



TM-Parcel Fresh Installation Guide

February 2024

Copyright © 2024 e2open, LLC. All rights reserved. CONFIDENTIAL.

This document is confidential information of e2open, LLC. You may not reproduce, disclose, or distribute any part of this document in any form or by any means, without the written permission of e2open, LLC, nor may you use it to create derivative works.

E2open and the e2open logo are registered trademarks of e2open, LLC. Other product or company names may be the trademarks of their respective owners.

Use of e2open, LLC software is subject to the terms of a master services agreement and applicable export and import restrictions. Restricted rights of U.S. government users.

This documentation may contain links to external websites that e2open does not own or control. E2open neither evaluates nor guarantees the availability of these websites.

Table of Contents

Introduction	5
Hardware and Software Requirements	8
Additional Hardware Considerations	9
Ports.....	10
Pre-requisites	10
Installing Parcel	11
Overview of Installation	11
Before you begin Parcel Installation	11
Complete Installation	11
Performing a Fresh Installation	11
Installing MySQL Server	19
Installing MySQL Connector/ODBC 64bit.....	26
Installing MySQL Connector/ODBC 32bit.....	29
Installing Parcel in a Distributed Environment.....	43
Installing Parcel on the Application Server	43
Installing Parcel DB on Aurora Server.....	44
Installing MySQL on Remote Server	44
Installing MySQL Connector/ODBC on Remote Server	45
Installing Parcel DB on Remote Server.....	45
Connecting Remotely to Database	47
Post Installation Steps.....	55
Configuring HTTPS Certificate on Apache Server	55
Enabling HTTPS on IIS Server	56
Configuring HTTPS Certificate for UCM.....	59
Configuring 64bit DSN	59
Accessing the Parcel Application	60
Registering Parcel.....	60
Importing UPS World Wide Validation Data	62
Add/Update Virtual Directory in IIS.....	63
Additional Optional Steps.....	69
Configuring an External Database	69
Using Batch Files to Run Scripts.....	70

Customizing Installation batch file for Oracle.....	71
Configuring LDAP User Authentication.....	85
Configuring LDAP with Parcel.....	85
Purge Utility.....	89
Supporting UCM Integration on HTTPS.....	93
Converting UCM from HTTPS to HTTP.....	93
Parcel Data Upload.....	94
Modifying parcel-data-upload-config.properties file.....	94
Installing and Starting the SOR Updater Windows Service.....	94
Converting Parcel from HTTPS to HTTP on Apache Server.....	96
Configuring Stunnel Settings for Encryption of Data in Motion.....	97
Configuring the Stunnel Settings in Client Machine.....	97
Configuring the Stunnel Settings in Server Machine.....	98
Encryption of Stored Data.....	99
Configuring Transparent Data Encryption in MySQL Server.....	99
Configuring Transparent Data Encryption in MSSQL Server.....	101
Configure Encrypted Connections to Database.....	104
Configuring MySQL to Use Encrypted Connection.....	104
Configuring the Application (Modules) to Use Encrypted Connections to the Databases – MySQL.....	105
Creating and Importing Truststore.....	109
Creating and Importing Client Keystore.....	111
Configuring SSL Settings in MySQL Connector/ODBC.....	112
Generating a Self-Signed SSL Certificate using OpenSSL.....	115
Configuring MSSQL to Use Encrypted Connection.....	116
Enabling Encryption at the MSSQL.....	117
Configuring the Application (Modules) to Use Encrypted Connections to the Databases – MSSQL.....	118
Generating a Keystore and Truststore.....	120
Configuring SSL Settings in MSSQL.....	122
Adding DSN for MSSQL Database Connection.....	122
Configuring Oracle to Use Encrypted Connection.....	128
Configuring Database to Use TCPS with Server Key.....	129
Configuring the Application (Modules) to Use Encrypted Connections to the Databases – Oracle.....	132
Configuring SSL DSN Settings in Oracle.....	134
Configure Edge in IE Mode.....	135

Change Log On user for all Kewill / BluJay Services	136
Changing Parcel Artifact Folder Location	136
Supporting UMS and E2Proxy Integration	138
Configuring IIS 10.0 on Windows Server 2019	140
Installing IIS 10.0.....	140
Printer Configuration on Windows 2019	148
Configuring PHP for IIS 10.0	148
Configuring the PHP.INI File.....	148
Configuring Bindings	151
Disabling Weak SSL Cipher Suites in IIS	153
Disabling Weak SSL Protocol in IIS	156
Additional Setup Tasks	157
Configuring a Connector/ODBC DSN for 32-bit Windows.....	157
Editing the php.ini File	158
Resetting the Login Timeout	159
Configuring Parcel with UTF-8 Support.....	159
Modifying SOR and IDATA database settings for UTF-8.....	161
Microsoft SQL Server SOR and IDATA settings for UTF-8.....	161
Troubleshooting	162
Database Errors with Port Blocking	163
DB Upgrade Problems with configuration.xml File	164
Log File Rollover Problems	164
Services Starting Problems	165
Uninstalling Parcel	165
Printing Reports	166
Installing MySQL on different drive	166
Glossary	177

Introduction

Notes on This Parcel Platform, Filenames, Path names, and Windows Service Names. When installing this version of Parcel, please keep the following considerations in mind:

- E2open LLC. represents a rebranding of BluJay Solutions and Kewill, Inc. E2open Parcel now includes the platform formerly named Flagship.
- Currently, *Parcel platform updates in this regard apply only to the product name and logo as they appear on the Parcel user interface, as well as references in Parcel documentation.* Most Folder names, filenames and Windows Service names currently still bear the BluJay Solutions, Kewill and/or Flagship label. These are to be updated in future releases to reflect the Parcel rebranding.

Note

The standard path for Parcel is C:\Program Files (x86)\Kewill\Flagship. If you are installing in different path, you need to refer to that path, wherever the installation path is preferred.

This guide also contains sections on uninstalling Parcel and troubleshooting your Parcel installation.

The following sections describe the Parcel Components, Third Party Applications, and Programs that are installed and configured during the installation process.

Parcel Components

Parcel User Interface (Client UI)	Matches the version of Parcel you are installing	Combination browser-based shipping application and Web Admin (carrier configuration) tool for setting up locations and carriers.
DIServer	Matches the version of Parcel you are installing	Required to run Parcel. Processes shipments and maintains the Parcel databases.
Interface Adapter	Matches the version of Parcel you are installing	Facilitates integration of customers' host applications with Parcel. The Interface Adapter (IA) Server is deployed as a Windows Service. Also known as Integration Adapter/Connect.

Third Party Applications Required by Parcel

Parcel is installed using a standard Installation Wizard program. Depending on the selections you make in the process, in addition to the Parcel Browser-based User Interface, DIServer, and Integration Adapter (Connect), and Windows services, the

Installation Wizard includes several third-party components needed to run Parcel. The following table lists and describes the third-party applications required by Parcel.

Note: In the following table of applications an asterisk (*) indicates an application for which another application may be substituted:

Third Party Application	Version	Notes
* Apache HTTP Server	2.4.57	<p>*Alternatively, you can use Microsoft Internet Information Services (IIS) as your Web Server. If you choose IIS, you must configure IIS previously to installing Parcel. In this case, the Wizard detects the presence of IIS and allows you to bypass the Apache installation.</p> <p>Note: If you prefer to use a different Web Server than either Apache or IIS, you must contact Technical Support for instructions before installing Parcel.</p>
Microsoft .NET Framework	4.0	Parcel is a Web-based application that uses Microsoft .NET Framework. The Parcel Installation Wizard checks to determine whether Microsoft .NET 4.0 is installed on the computer where Parcel is being installed and, if not, automatically installs and registers .NET 4.0 before proceeding with the installation.
MySQL Server database application	8.0.32	Required by carrier compliance engines and Business Rules modules.
MySQL Connector/ODBC Driver	8.0.33	Required by MySQL ODBC connector for following: <ul style="list-style-type: none"> • 34bit • 64bit
PHP	8.2.7	Required to view the Parcel user interface.
Windows Services	N/A	These include services such as: <ul style="list-style-type: none"> • STunnel (needed to upload files to UPS) • Tracking service for tracking all packages • Notification service for sending and receiving shipment notification emails • Scheduler service for scheduling systems tasks
Java Run-time Environment (JRE)	1.8.0_92	This is JRE v. 8, required for the Jasper reporting tool. Java is installed in the Parcel directory only. It does not have any impact on any existing customer applications.
FedEx Ship Manager® Server	20.x	The FedEx Ship Manager® Server must be installed separately and runs independently from Parcel, although data is passed from and to Parcel.

Note on Third Party Applications with Parcel

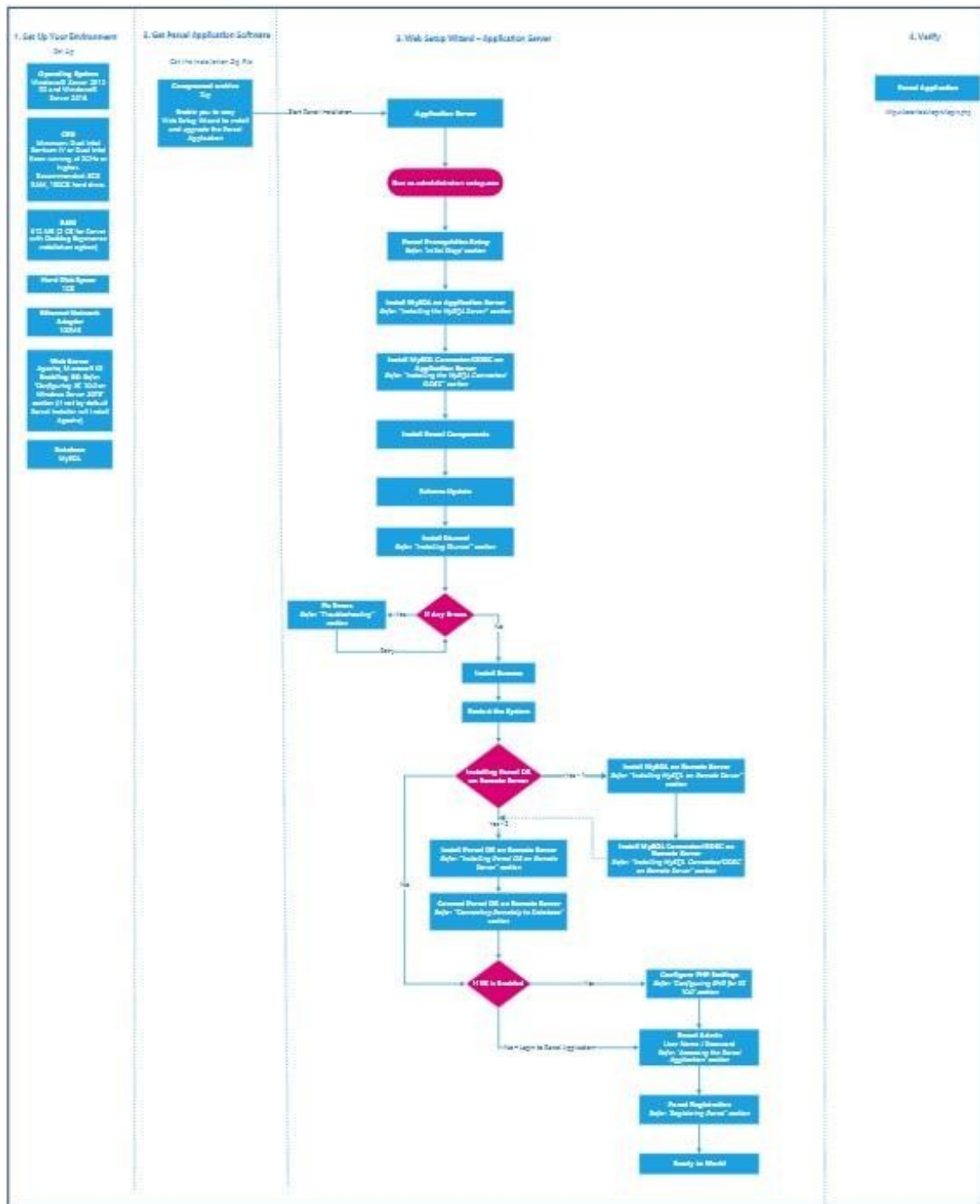
The following third party applications are embedded with Parcel when you run the Parcel Installer:

- Apache (if you choose Apache as your Web server – see the following note)
- Java Run-time Environment (JRE)
- MySQL
- MySQL connector
- PHP and the PHP engine

This embedding means that the process of installing Parcel controls the version of these applications. This embedding also means that these applications cannot be used independently or separately outside of Parcel. Additionally, because Parcel relies on the specific versions (see previous table) and locations of these applications configured during the Parcel installation, you cannot independently upgrade or change versions for these third party applications and you cannot change their locations. Such modifications can introduce changes that disable the automated upgrades of Parcel or introduce hard-to-trace issues in Parcel itself. A partial exception to this rule is the MySQL connector, which can be used to create new connections to other MySQL databases. However, you should never independently install another version of the MySQL connector on the Application Server. **Notes:**

- If you choose IIS as a Web server, this application is not embedded.
- You can install additional instances with other versions of MySQL for other purposes such as reporting, analysis, etc., including for the Parcel SOR database. However, you cannot "repurpose" the MySQL instance used for the didb database.
- The FedEx Ship Manager® Server must be installed separately and runs independently from Parcel, although data is passed from and to Parcel. (See the following section.)

Navigation Chart of Parcel Installation in Distributed Environment.



Hardware and Software Requirements

The following table shows the minimum hardware and software requirements that must be in place before installing the Parcel application and Application Server. In addition, below the table, please note the ports that must be open for Parcel to work correctly and

the additional deployment attributes that will affect the hardware requirements listed after the following table.

Component	Server	Workstations
Operating Systems	Windows® Server 2019 and Windows® Server 2022	Windows® 10
CPU	Minimum: Dual Intel Pentium IV or Dual Intel Xeon running at 2GHz or higher. Recommended: 8GB RAM, 100GB hard drive.	Single Intel Pentium running at 700 MHz
RAM	512 MB (2 GB for Server with Desktop Experience installation option)	512 MB (2 GB for Server with Desktop Experience installation option)
Hard Disk Space	32 GB (Drive should be mirrored)	1 GB
Ethernet Network Adapter	100 MB	100 MB
Internet connection	Full-time direct connection to allow FTP of data files to carriers	N/A
Web browser	Microsoft Internet Explorer Version 11 Edge in IE mode Chrome	Microsoft Internet Explorer Version 11 Edge in IE mode Chrome
Report viewer	None required	Adobe Acrobat Reader (required by the Jasper reporting tool which is used to view reports in Parcel).

Additional Hardware Considerations

The minimum hardware configuration listed in the previous table is sufficient for basic daily shipment transaction volumes of up to 25,000 packages per day. However, the following additional customer deployment attributes will affect hardware requirements:

- Peak transaction volumes in excess of 25,000 packages per day.
- Use of Pre-Ship (PSHP) and Confirm Ship (CSHP) workflows.
- Use of the Configurable Business Rules Module and the related Orchestration Layer.
- Universal Carrier Module (UCM) development environments (clients).
- System of Record (SOR) database topology and database type (MySQL, MS SQL, or Oracle).
- Required performance characteristics.

Prior to obtaining the required hardware for installing and operating your Parcel system, please consult BluJay Solution's Profession Services team for specific hardware recommendations based on your specific requirements.

Note: If you are also using the FedEx Ship Manage Server® (FSMS) in conjunction with your Parcel system, please refer to the FedEx hardware and software requirements for the current required version.

Ports

In order for Parcel to function properly, the following ports must be open to accept requests.

Port	Usage
80	Microsoft Internet Information Services (IIS) or Apache HTTP Server
135	Microsoft DCE Locator Service (end-point mapper) - required by Windows Server
1028	Isass.exe (Local Security Authentication Server) - required by Windows Server
1200	DIServer_Svc.exe (Kewill DI Server service)
3306	mysqld-nt.exe (MySQL)
4010	Stunnel.exe (Universal SSL wrapper)
4011	Stunnel.exe (Universal SSL wrapper)
8101	Orchestration Layer
6789, 8102	Universal Carrier Module
8103	Configurable Business Rules Module
10001	Tracking Service
23000	Scheduler Service

Pre-requisites

As Parcel and other modules supports storing the Parcel Artifacts to remote folder location for secured storage and if user prefer to configure remote folder location using either network or mapped drive then user need to ensure that they have full access to the configured remote folder location.

Below are the minimum access permissions required for remote folder location to install Parcel Application.

1. Full access to Domain Computers.
2. Full access to the User, who is installing Parcel in the Application Server. **Notes:**
 - Please ensure configured remote location exists before initiating Parcel Application and it should have all required permissions.
 - Windows services by default run with windows system account privileges. To provide access to System user, we need to provide full access to Domain Computers.

Installing Parcel

Overview of Installation

Before you begin Parcel Installation

The initial steps of the Parcel Installation Wizard include the following:

- Selecting a destination folder to install Parcel.
- Selecting an installation type: Complete or Custom.
- Detecting the existence of a Web Server (Apache or IIS).
- Selecting where to install the MySQL Server (local computer or a separate computer)

Note

Before starting the Installation Wizard, you can save time by determining in advance which of the following Web servers you want to use with Parcel, and whether one or both of these Web servers is already installed on your system.

Apache – The Parcel installation program installs this Web server if one does not already exist.

Microsoft IIS – You must install this Web service yourself. See the Microsoft Web site for details. The IIS Web server also requires additional configuration to work with Parcel: If you are using windows 2019 or IIS web server, please follow the steps described in the Configuring IIS 10.0 on Windows Server 2019 section.

Complete Installation

Performing a Fresh Installation

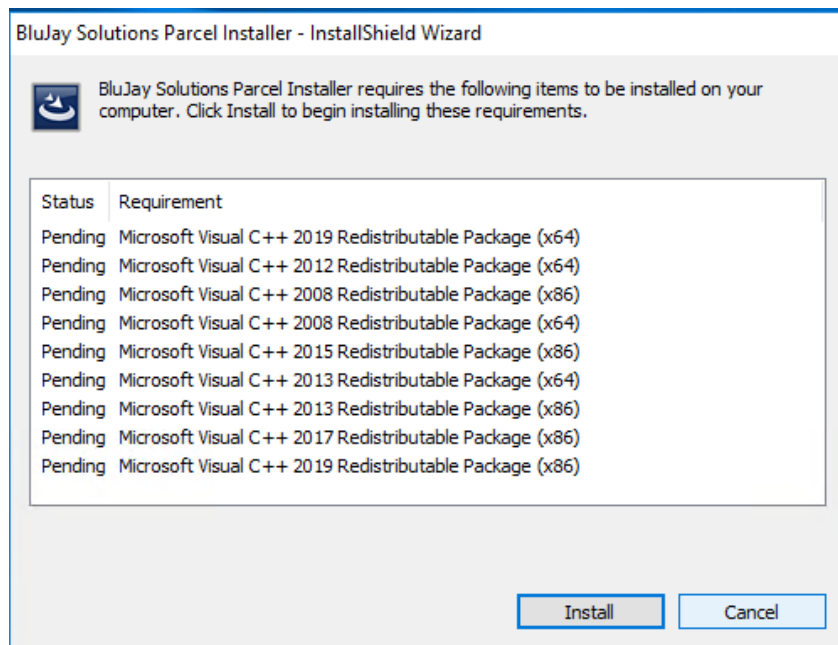
To begin installing Parcel, follow these steps:

1. Download Parcel from the BluJay Solutions FTP site and extract the contents from the installation zip file to a local system.
2. Navigate to extracted folder, right click on setup.exe from the Pop-up menu.
3. Select 'Run as administrator'.

