the saved settings are displayed automatically.
4. Click **Close** to exit the Configuration Tool.

Determining the version

The Version tab shows the versions of the Hybrid Data Pipeline connectivity service and components of the On-Premises Connector.

1. Open the Configuration Tool, and click the **Version** tab.



2. When requested, provide this information to Progress Hybrid Data Pipeline technical support.
3. Click **Save** to persist your settings on other Configuration Tool tabs. If you save your settings, then close and reopen the Configuration tool, the saved settings are displayed automatically.
4. Click **Close** to exit the Configuration Tool.

Checking the configuration status

Use the Status tab of the On-Premises Connector Configuration Tool to determine whether the On-Premises Connector is configured correctly. When you click **Test**, connections are made to the different services used by the On-Premises connector. (Because the proxy password value is encrypted when added to the Configuration Tool, you are prompted to re-enter your Proxy Password when you click **Test**.) The On-Premises Connector is configured properly if a green check is shown next to each service. Click **Details** for additional status information. If a red **x** is shown next to any service, see the table in Troubleshooting the On-Premises Connector on page 202 or contact Progress Technical Support.

Configuring failover and balancing requests across multiple On-Premises Connectors

Hybrid Data Pipeline supports failover and balancing the load of requests across multiple On-Premises Connectors.

You can use the Hybrid Data Pipeline Connector API to configure failover across multiple On-Premises Connectors. If a request to a specific On-Premises Connector fails and the connectors are configured for failover, the failed request will be retried on another On-Premises Connector.

You can also use the Connector API to balance the load of requests across multiple On-Premises Connectors. This allows more traffic to be directed to a specific connector if needed. For example, if Connector1 is running on a faster server than Connector2, a higher number of requests can be sent to Connector1.

See Hybrid Data Pipeline Connector API for additional information.

Configuring the Microsoft Dynamics CRM On-Premises data source for Kerberos

During installation of the On-Premises Connector, the files required for Kerberos authentication are installed in the `\jre\lib\security` subdirectory of your product installation directory:

- krb5.conf is a Kerberos configuration file containing values for the Kerberos realm and the KDC name for that realm. You must modify the generic file that is installed for your environment.
- JDBCDriverLogin.conf file is a configuration file that specifies which Java Authentication and Authorization Service (JAAS) login module to use for Kerberos authentication. This file loads automatically unless the java.security.auth.login.config system property is set to load another login configuration file. You can edit this file, but the On-Premises Connector must be able to find the JDBC_DRIVER_01 entry to configure the JAAS login module. Refer to your J2SE documentation for information about setting options in this file.

Note: You must download the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for JDK/JRE 7 at http://www.oracle.com/technetwork/java/javase/downloads/index.html. Unzip the files into the `\jre\lib\security` subdirectory of your product installation directory.

To configure the On-Premises Connector for Microsoft Dynamics CRM:

1. Set the AuthenticationMethod property to `kerberos`.
2. Modify the krb5.conf file to contain your Kerberos realm name and the KDC name for that Kerberos realm by editing the file with a text editor. Alternatively, you can specifying the system properties, java.security.krb5.realm and java.security.krb5.kdc. You may need to contact your network administrator for the Kerberos realm name and KDC name.

   Note: If using Windows Active Directory, the Kerberos realm name is the Windows domain name and the KDC name is the Windows domain controller name.

   For example, if your Kerberos realm name is XYZ.COM and your KDC name is kdc1, your krb5.conf file would look like this:

   ```
   [libdefaults]
   default_realm = XYZ.COM

   [realms]
   XYZ.COM = {
   kdc = kdc1
   }
   ```

   If the krb5.conf file does not contain a valid Kerberos realm and KDC name, the following exception is thrown:

   ```
   Message:[DataDirect][JDBC Cloud Driver][Microsoft Dynamics CRM]Could not establish a
   connection using
   integrated security: No valid credentials provided
   ```

   The krb5.conf file loads automatically unless the java.security.krb5.conf system property is set to load another Kerberos configuration file.

Troubleshooting the On-Premises Connector

Use the Status tab of the On-Premises Connector Configuration Tool to determine whether the On-Premises Connector is configured correctly. When you click **Test**, connections are made to the different services used by the On-Premises Connector. The On-Premises Connector is configured properly if a green check is shown next to each service. If a red **x** is shown next to any service, see the troubleshooting table below or contact Progress Technical Support. Click **Details** for additional status information.

The following table can be used to help troubleshoot configuration properties. If a red x is shown next to a service, see the recommendations for that service for possible actions to correct the problem. Then, click **Test** again. If the recommended actions do not correct the problem, contact Progress Technical Support.

If changes were made to correct any configuration problems, click **Save** to save the changes, and then click **Test** to recheck the status.

Service	Recommended Actions
Cloud Service	Does your network environment require a Proxy? If so, verify that the Proxy connection information is specified correctly on the Proxy Tab of the Configuration Tool.
Notification Service	Is the User Id and Password for the On-Premises Connector correct? The user name and password should be your Progress ID and password. You can change the connector user id and password in the On-Premises Connector Configuration Tool.
On-Premise Access Service	Does your network environment require a proxy? If so, verify that the Proxy connection information is specified correctly on the Proxy Tab of the Configuration Tool.
Connector Service	Are the On-Premises Connector services running on this client machine? The On-Premises Connector services can be started by selecting the **Start Services** item under the Progress DataDirect Hybrid Data Pipeline On-Premises Connector folder in the Start Menu.

Uninstalling the On-Premises Connector

You can uninstall the product through the **Uninstall DataDirect Hybrid Data Pipeline On-Premises Connector** option in the DataDirect program group, or through the **Add/Remove Programs** feature in the Windows Control Panel.

If multiple On-Premises Connectors have been installed, each Connector must be uninstalled separately. Uninstalling one Connector has no effect on the other installed Connectors.