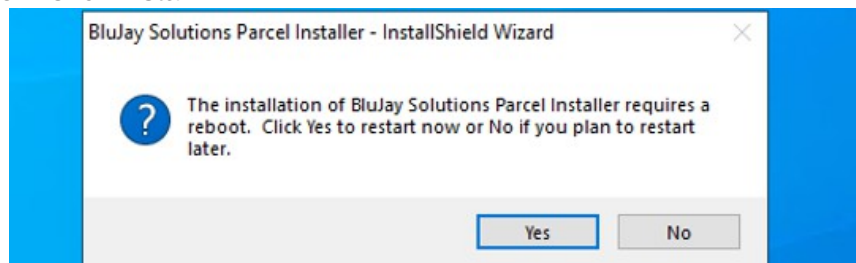
Note

Ensure that installer path to the setup.exe file should not contain spaces. The Parcel Installation Setup Wizard guides you through the steps to install all the Parcel components.

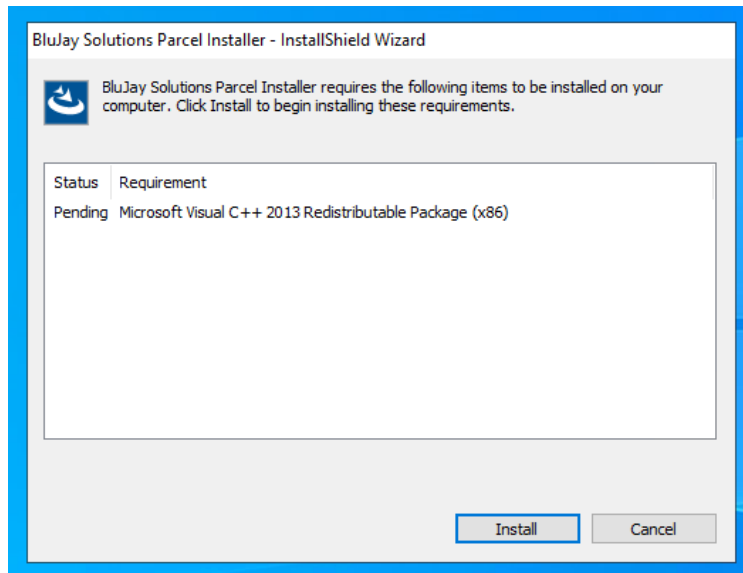
4. If the Parcel Installation Setup Wizard has not already started, double-click the setup.exe file in the folder. The Installer checks to see if the computer where you are installing Parcel 24.1.0 has the required Microsoft Visual C++ redistributables. If it is not installed the installer displays the following screen:



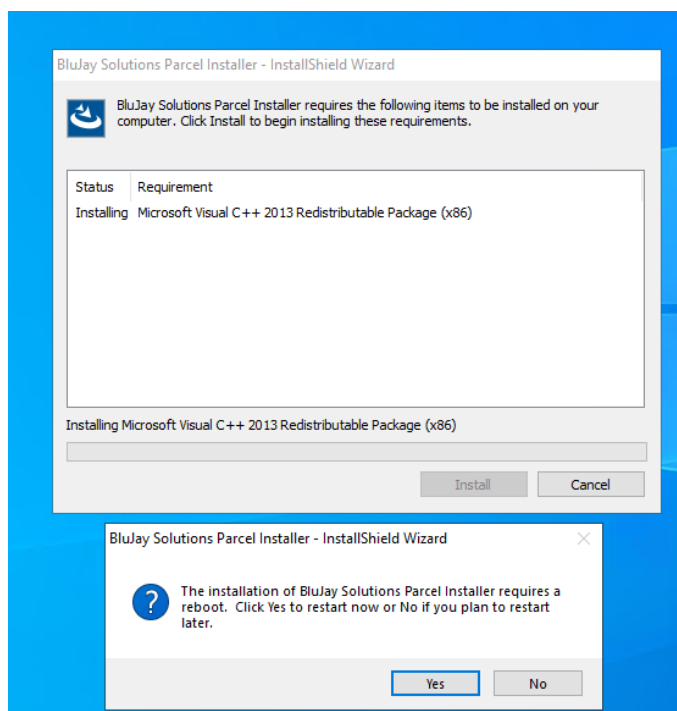
5. Click Install.



Click [Yes]. The parcel server will reboot.
After parcel server is rebooted, the following screen will be shown.

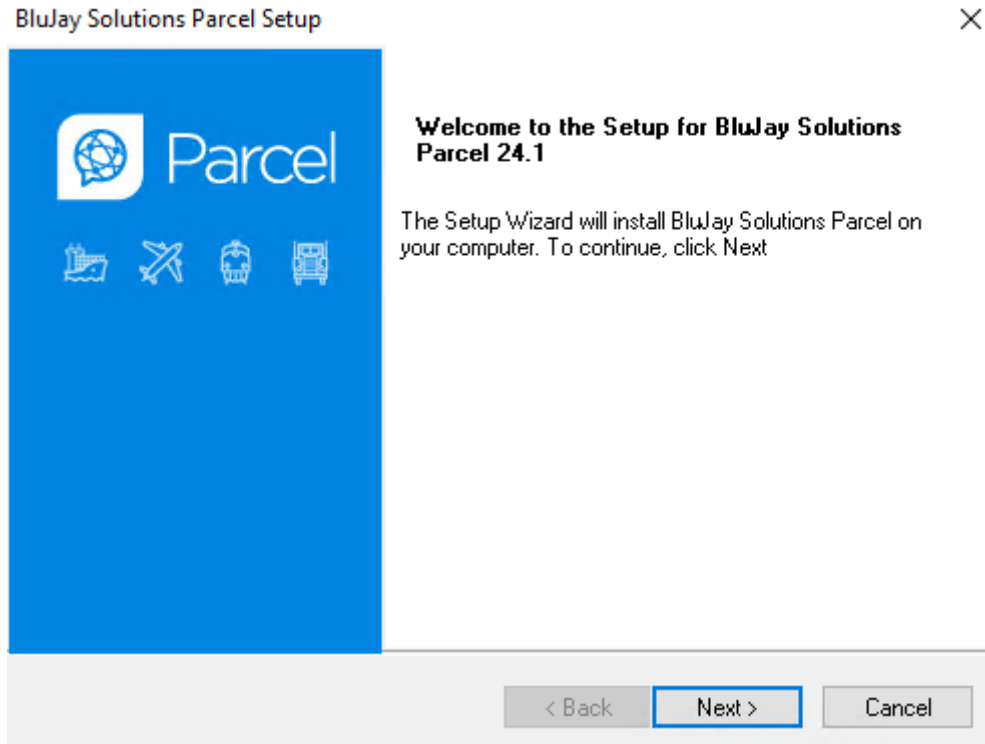


Click [Install].



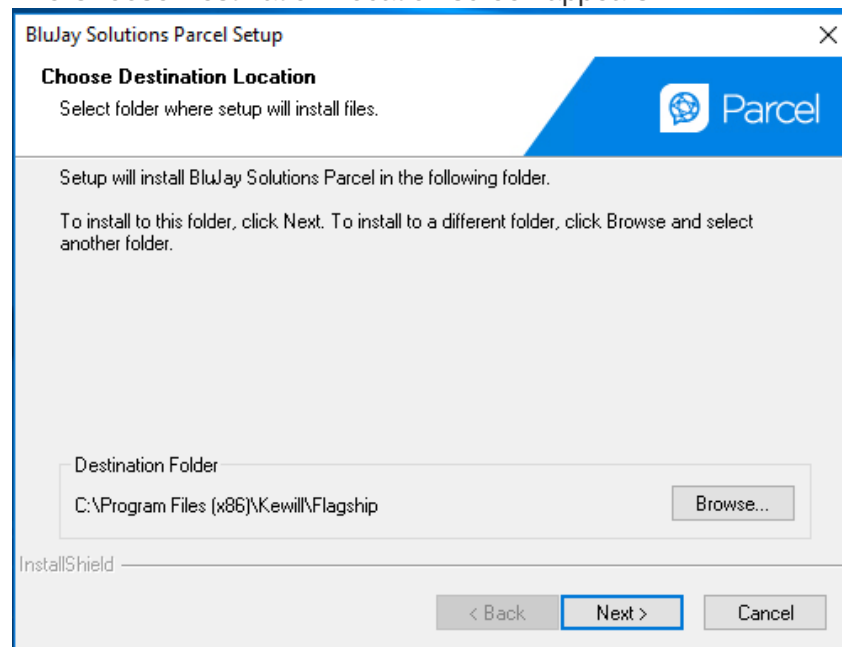
It will ask parcel server restart again, click Yes.

After parcel server is rebooted, the following Welcome wizard screen will be shown



6. Click Next.

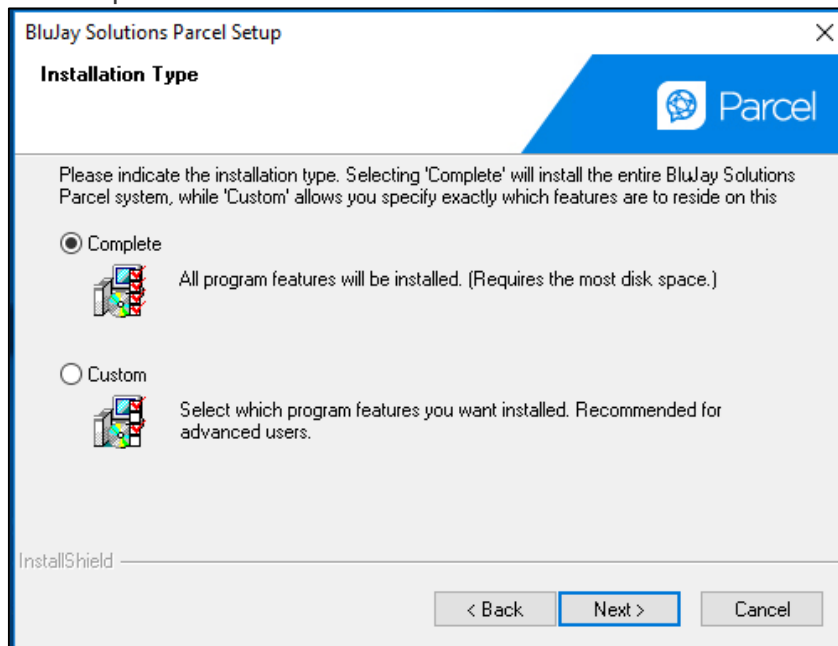
The Choose Destination Location screen appears.



On the Choose Destination Location screen, review the Destination Folder location. If you want to install the Parcel Application somewhere else, click Browse and select the location. On the next screen of the wizard, you will choose which of the Parcel components you want to install on this computer.

7. Click Next.

The Installation Type screen appears. On the Installation Type screen, select Complete and then click Next.



Installation Type	Description
Complete	Install all Parcel components. <i>Note:</i> All of the Parcel components (DIServer, User Interface, and Interface Adapter) are installed on the same computer as the one on which you are running the Installation Wizard. To install the DIServer on a different machine from the client, you need to select Custom installation run the Installation Wizard on that machine.

Custom	<p>Choose which Parcel components you want to install. You can choose whether you want to install the User Interface, DIServer, and Demo scripts.</p> <p><i>Notes:</i></p> <ul style="list-style-type: none"> • If you select Demo Scripts, the DIServer is selected automatically (because the demo scripts require the DIServer on the same machine). • You must install the DIServer either on this machine or on a different machine. (You can install the DIServer and the User Interface on separate computers.
--------	---

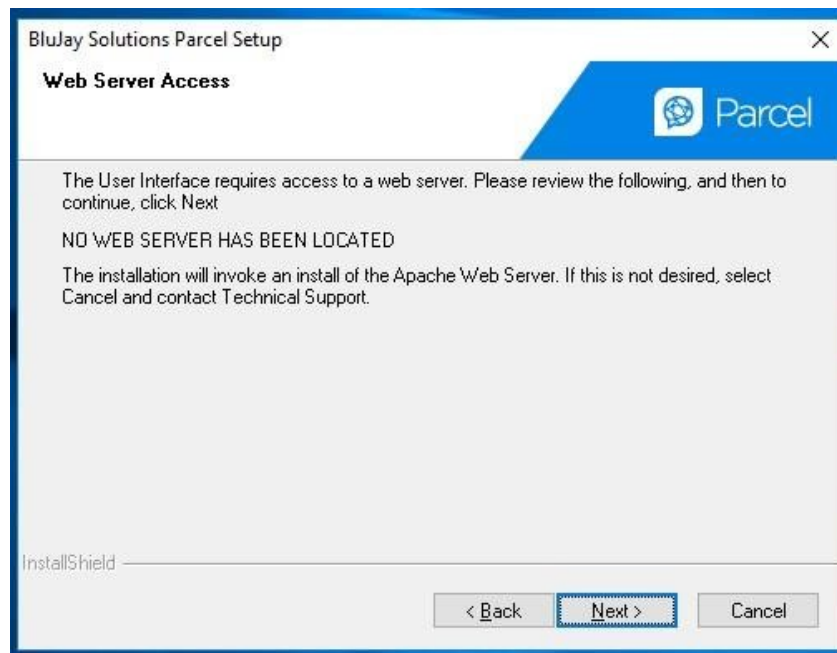
The installation program looks for a Web Server on your computer and responds as follows:

If an existing Apache HTTP Server is detected, the Installation Wizard returns a message that it found an Apache Web Server and asks if you wish to use this existing Apache Web Server as the Web Server for Parcel. If so, click Next to continue.

If Microsoft IIS is detected, the Installation Wizard returns a message that it found IIS. If you want to use IIS as the Web Server for Parcel, click Next to continue. If you do not want to use IIS for the Web server and wish to install Apache instead, you must first exit the Parcel Installation Wizard, stop the World Wide Web Publishing service and the IIS Admin service, and then restart the Installation

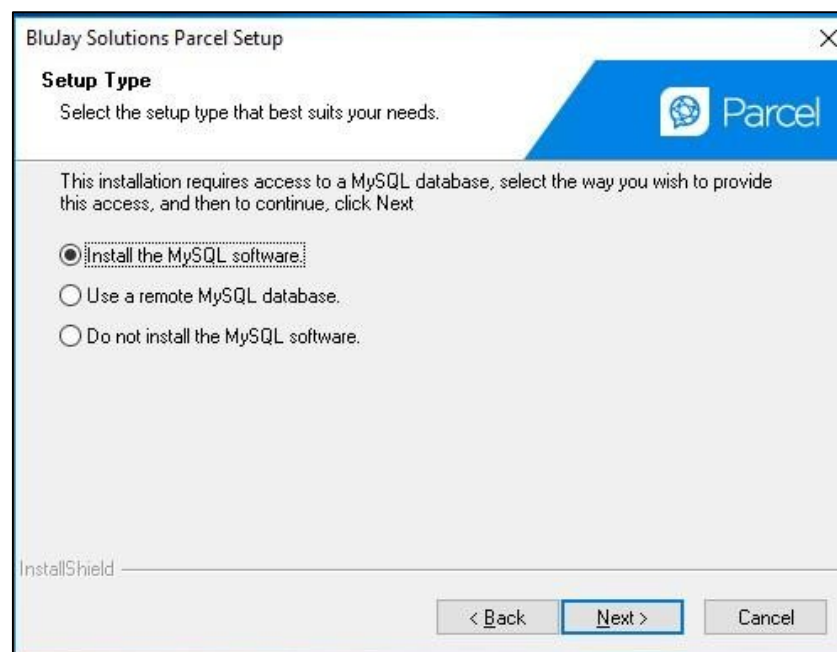
Wizard. (Note also that the World Wide Web Publishing service and the IIS Admin service must be running in order for the Installation Wizard to detect IIS.) If both an Apache Web Server and a Microsoft IIS Web server are detected, the Installation Wizard returns a message that it found both and prompts you to choose which one to use as the Web Server for Parcel. After making this choice, click Next to continue.

If no Web Server is detected, the Installation Wizard displays the following message: NO WEB SERVER HAS BEEN LOCATED.

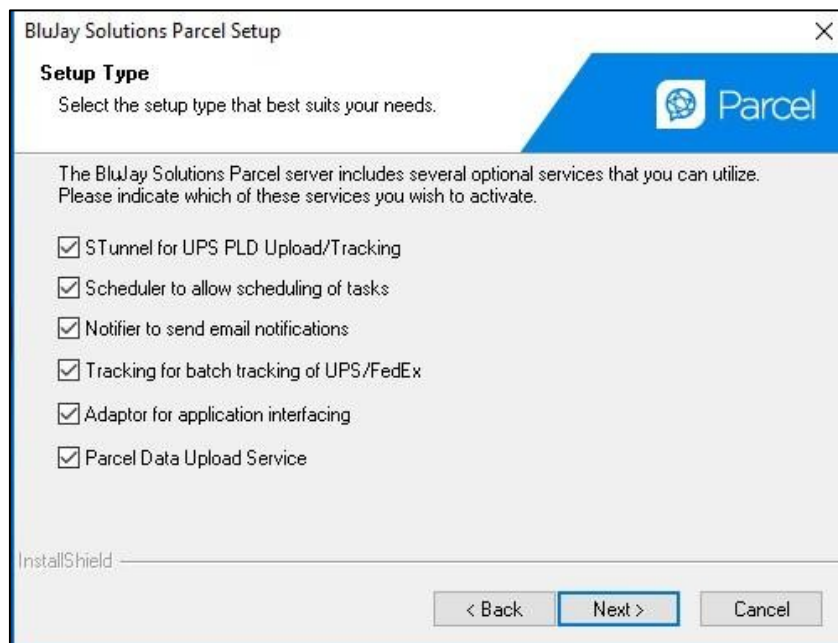


If you want the Wizard to install the Apache Web Server, click Next to continue. If no Web Server is detected, and you wish to use Microsoft IIS instead of Apache, click Cancel to exit the installation. If this is the case, you need to install IIS separately. After installing IIS, you also need to configure IIS to work with Parcel. After installing IIS, run the Parcel installation program again.

8. On the Setup Type screen (as shown in the following illustration), select the 'Install the MySQL software' option to install the MySQL software and then click Next.



9. On the next Setup Type screen, select the services that you want to install as (as described in the table) and then click Next.

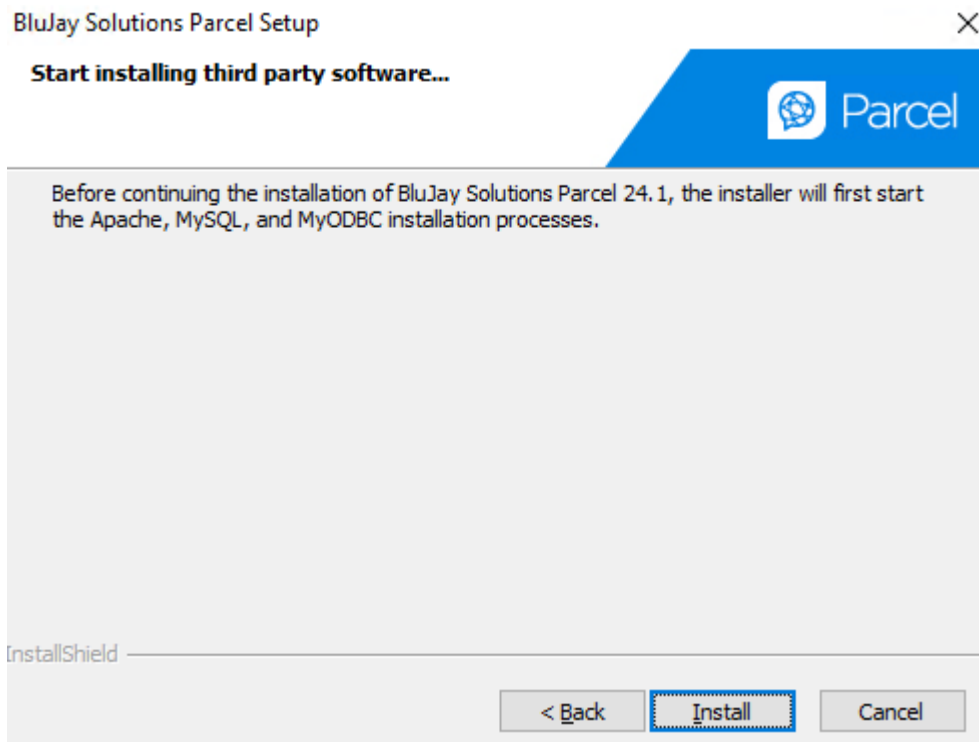


Service	Description
STunnel for UPS PLD Upload/Tracking	Required to upload files to UPS and track UPS packages, including batch tracking. <i>Note:</i> When you change from a test environment to a production environment, you need to edit the stunnel configuration file.
Scheduler to allow scheduling of tasks	Required to schedule system tasks in Parcel (such as backing up the database or batch tracking).
Notifier to send email notifications	Required to send shipment and other event notification e-mails.
Tracking for batch tracking of UPS/FedEx	Required to track UPS/FedEx packages in Parcel using the Scheduler for to set up batch tracking.
Adapter for application Interfacing	This checkbox is deactivated by default. Activation is required to use the Interface Adapter (IA Server). If you want to use Parcel's Connect add-on, select (check) this checkbox. <i>Note:</i> Connect requires carrier-level configuration.
Service	Description

Parcel Data Upload Service	This checkbox is unselected by default. Selection is required to use the Parcel Data Upload Service. If you want to use Parcel Data Upload Service, select (check) this checkbox.
----------------------------	--

Note: We strongly recommend that you select (activate) the first four checkboxes on this screen, especially if you plan to track shipments using batch tracking via the Scheduler.

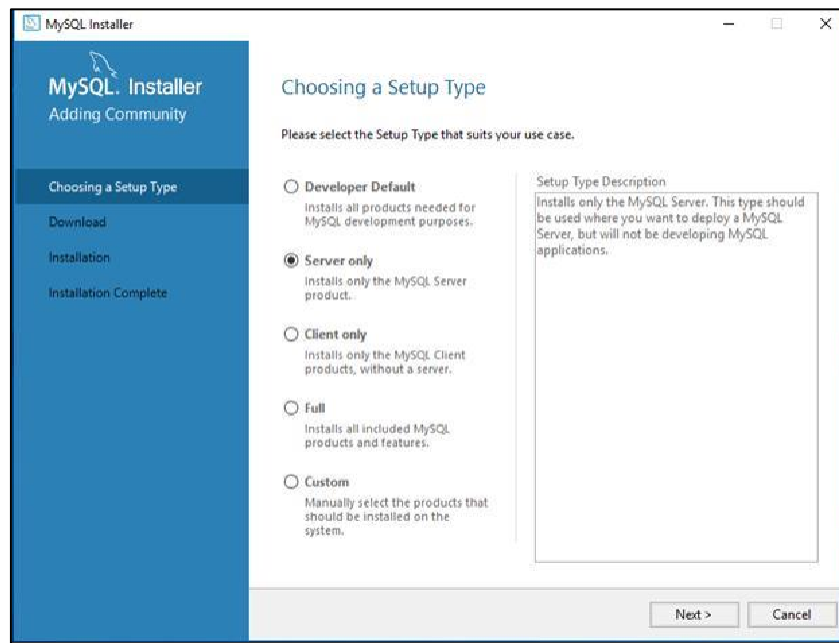
- The Installation Wizard displays the message: "Start installing third party software..." on the next Setup Type screen. Click Install to continue with the installation.



Installing MySQL Server

If you select to install the MySQL Server on this machine (as described in Step 6), the installation wizard program will guide you through the installation as follows:

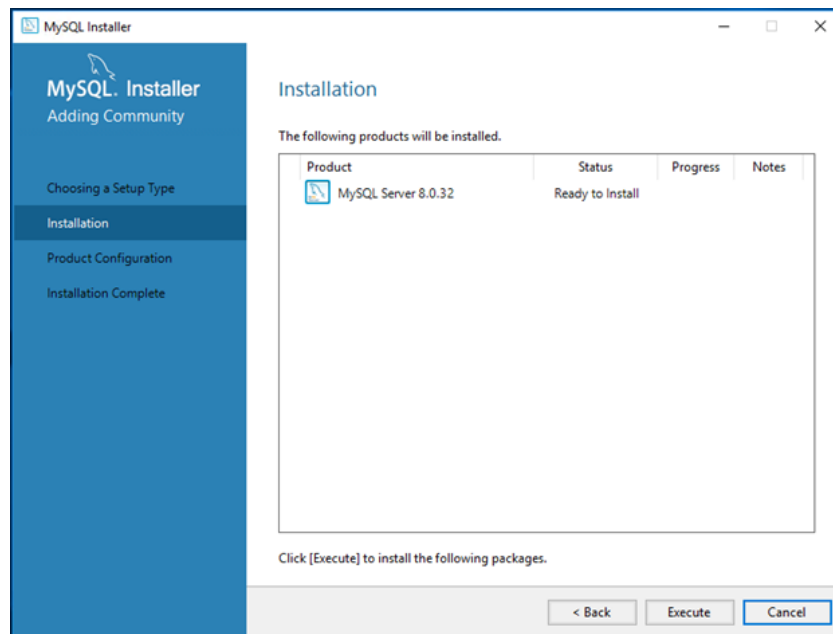
1. On the Setup Type screen, select the Server only option and then click Next, as shown in following illustration:*Note: If you want to install MySQL on different drive, refer to [Installing MySQL on different drive section](#) under [Troubleshooting](#).*



Setup Type	Description
Developer Default	Select this option to install all products needed for MySQL application development.
Server only	Select this option to install only the MySQL Server product.
Client only	Select this option to install the MySQL Client products, without a server.
Full	Select this option to install all including MySQL products and features.
Custom	Select this option to manually select the products that you want to install in different drive or system.

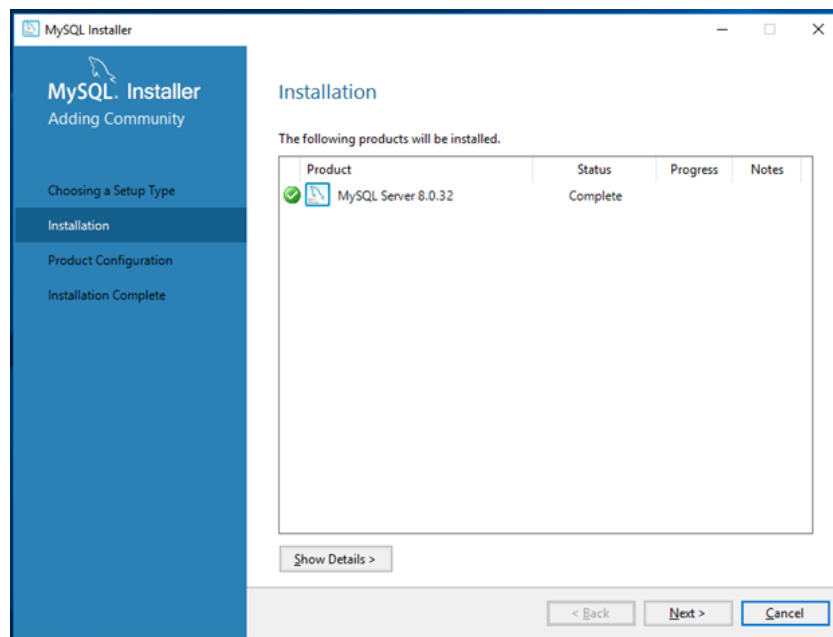
The Installation screen appears.

2. On the Installation screen, click Execute.

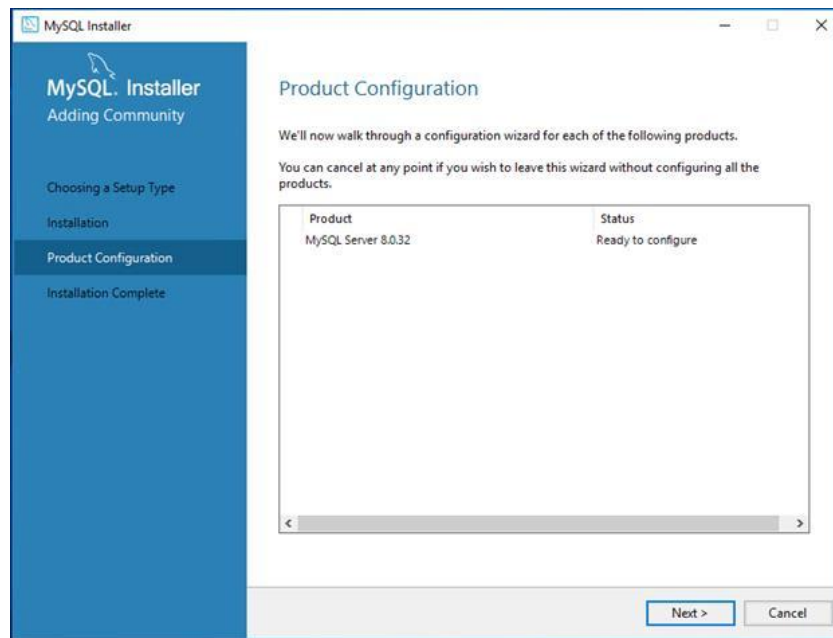


After few seconds, the MySQL Installation gets completed.

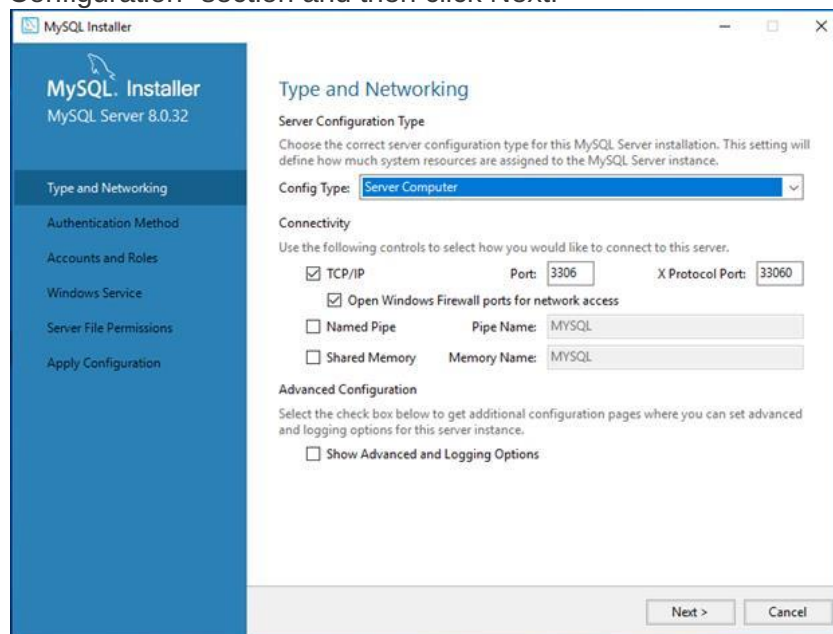
3. On the Installation screen, click Next to continue with the Product configuration.



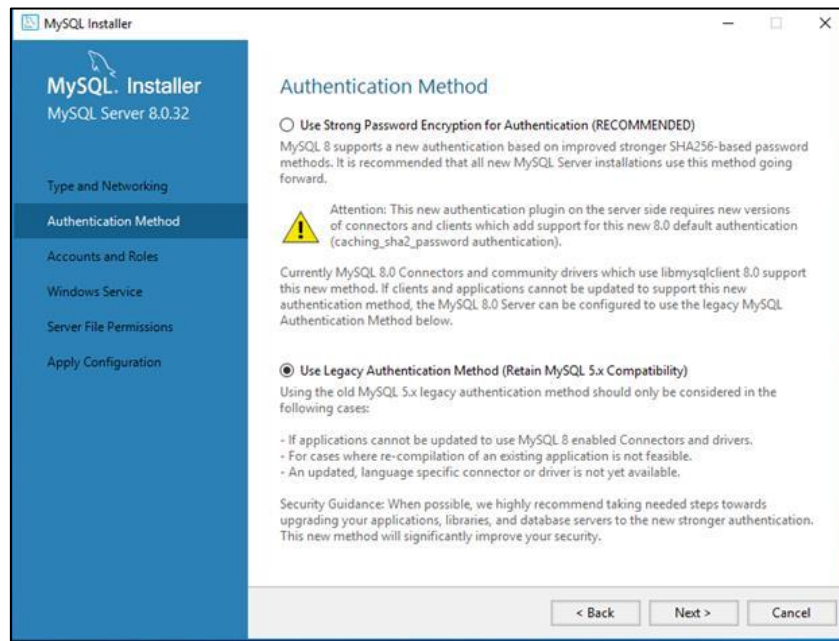
4. On the Product Configuration screen, click Next.



5. On the Type and Networking screen, select "Server Computer" from the "Config Type" drop-down and leave the default settings in "Connectivity" and "Advanced Configuration" section and then click Next.

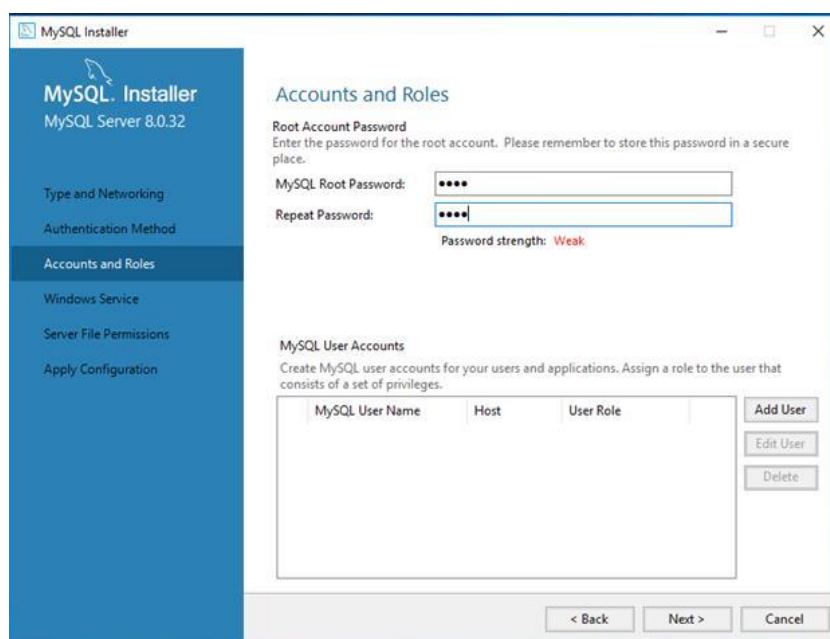


6. On the Authentication method screen, select "Use Legacy Authentication Method" and click Next.



- On the Accounts and Roles screen, type "root" (all lowercase letters without quotation marks) in the "MySQL Root Password" and "Repeat Password" fields, and then click Next.

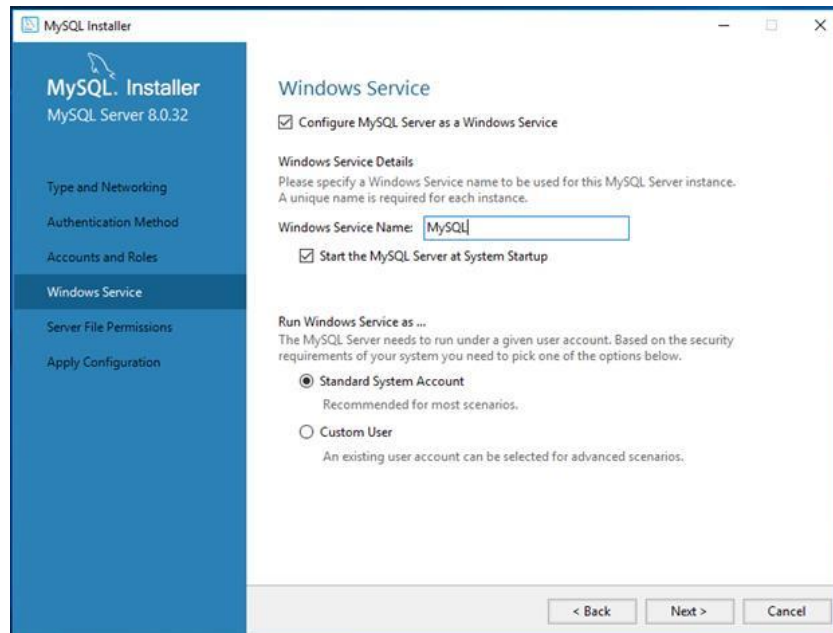
You must type this specific password, since Parcel uses this as the root account password as required by the Parcel Configuration (Web Admin) Tool. The root account has all privileges in the MySQL database. It is important to create a root account password. Any user logged in from a valid hostname can access MySQL and make alterations to the database using this root account.



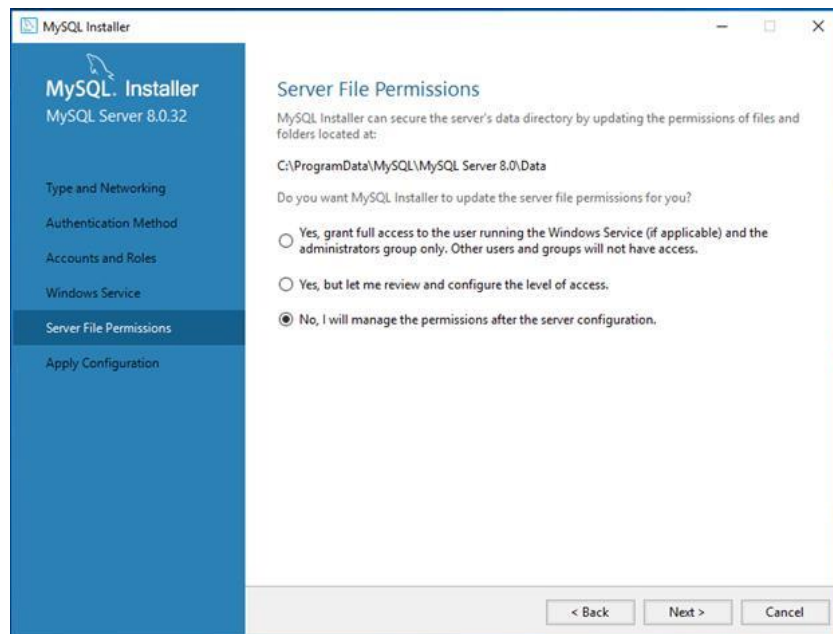
- On the Windows Service screen change the window service name to MySQL in "Windows Service Name" field and leave the default settings as it is in the screen and then click Next.

Note

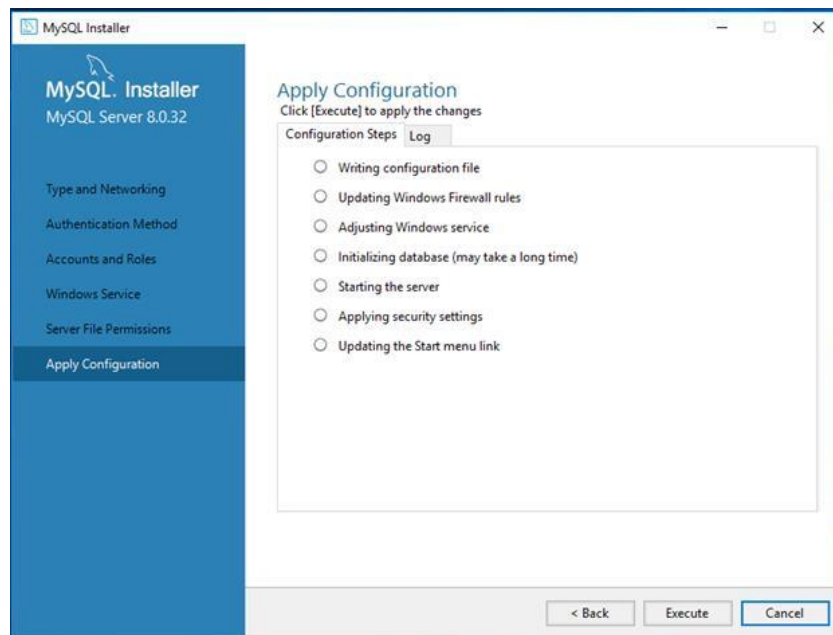
Ensure that the Windows Service Name field is MYSQL.



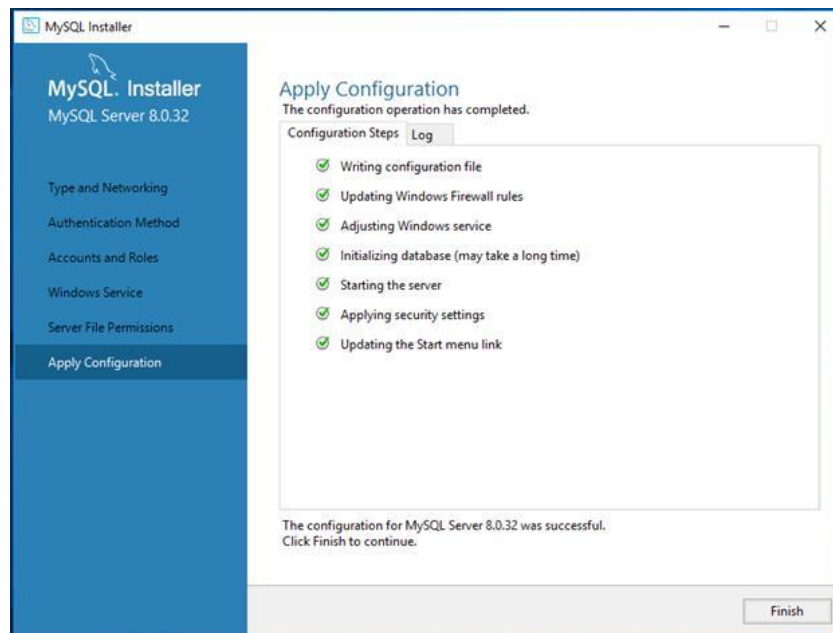
- On the Server File Permissions screen, select "No, I will manage the permissions after the server configuration" option and click Next.



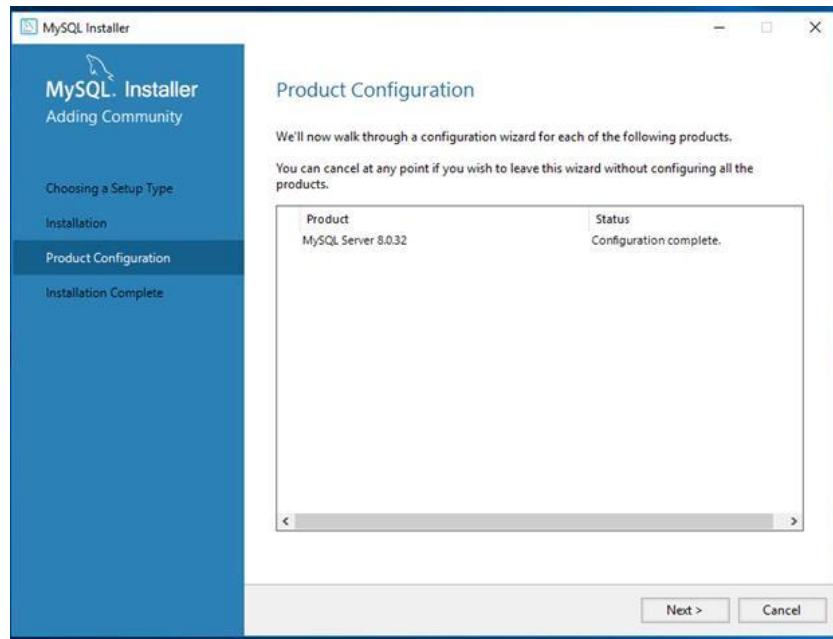
10. On the Apply Configuration screen, click Execute to enable your configuration settings.



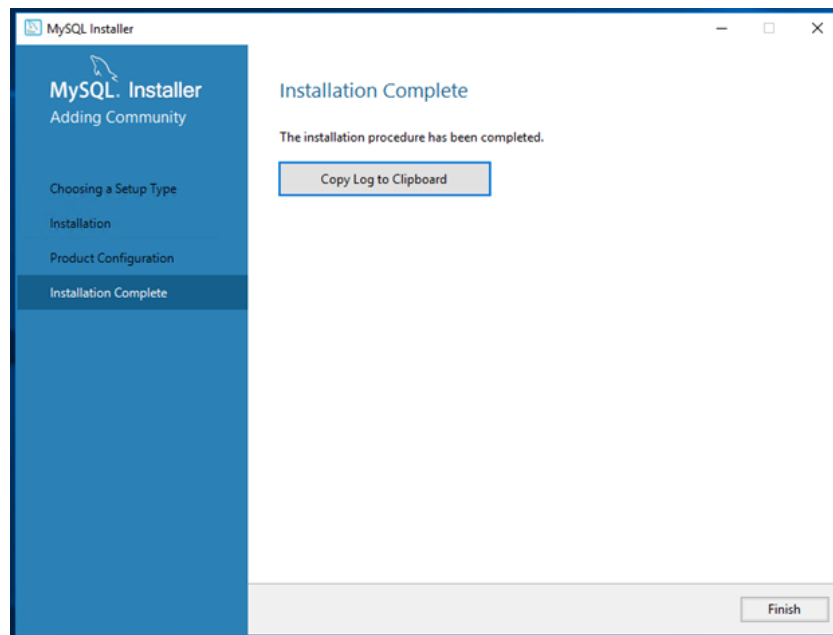
11. On the Apply Configuration screen, click Finish.



12. On the Product Configuration screen, click Next.

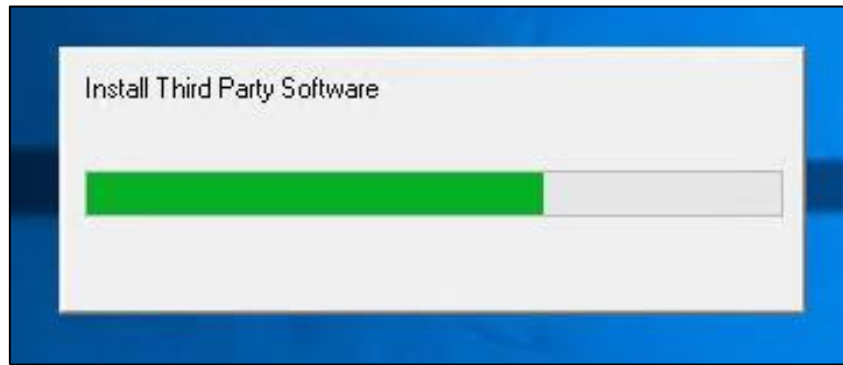


13. On the Installation Complete screen, click Finish to complete the MySQL installation.



Installing MySQL Connector/ODBC 64bit

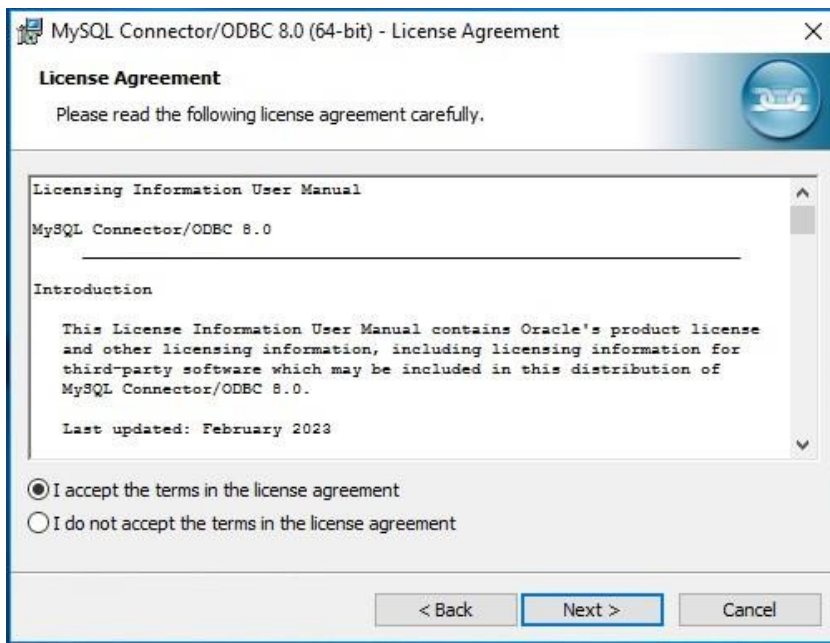
After you install the MySQL Server, the MySQL Connector/ODBC Setup Wizard opens.



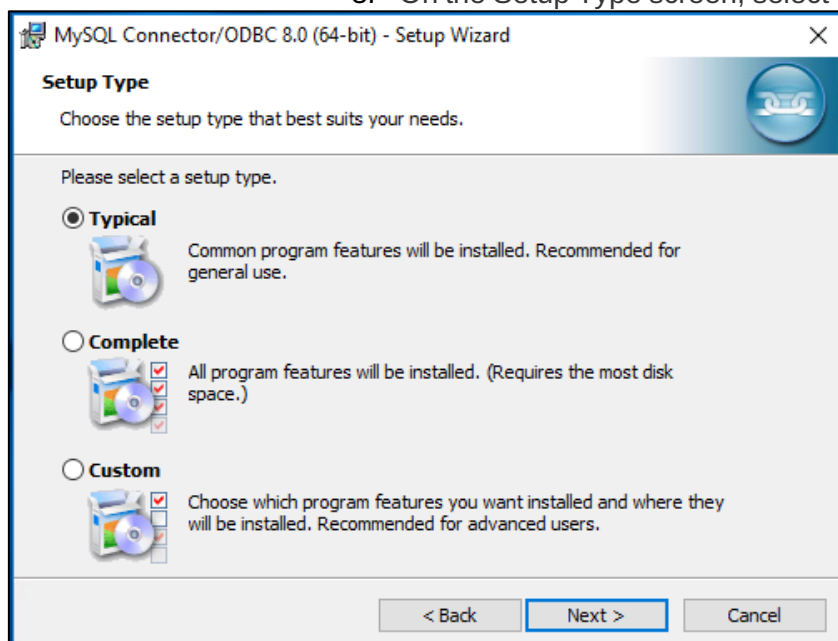
1. On the Welcome screen of the MySQL Connector/ODBC Setup Wizard, click Next.



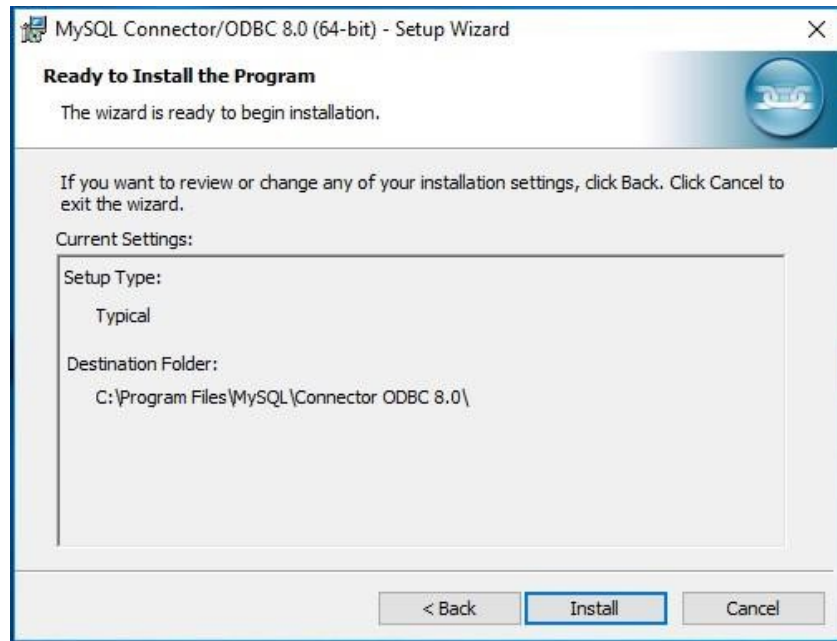
2. Accept the MySQL ODBC License Agreement.



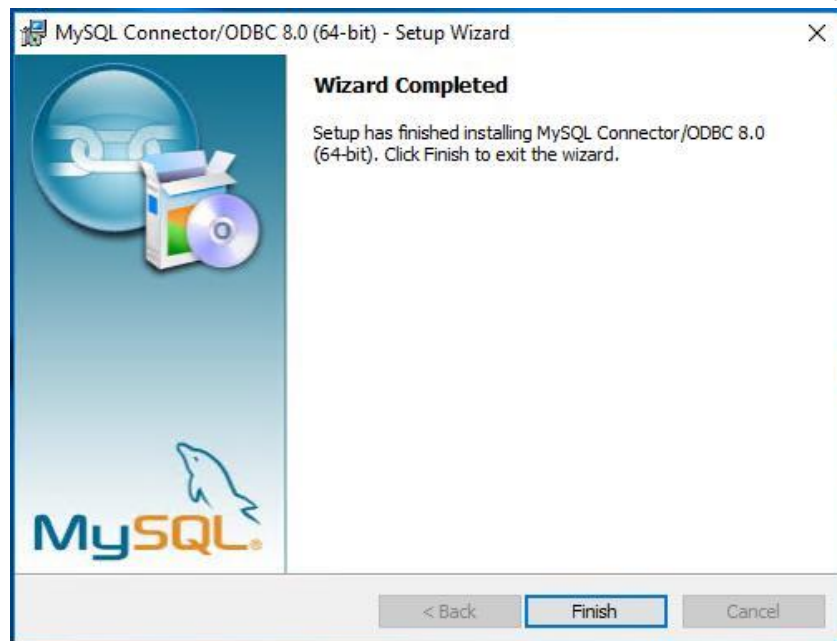
3. On the Setup Type screen, select the Typical option and then click Next.



4. On the Ready to Install screen, click Install.



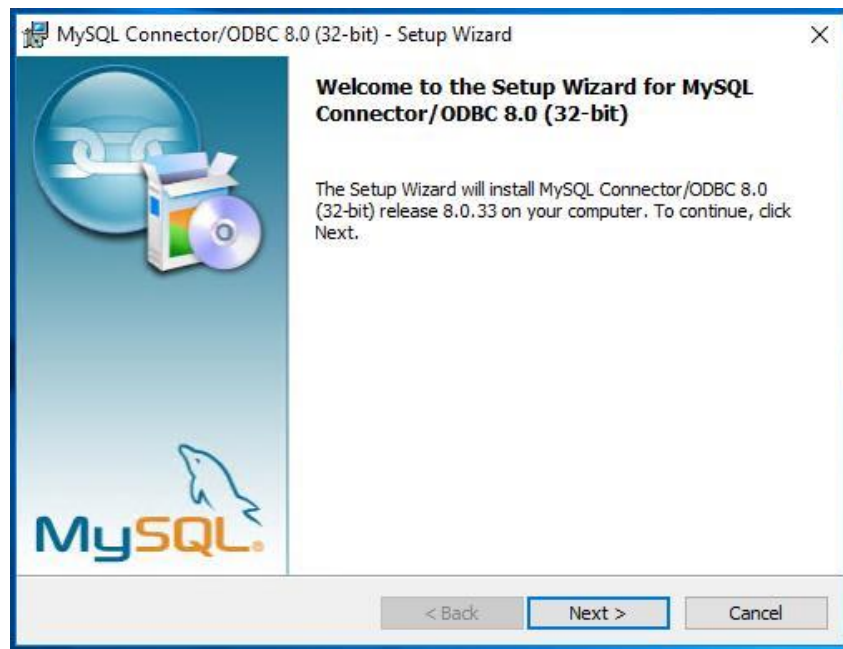
5. Click Finish in MySQL Connector/ODBC 8.0 (64-bit)-Setup Wizard to complete the installation.



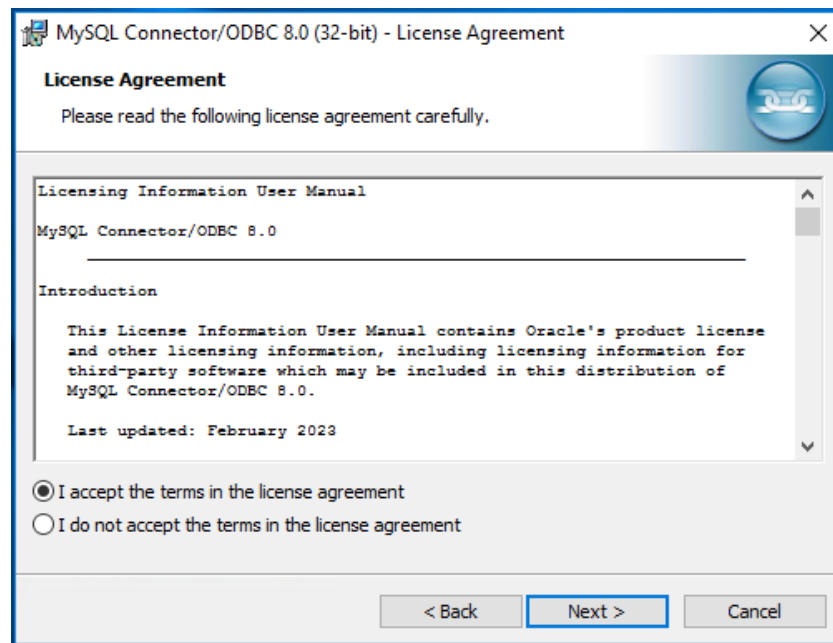
Installing MySQL Connector/ODBC 32bit

After you install the MySQL Server, the MySQL Connector/ODBC Setup Wizard opens.

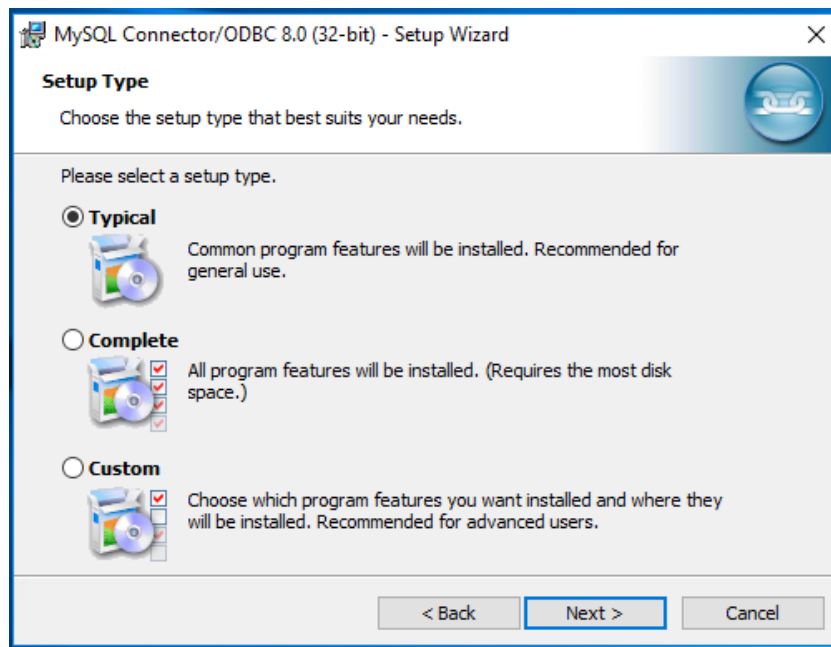
1. On the Welcome screen of the MySQL Connector/ODBC Setup Wizard, click Next.



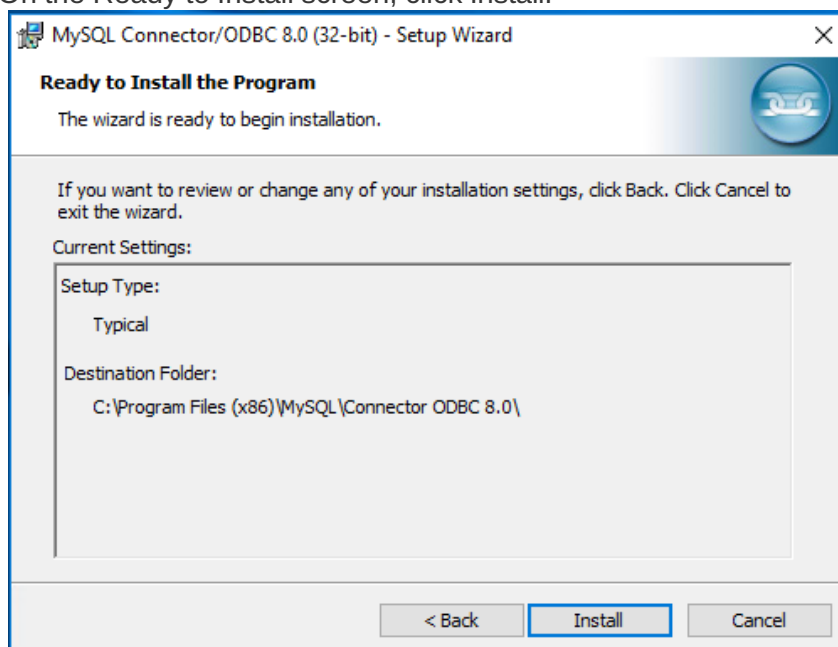
2. Accept the MySQL ODBC License Agreement.



3. On the Setup Type screen, select the Typical option and then click Next.



4. On the Ready to Install screen, click Install.

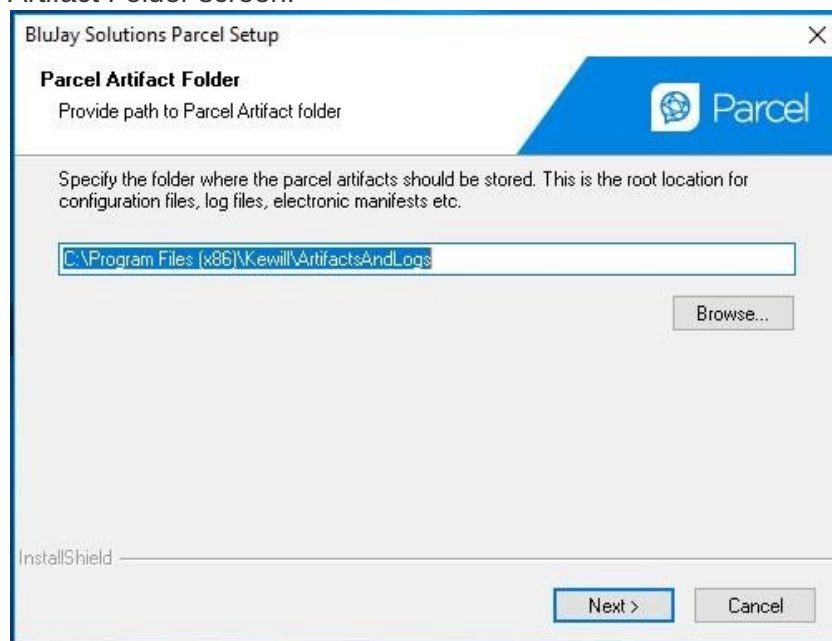


5. A progress bar enables you to view the progress of the installation. Installation completes when the MySQL Connector/ODBC 8.0 Setup Wizard displays the Finish window. Click Finish.



After the installation wizard completes installing the MySQL components that you selected to install, there are a few more steps to complete the Parcel installation.

6. Enter the Parcel Artifacts Folder path for storing the Parcel Artifacts of Parcel, UCM and Java services such as configuration files, log files, etc., in the Parcel Artifact Folder screen.



7. The Parcel Artifacts Folder location can be configured using any one of the following methods:
 - a. Application Server Local Path. For Example: C:\BluJay\ParcelArtifacts
 - b. Universal Naming Convention (UNC) Path. For Example:
\\blujay.global\GlobalShares\ParcelArtifacts
 - c. Mapped Drive. For Example: Z:\
 - d. AWS FSx. For Example:
\\amznfsxw4c3qtd6.iaaad.blujaysolutions.net\share

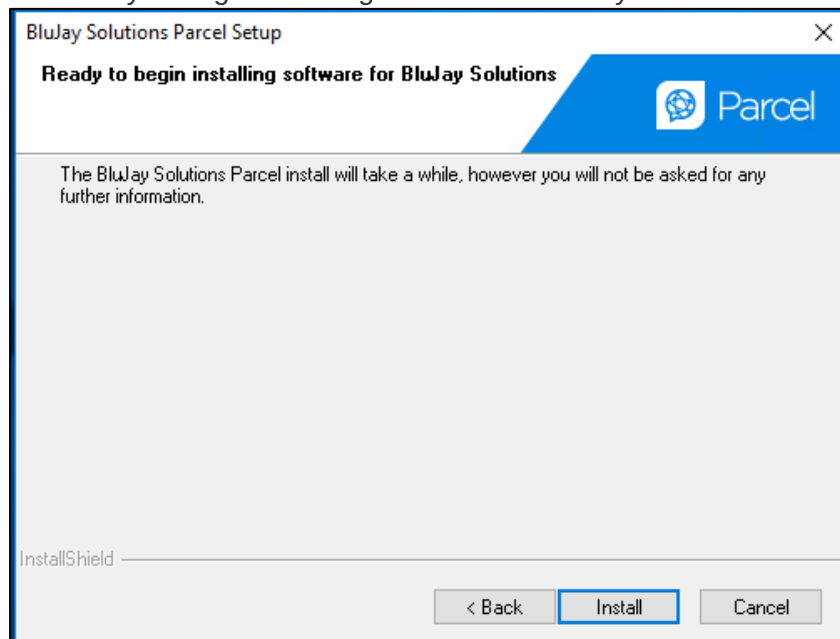
Notes

The Parcel Artifact Folder provided in the above screen should be same across all the products.

The Parcel Artifact Folder provided in the above screen gets saved in ParcelSystem.ini file (under installation folder/flagship/bin).

8. Click Next.

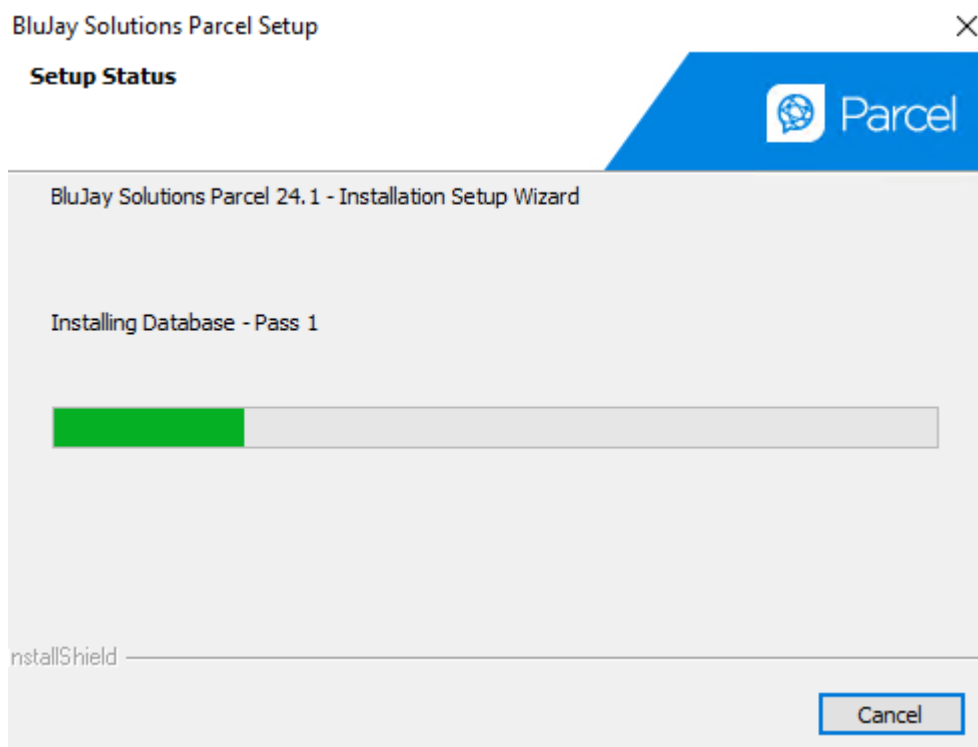
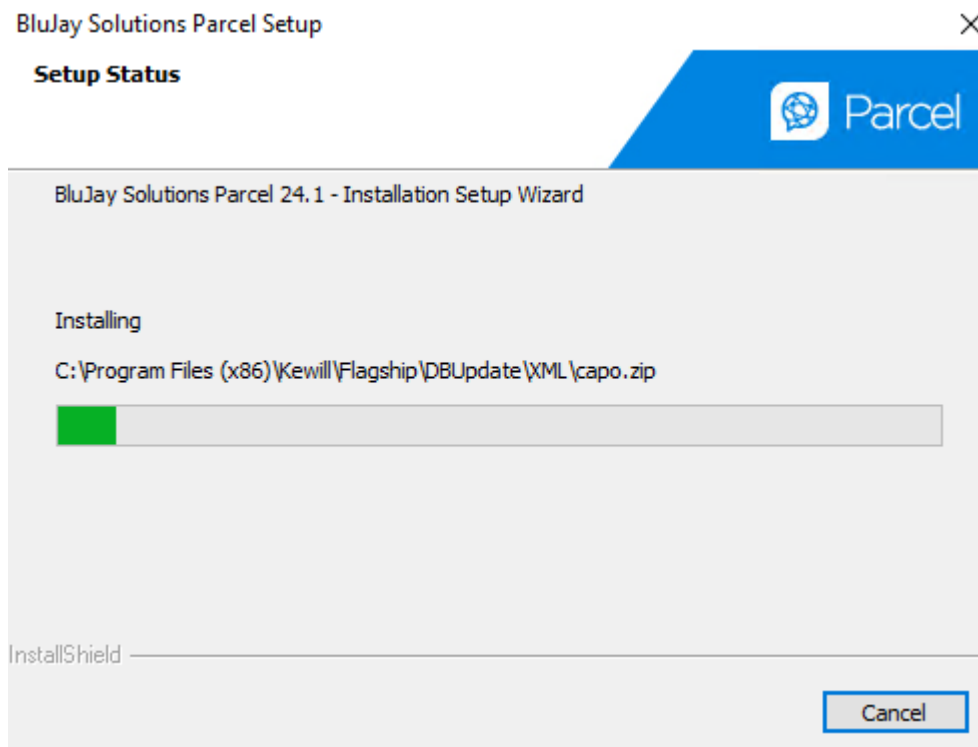
The Ready to begin installing software for BluJay Solutions screen appears.



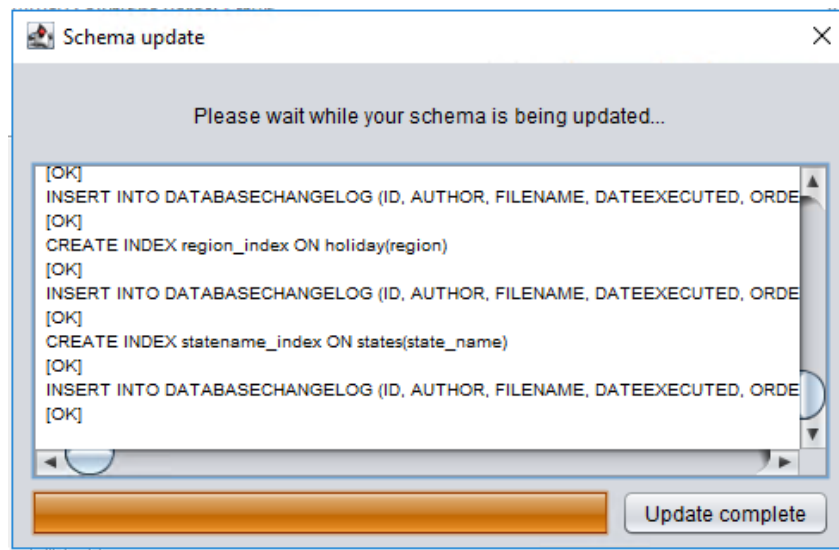
9. Click Install to begin installing the Parcel components – DIServer, Parcel User Interface, and Parcel databases – that you selected to install at the beginning of the installation program. While installing the Parcel components, the Installation Wizard displays a progress bar (as shown in following illustration) enabling you to track the progress of the installation. This could take anywhere from several minutes to an extended period of time (depending on machine speed) to complete.

Completing Database Installation

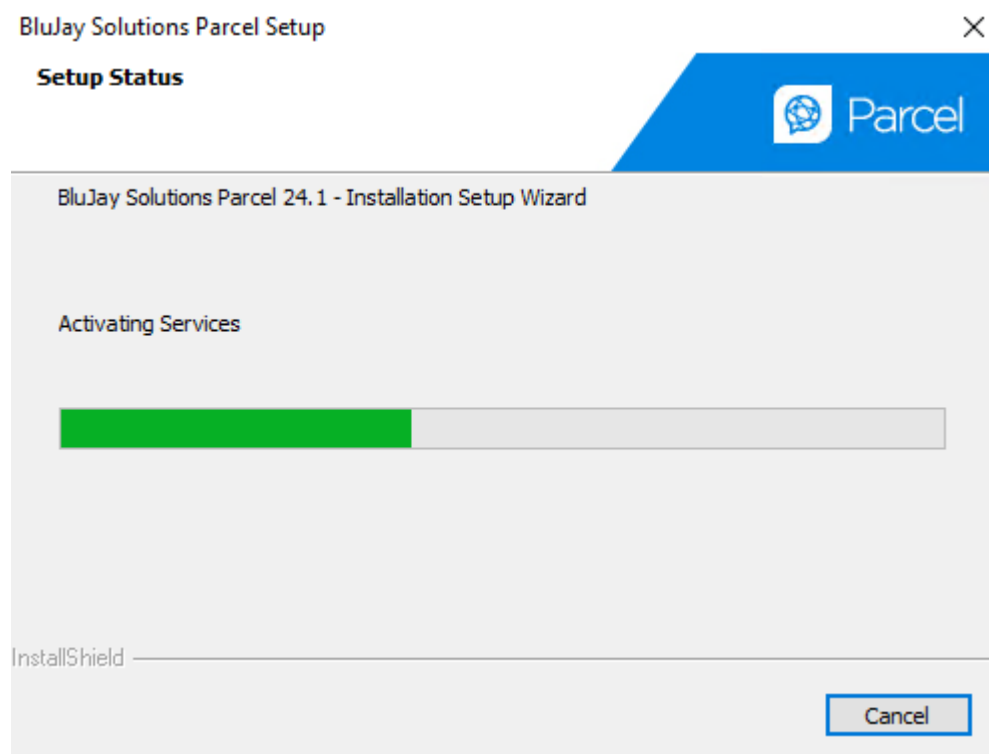
The following status screens display progress of database installation:



After the Parcel Database installation, the installer displays the Schema update screen.

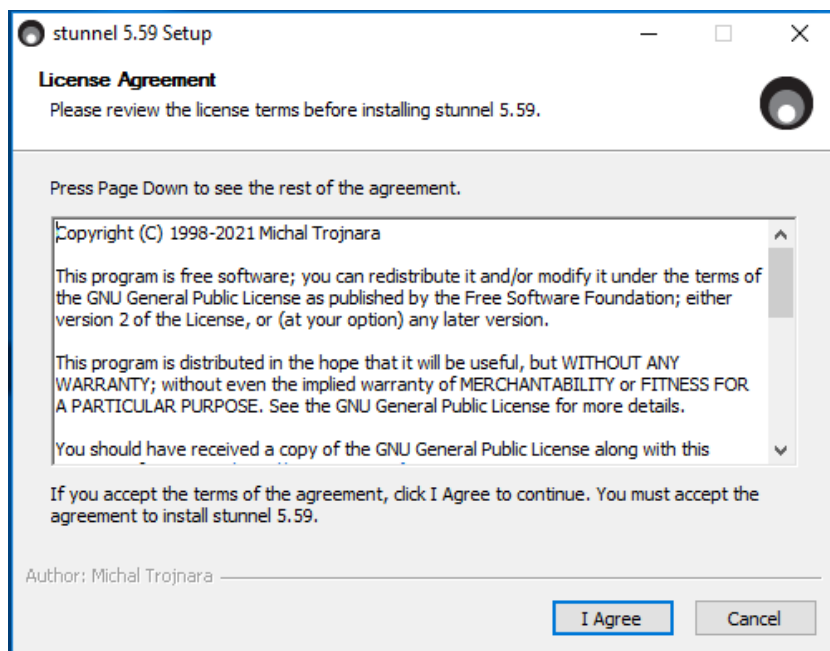


When the Schema update is complete, click Update complete to finish the installation. The Setup Status screen appears with the Activating Services progress bar.

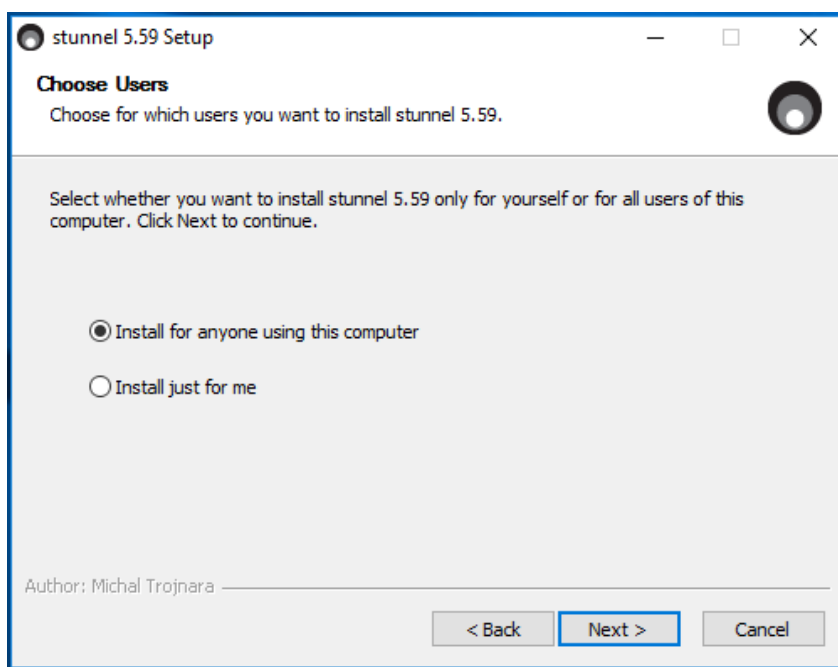


Installing Stunnel

1. Click I Agree on Setup License Agreement screen, when the stunnel 5.59 installer opens.



2. On the stunnel 5.59 Setup: Choose Users screen, select **Install for anyone using this computer** option, and then click Next.



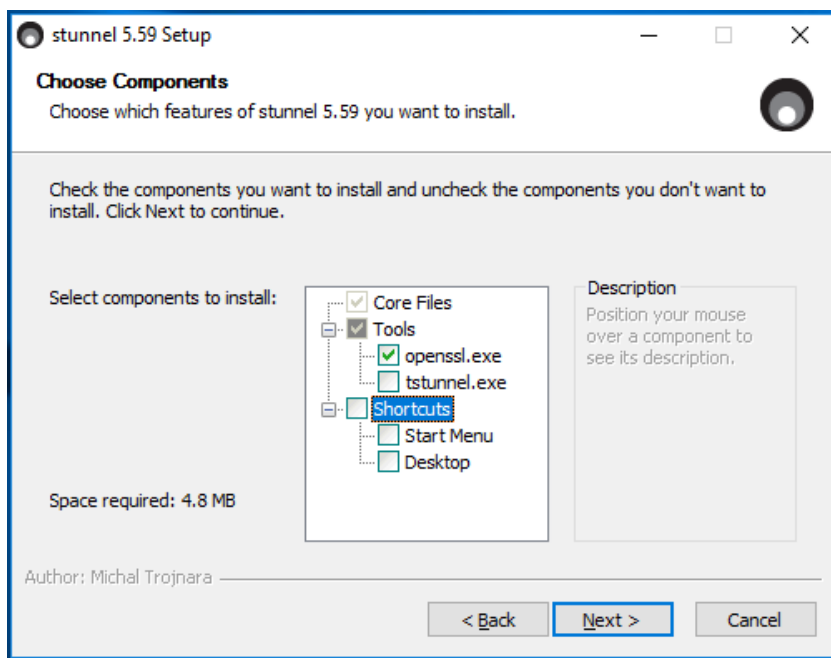
Install stunnel users	Description
Install for anyone using this computer	Install stunnel 5.59 for all users of this computer.
Install just for me	Install stunnel 5.59 for just for yourself.

3. On the stunnel 5.59 Setup: Choose Components to install stunnel with selecting **openssl.exe** check box or without selecting **openssl.exe** check box.

With selecting openssl.exe check box

If you plan to use stunnel with client-side certificates (i.e., certificatebased authentication), then you must select **openssl.exe** check box during stunnel installation.

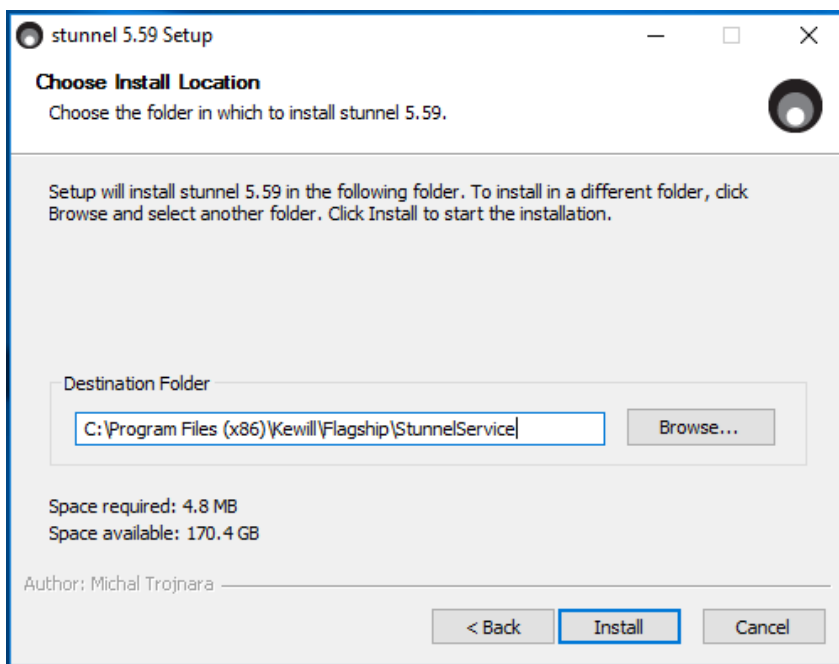
- a. Select **openssl.exe** check box and then click Next.



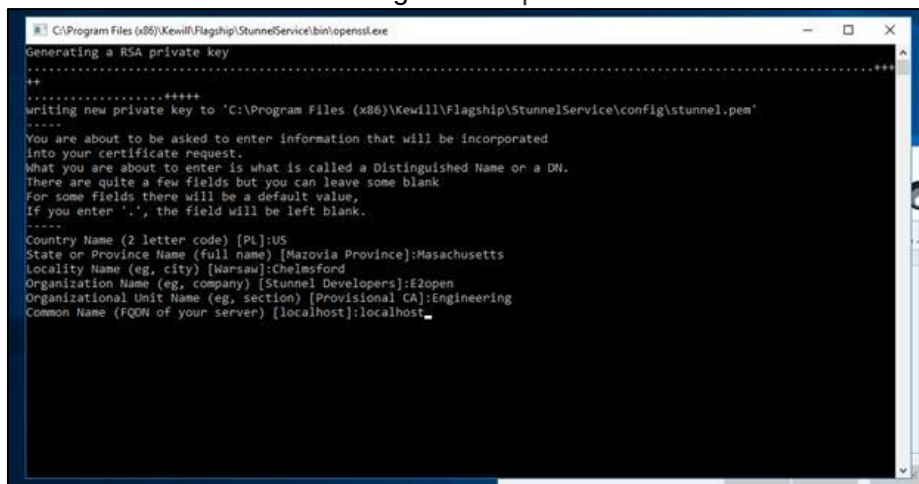
- b. On the stunnel 5.59 Setup: Choose Install Location screen, click Browse... and specify the following Destination Folder and then click Install to proceed with the stunnel installation.

<Drive>: \<Parcel Install Folder>\Flagship\STunnelService\

For Example: C:\Program Files
(x86)\Kewill\Flagship\STunnelService\



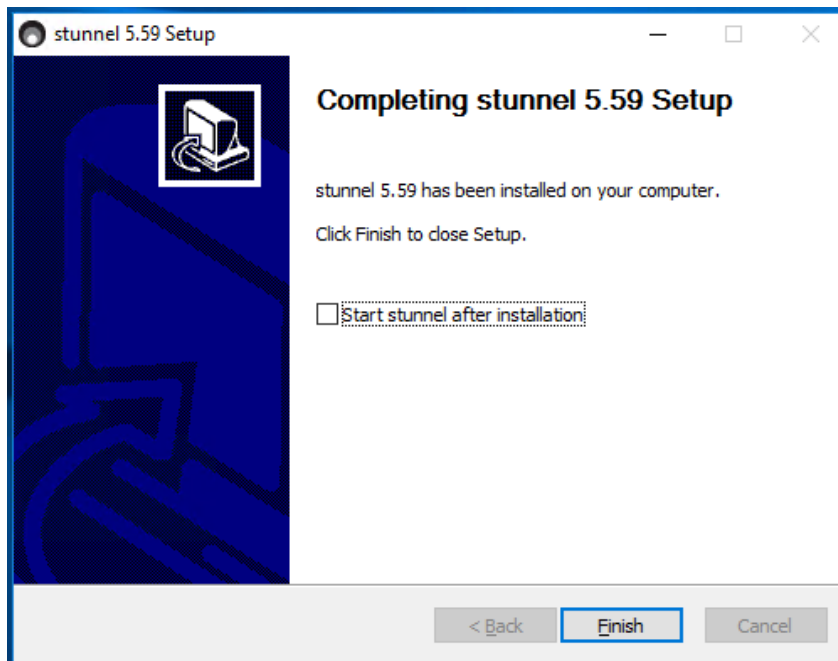
- c. Enter your address details for the certificate in the openssl.exe file, as shown in following table to proceed with the stunnel installation.



In this field...	Do this...
Country Name	Enter the country name in 2 letter code. For Example: US
State or Province Name	Enter the state or province name. For Example: Massachusetts
Locality Name	Enter the city name. For Example: Chelmsford
Organization Name	Enter the organization name (i.e., company name.) For Example: CA Solutions Ltd.
Organization Unit Name	Enter the company unit name. (i.e, section) For Example: Engineering

Common Name	Enter the FQDN details of your server. For Example: localhost
--------------------	---

- d. On the stunnel 5.59 Setup: Completing stunnel 5.59 Setup screen, click Finish to complete the stunnel installation.



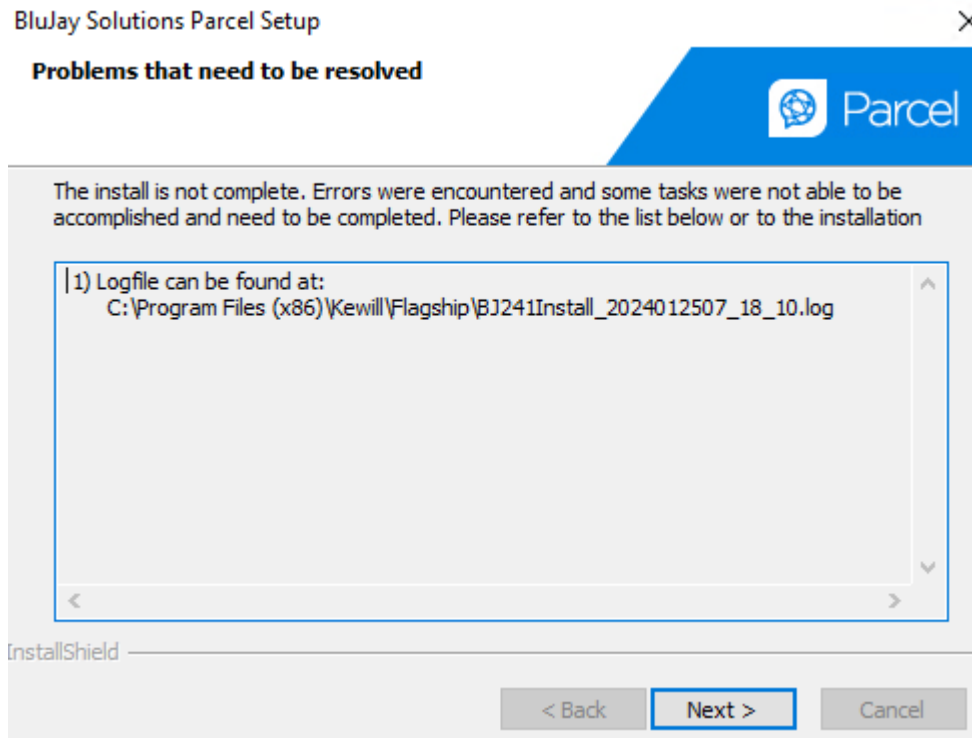
After Stunnel installation is complete, Setup Status screen displays Activating Services progress bar.

After the Activating Service is completed, if there are any errors, the Parcel Setup wizard displays these errors, along with the location of the installation log file.

Note

If there are errors, see the sections under [Troubleshooting](#) for information on resolving these.

Otherwise, click Next to complete the installation.

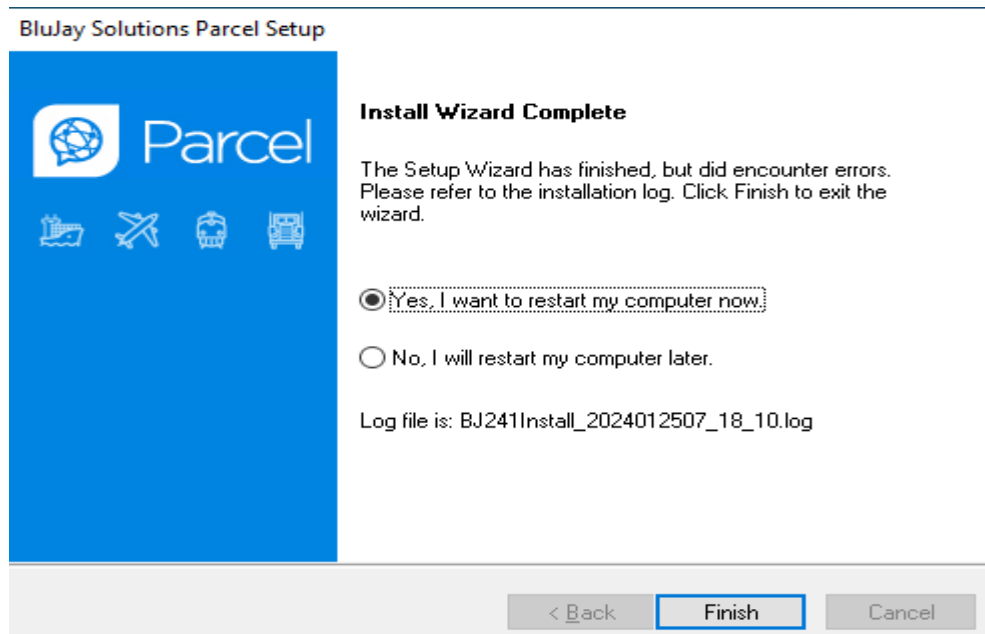


The Install Wizard Complete screen appears.

4. To run Parcel, you need to restart the computer where it is installed. The Install Wizard Complete screen gives you the following options:

- Yes, I want to restart my compute now (the default selection)
- No, I will restart my computer later.

5. Make the desired selection, and then click Finish to complete the installation.

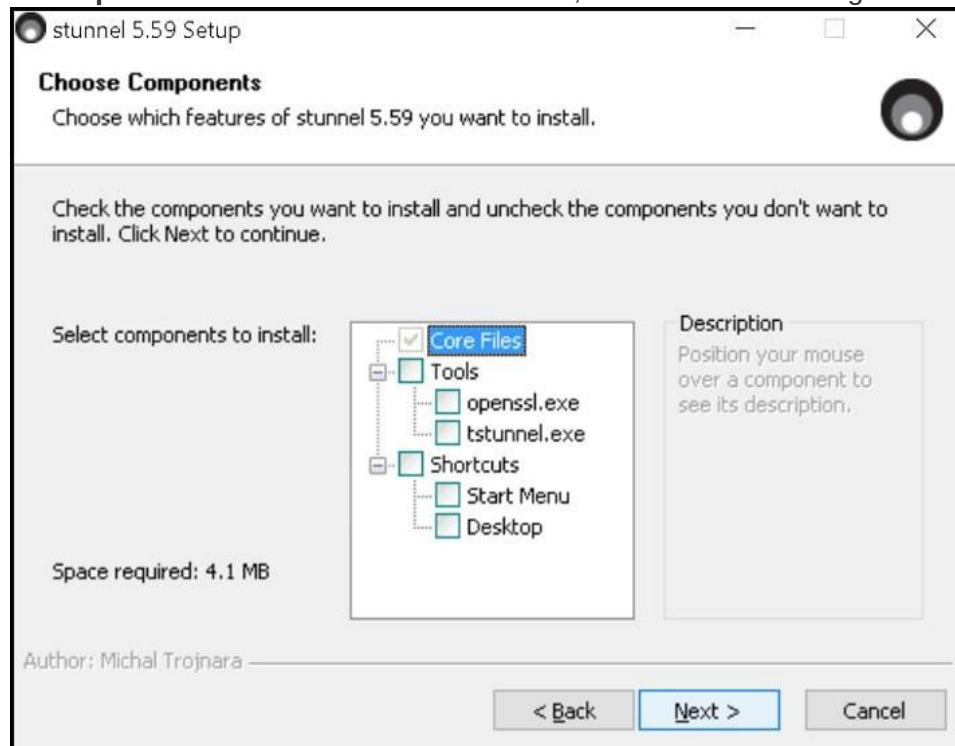


After Parcel installation is successful, follow the [Post Installation Steps](#).

Without selecting openssl.exe check box

If you are not planning to use stunnel with client-side certificates (i.e., certificatebased authentication), then you do not need to select **openssl.exe** check box during the stunnel installation.

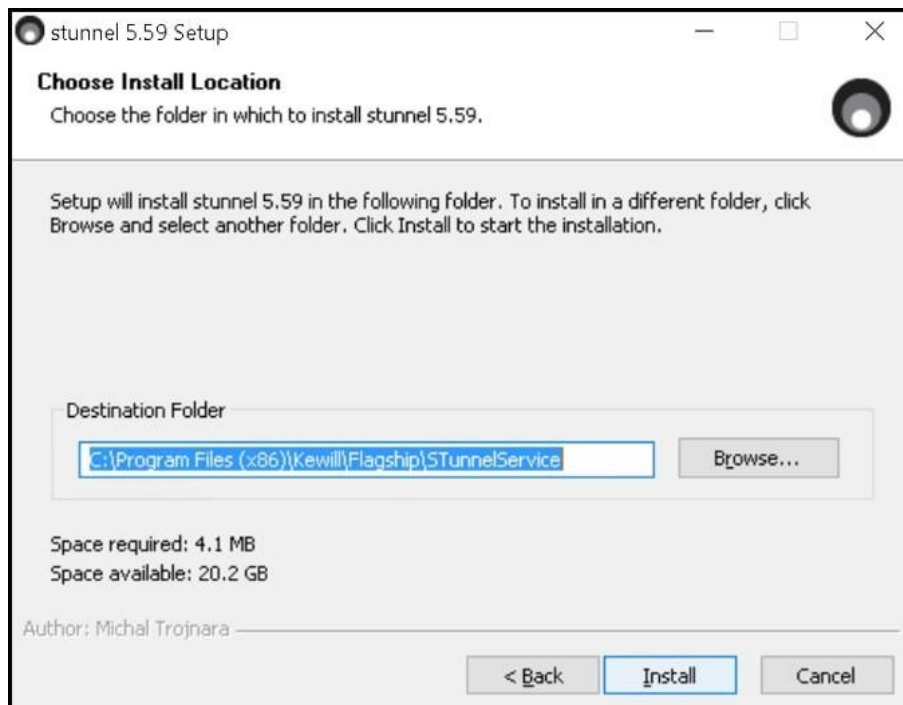
1. Clear **openssl.exe** check box and click Next, as shown in following screen.



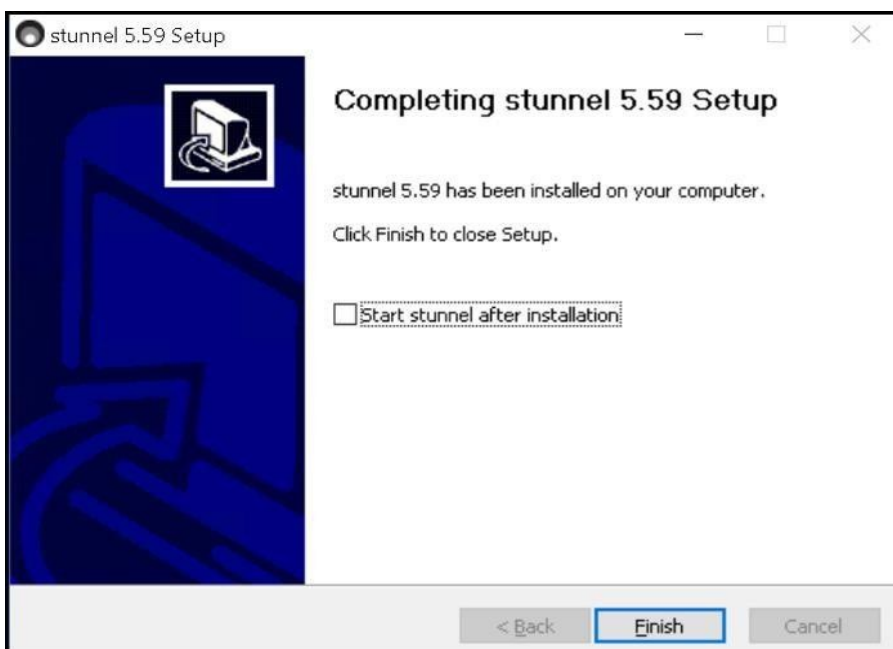
2. On the stunnel 5.59 Setup: Choose Install Location screen, click Browse... and specify the following Destination Folder and the click Install to proceed with the stunnel installation.

<Drive>:<Parcel Install Folder>\Flagship\STunnelService\

For Example: <Parcel Install Folder>\Flagship\STunnelService\



3. On the stunnel 5.59 Setup: Completing stunnel 5.59 Setup screen, click Finish to complete the stunnel installation.



After Stunnel installation is completed the Installation Wizard continues with the installation.

Installing Parcel in a Distributed Environment

Installing Parcel on the Application Server

To install Parcel on the Application Server so that it points to the Remote MySQL server, please follow these steps:

1. Install Parcel on the Application Server, as per the instructions mentioned in "Complete Installation" section.
2. Setup and Install Parcel DB on Remote Server, as per instructions mentioned in "Installing Parcel DB 24.1.0 on Remote Server" section.
3. Connect Application Server with Remote MySQL Server, as per instructions mentioned in "Connecting Remotely to Database" section.
4. Restart DIServer.

Installing Parcel DB on Aurora Server

Prerequisites:

- Application Server should be installed with Parcel 24.1.0.
- Aurora Server.

To install Parcel DB 24.1.0 on Aurora Server, follow these steps:

1. In Application Server, Navigate to
<Parcel Artifact Folder>\Flagship\DBUpdate\XML\flagshipProperties.xml to change the value for 'flagshipHost' element from 'localhost' to the Remote IP Address or Remote Hostname.
2. Navigate to<Parcel Install Folder>\Flagship\DBUpdate\XML\SetupProperties.bat
3. Replace the line "mysql -N -e "SELECT SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA WHERE SCHEMA_NAME='didb'" > "%CURR_DIR%didb_exists.txt" with the line below and replace <hostname>, <username>, <pwd> with the Hostname/IP, username and password of the Aurora Sever respectively.

```
mysql -h <hostname> -u<username> -p<pwd> -N -e "SELECT SCHEMA_NAME
FROM INFORMATION_SCHEMA.SCHEMATA WHERE
SCHEMA_NAME='didb'" > "%CURR_DIR%didb_exists.txt"
```

4. Replace the line "mysql -f < %drop_fs_user%" with the line below and replace <hostname>, <username>, <pwd> with the Hostname/IP, username and password of the Aurora Sever respectively.

```
mysql -h <hostname> -u<username> -p<pwd> -f < %drop_fs_user%
```

5. Replace the line "mysql -f < %create_fs_user%" with the line below and replace <hostname>, <username>, <pwd> with the Hostname/IP, username and password of the Aurora Sever respectively.

6. mysql -h <hostname> -u<username> -p<pwd> -f < %create_fs_user%

7. Save the file.

8. Navigate to<Parcel Install Folder>\Flagship\DBUpdate\InstallDB_ALL_50.bat

9. Replace the line "mysql -f < set_permissions.sql" with the line below and replace <hostname> with the Hostname/IP, username and password of the Remote Server respectively.

```
mysql -h <hostname> -u<username> -p<pwd> -f < set_permissions.sql
```

10. Open a command prompt using Administrative privileges and change directory to folder: <Parcel Install Folder>\Flagship\DBUpdate and Execute the command.

11. Execute the following command and wait for it to complete.

```
InstallDB_ALL_50.bat 1 > update.log 2>&1
```

Now, the Parcel DB 24.1.0 on Aurora Server is successfully installed.

Installing MySQL on Remote Server

This section provides the information on installing MySQL on Remote Server. To install MySQL on a Remote Server, follow these steps:

1. Extract the contents of the Parcel distribution zip file to a folder with no spaces on the remote server.
2. Navigate to ThirdParty/MySQL folder and install MySQL. Carry out steps 1-12 from **Installing the MySQL Server** section. Now, the MySQL on Remote Server is successfully installed.

Note

Make sure that the Remote DB Server has 'Environment Variables' > 'System variables' > 'Path' as "C:\Program Files\MySQL\MySQL Server 8.0\bin" set. Add if it is not available already.

3. In the ThirdParty/MySQL folder, double-click the **CreateRemoteRootUser.bat** file.
4. Copy the my.ini file from Application Server and replace the file on MySQL Server folder on Remote Server.

For Example:

C:\ProgramData\MySQL\MySQL Server 8.0

5. Ensure that the **datadir** field in my.ini file is correctly pointed to database root folder in Remote Machine.
6. Restart MySQL on Remote Server.

Installing MySQL Connector/ODBC on Remote Server

After you install the MySQL Server, the MySQL Connector/ODBC Setup Wizard opens. To install the MySQL Connector/ODBC on Remote Server, carry out steps 1-5 from Installing the MySQL Connector/ODBC section. Now, the MySQL Connector/ODBC on Remote Server is successfully installed.

After the successful installation of MySQL Connector/ODBC on Remote Server, you must install Parcel DB 24.1.0 on Remote Server. Refer [Installing Parcel DB on Remote Server](#) for details. After Parcel DB installation, you connect Parcel DB on Remote Server. Refer to [Connecting Remotely to Database](#) for details.

Installing Parcel DB on Remote Server


Prerequisites:

- Application Server should have Parcel 24.1.0 and ensure that MySQL along with data folder exists.
- Install MySQL on Remote Server. Follow the steps mentioned in Installing MySQL on Remote Server section.

To install Parcel DB 24.1.0 on Remote Server, follow these steps:

In Application Server:

1. Copy the 'RemoteMySQL' folder from Parcel 24.1.0 installation package to any of the drive.
2. Unzip 'RemoteMySQL' and open shipnow.ini file. Replace Hostname "127.0.0.1" with "Remote Server Name or IP" and save the file.
3. Navigate to 'RemoteMySQL' folder and double click on "EnableAnonymous_RemoteServer_install.bat" file to enable anonymous user. In command prompt "Enabled Anonymous MySQL user" confirmation message will be displayed, as shown in the following screen.



```

C:\Windows\system32\cmd.exe
Resetting root password
34870
ResetRootID
Reset root password completed
Enabling 'root' password
C:\shipnow.ini
1 File(s) copied
Resetting root password
ManageRootID
Reset root password completed
'root' password enabled
Enabling Anonymous MySql user
34870
EnableAnonymous
Info: Granting Privileges.
Info: Granted Privileges.
Enabled Anonymous MySql user
Press any key to continue . . . _

```

The SqlUserAdmin.log file is generated and placed in the same file path folder.

4. Navigate to <Parcel Artifact Folder>\Flagship\DBUpdate\XML\flagshipProperties.xml to change the value for 'flagshipHost' element from 'localhost' to the Remote IP Address or Remote Hostname and 'mySqlRootUsername' and 'mySqlRootPassword' element values need to updated to 'root' and 'root'.
5. Navigate to <Parcel Install Folder>\Flagship\DBUpdate\XML\SetupProperties.bat
 - a. Replace the line "mysql -N -e "SELECT SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA WHERE SCHEMA_NAME='didb'" > "%CURR_DIR%didb_exists.txt" with the line below and replace <hostname> with the Hostname/IP of the Remote Server.
mysql -h <hostname> -N -e "SELECT SCHEMA_NAME FROM INFORMATION_SCHEMA.SCHEMATA WHERE SCHEMA_NAME='didb'" > "%CURR_DIR%didb_exists.txt"
 - b. Replace the line "mysql -f < %drop_fs_user%" with the line below and replace <hostname> with the Hostname/IP of the Remote Server.mysql h
<hostname> -f < %drop_fs_user% .
 - c. Replace the line "mysql -f < %create_fs_user%" with the line below and replace <hostname> with the Hostname/IP of the Remote Server.mysql h
<hostname> -f < %create_fs_user%
 - d. Save the file.

6. Navigate to <Parcel Install Folder>\Flagship\DBUpdate\InstallDB_ALL_50.bat
Replace the line "mysql -f < set_permissions.sql" with the line below and replace <hostname> with the Hostname/IP of the Remote Server. mysql -h <hostname> -f < set_permissions.sql
7. Open a command prompt using Administrative privileges and change directory to folder: <Parcel Install Folder>\Flagship\DBUpdate and Execute the command.
8. Execute the following command and wait for it to complete.

InstallDB_ALL_50.bat 1 > update.log 2>&1

Once the database update is completed, the command prompt gets closed.

Now, the 24.1.0 Parcel DB is installed on Remote Server.

9. To disable anonymous user navigate to 'RemoteMySQL' folder and double click on 'DisableAnonymous_RemoteServer.bat' file.

After the user successfully installs the Parcel DB 24.1.0 on Remote Server, they must connect Application Server with Remote MySQL Server, so refer to Connecting Remotely to Database section.

Connecting Remotely to Database

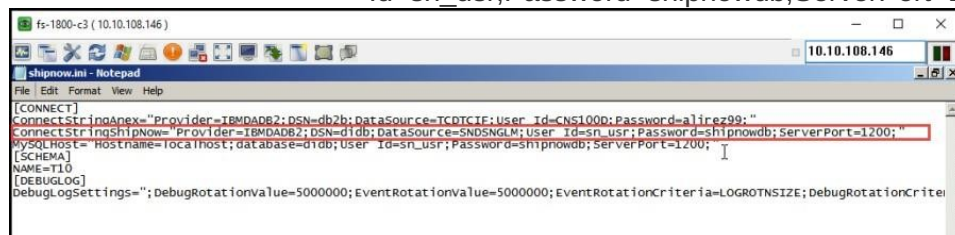
This section provides the information on connecting Application Server with Aurora DB and Remote MySQL Server.

1. In Application Server, Navigate to

<Parcel Artifact Folder>\Flagship\bin\shipnow.ini

2. In shipnow.ini file, comment and place the below code in shipnow.ini and configure Machine Name or IP (depending whether both Application Server and Remote MySQL Server available on same network) in the place of localhost (Remote MySQL Server IP).

MySQLHost="Hostname=localhost;database=didb;User
Id=sn_usr;Password=shipnowdb;ServerPort=1200;"



3. Navigate to <Parcel Artifact Folder>\Flagship\WebGUI\config\config-Flagship.php and provide Remote MySQL Server IP address replacing localhost under "mysql didb connection settings" section, as shown in following screen.

```

1  <?php
2  define( 'WEBROOT', $_SERVER["DOCUMENT_ROOT"] );
3  define( 'WEBAPPROOT', WEBROOT . '/integration/Flagship' );
4  define( 'WEBAPPCONFIGDIR', dirname( __FILE__ ) );
5  define( 'WEBAPPCONFIGFILE', __FILE__ );
6
7  define( 'INTEGRATION', WEBROOT . '/integration' );
8  define( 'INTEGRATION_FLAGSHIP', WEBROOT . '/integration/Flagship' );
9
10 //mysql didb connection settings
11 define( 'DBHOST' , '10.10.108.202' );
12 define( 'DBUSER' , 'sn_usr' );
13 define( 'DBPWD' , 'shipnowdb' );
14 define( 'USE_ENCRYPTED_PASSWORDS' , 'n' );
15 define( 'DBMYSQL', 'didb' );
16
17 //define default server locations
18 define( 'FLAGSHIP_SERVER_DEFAULT_HOST', 'localhost' );
19 define( 'FLAGSHIP_SERVER_DEFAULT_PORT', '1200' );
20 define( 'FLAGSHIP_SERVER_DEFAULT_OPEN_TIMEOUT', '10' );
21 define( 'FLAGSHIP_SERVER_DEFAULT_RECEIVE_TIMEOUT', '600' );
22
23

```

4. Navigate to <Parcel Artifact Folder>\Flagship\WebGUI\defines\dbdefines.php and provide Remote MySQL Server IP address replacing localhost under "mysql didb connection settings" section, as shown in following screen.

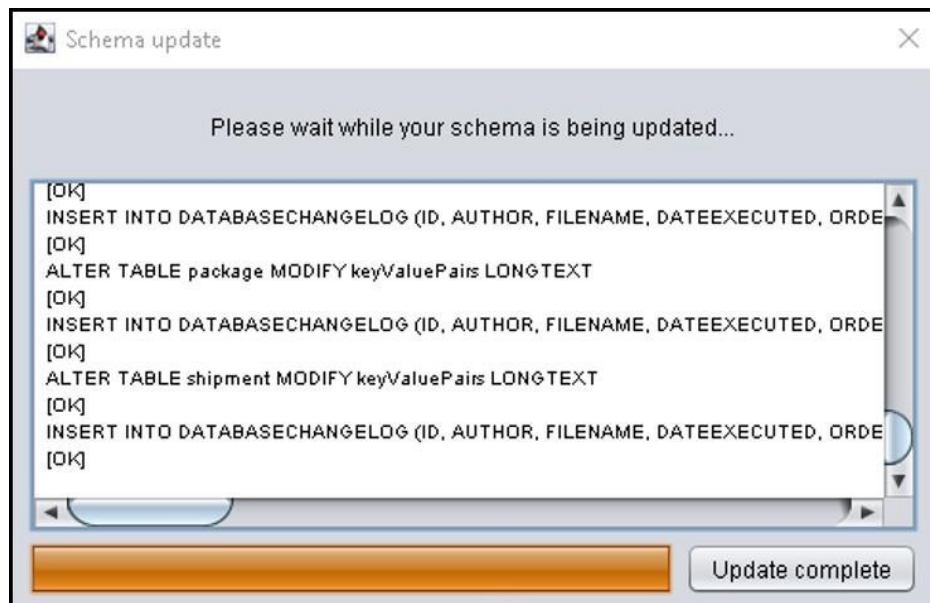
```

1  <?php
2  /*
3  +-----+
4  | FILE DESCRIPTION - Javalin database connection settings
5  +-----+
6  | AUTHORS: aslam sayyed
7  +-----+
8  */
9
10 //mysql didb connection settings
11 define( 'DBHOST', '10.10.108.202' );
12 define( 'DBUSER', 'sn_usr' );
13 define( 'DBPWD', 'shipnowdb' );
14 define( 'USE_ENCRYPTED_PASSWORDS', 'n' );
15 define( 'DIDB', 'didb' );
16
17 //some client may hide the port for security reasons
18 //define( 'DBPORT' , '' );
19 ?>

```

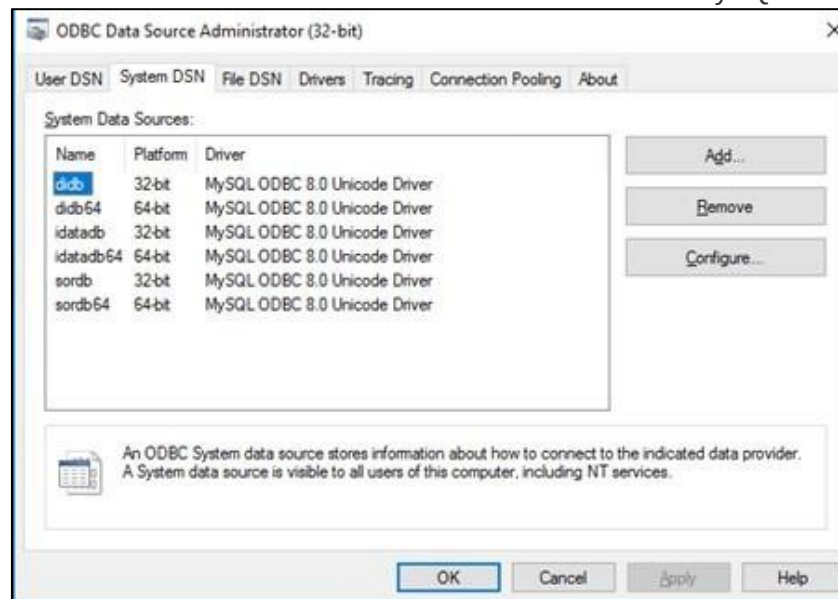
5. For UCM - configure the details in Config.xml file: **ucm/java/META-INF** and Persistence.xml file: **ucm/java/META-INF** (replace localhost and provide Remote MySQL Server IP address and update username and password.)
6. Navigate to <Parcel Install Folder>\Flagship\ucm\java folder, open 'UCM-ServerService-Install.bat' file and replace localhost with Remote MySQL IP address.
7. Open a command prompt using Administrative privileges and navigate to the <Parcel Install Folder>\Flagship\ucm\java folder and then run 'UCM-ServerService-Install.bat' file by passing DBUsername and DBPassword as command line arguments.

For Example: UCM-Server-Service-Install.bat <DBUsername> <DBPassword>The Schema update screen displays, as shown in following screen.



When the Schema update (foreground screen) is complete, the Update complete is activated. Click Update complete to finish the schema upgrade.

8. Do the below modifications as shown in ODBC 32 bit (replace localhost with the Remote MySQL Server IP address.

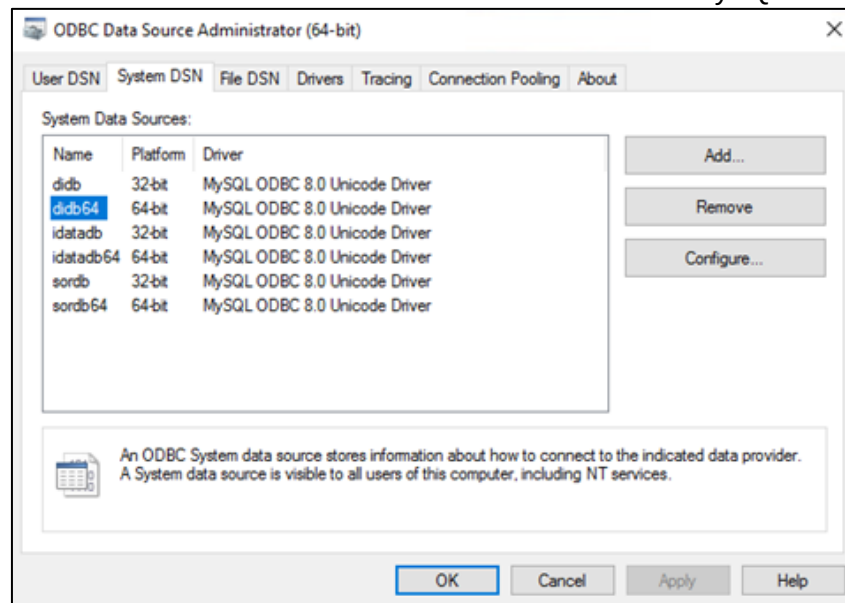


9. Select **didb** and click Configure.
10. In **didb** replace localhost of TCP/IP server and provide Remote MySQL Server IP address, as shown in following screen.



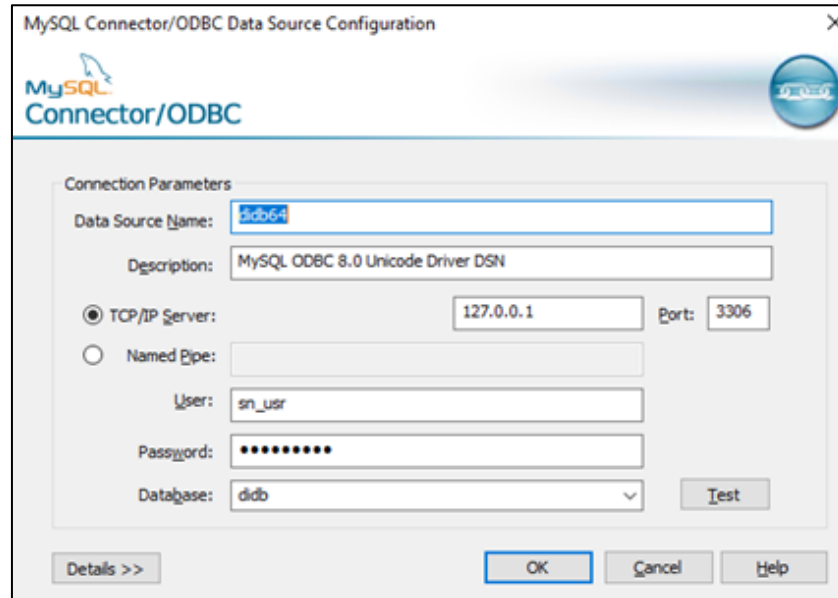
11. Similarly do for **idatadb** and **sordb**.

12. Do the below modifications as shown in ODBC 64 bit (replace localhost with the Remote MySQL Server IP address).



13. Select **didb64** and click Configure.

14. In **didb64** replace localhost of TCP/IP server and provide Remote MySQL Server IP address, as shown in following screen.



15. Similarly do for **idatadb** and **sordb**.

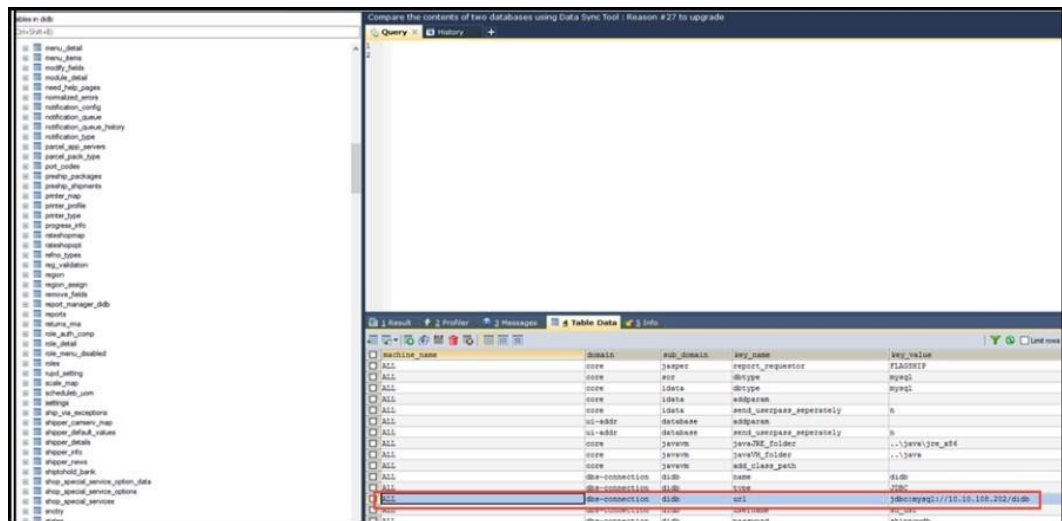
16. Update the following configuration files (files with the .ini extension) in the local <Parcel Artifact Folder>\Flagship\bin folder so that these files point to the remote MySQL server:

a.

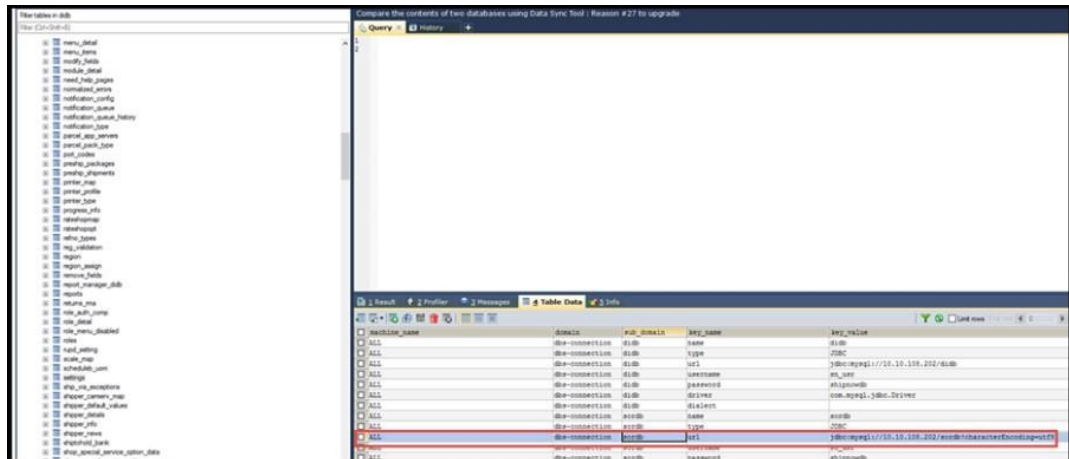
- checkver.ini
- purge.ini
- tracking.ini

Note: Wherever you see "localhost" in these files, substitute the IP address of the MySQL server.

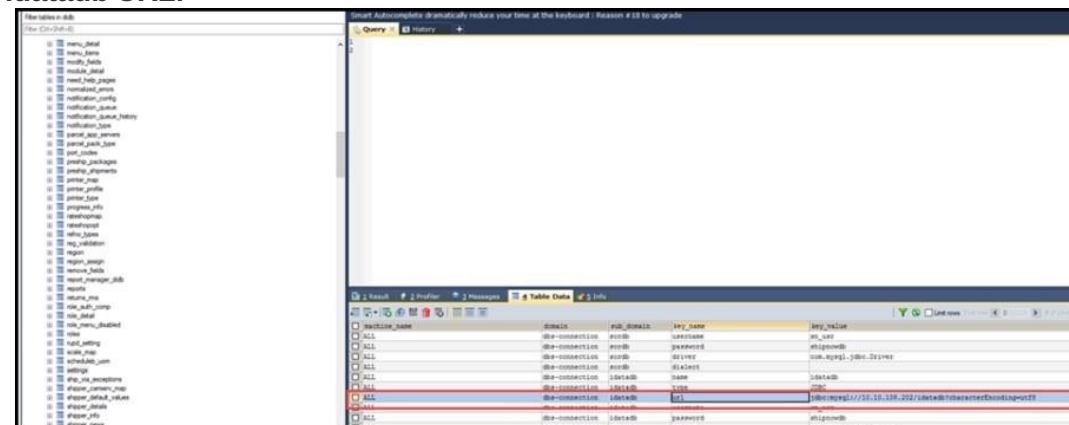
17. Do the below changes in **didb.settings** (replace localhost and provide Remote MySQL Server IP address in Remote MySQL Server) **Didb URL:**



Sordb URL:



Idatadb URL:



Note: Update didb.settings table set key_value with <Parcel Artifact Folder>\Flagship\WebGUI\output where key_name is 'output_dir'

18. Configure Parcel App Servers in Remote MySQL Server (by default localhost will be available)

The screenshot displays the e2open TM-Parcel application. The top navigation bar includes links for Ship, Track, My Profile, System, Workstation, UCM, and Help. The main content area is titled 'System / Parcel App Servers'. On the left, a sidebar shows a tree view of settings, with 'Parcel App Servers' selected. The main panel shows a table with columns for 'Location ID', 'Location Name', 'Parcel Server', and 'Parcel Web Host'. The table contains one entry with 'localhost' in the 'Parcel Server' column and 'http://localhost' in the 'Parcel Web Host' column. Below the table, there is a 'Data Search' window with a query editor and a results table.

Data Search - search and navigate to the respective record in a single click : Reason #72 to upgr

Query: `SELECT * FROM 'settings' WHERE KEY_NAME LIKE "flagship_web_host"`

Results:

Parcel Server	Parcel Web Host
parcel_server	parcel_web_host
10.10.108.144	http://10.10.108.144
10.10.108.202	http://10.10.108.202
localhost	http://localhost

19. Verify the configuration of Parcel App Servers in didb.parcel_app_servers.

After making all the changes Restart MySQL Server in Application Server.

Note: If you are running the Script to add UPS SurePost, update the UPS SurePost activation batch file as follows:

Replace the line "mysql -ufs_admin_user -pF5@dM1nU5er0!1 -f < UPS_SurePost_Activation.sql" with the line below and replace <hostname> with the host name/ip of the remote server

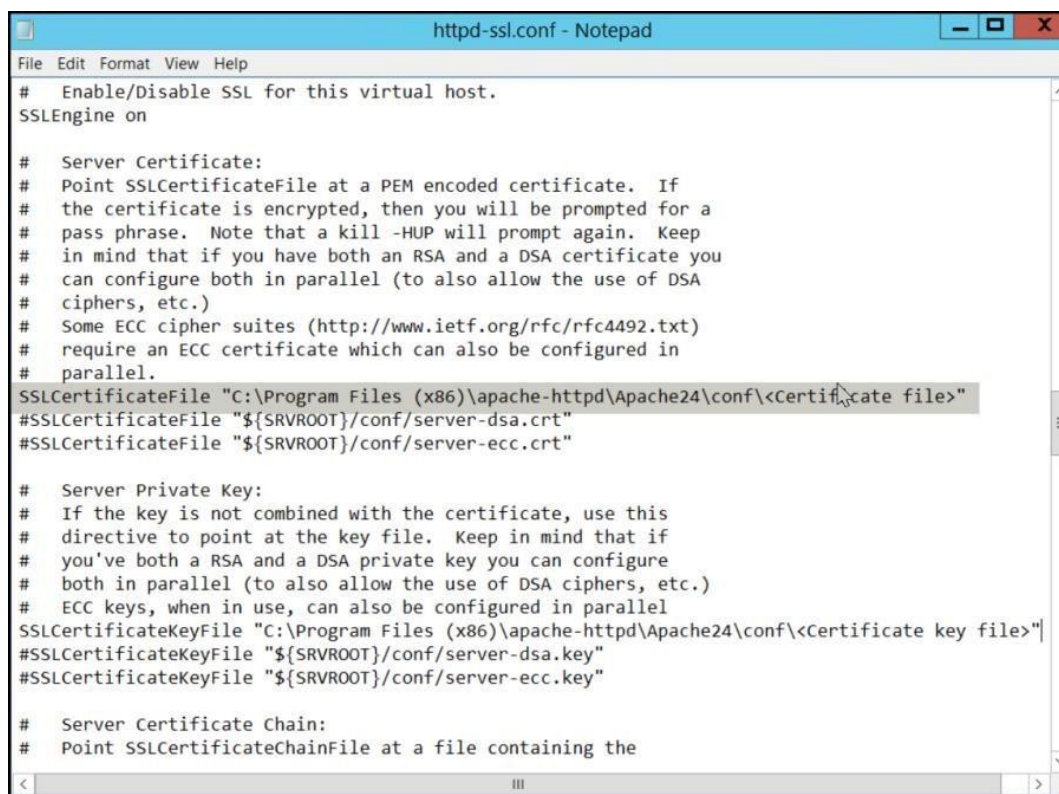
```
mysql -h <hostname> -ufs_admin_user -pF5@dM1nU5er0!1 -f < UPS_SurePost_Activation.sql
```

Post Installation Steps

Configuring HTTPS Certificate on Apache Server

Note: By default, Parcel uses the server.crt and server.key files as certificate in C:\Program Files (x86)\Apache-httpd\Apache24\conf. It is suggested to get the certificates from a certification authority and follow the below steps to deploy:

1. Copy the certificate issued from certification authority to the following location.
C:\Program Files (x86)\Apache-httpd\Apache24\conf
2. Navigate to the following location and open the httpd-ssl.conf file in a text editor:C:\Program Files (x86)\Apache-httpd\Apache24\conf\extra
3. Search for the word 'SSLCertificateFile' and replace the <Certificate file> as per the certificate received from certification authority, as shown below:



```
File Edit Format View Help
# Enable/Disable SSL for this virtual host.
SSL Engine on

# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. Keep
# in mind that if you have both an RSA and a DSA certificate you
# can configure both in parallel (to also allow the use of DSA
# ciphers, etc.)
# Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
# require an ECC certificate which can also be configured in
# parallel.
SSLCertificateFile "C:\Program Files (x86)\apache-httpd\Apache24\conf\<Certificate file>"
#SSLCertificateFile "${SRVROOT}/conf/server-dsa.crt"
#SSLCertificateFile "${SRVROOT}/conf/server-ecc.crt"

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
# ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile "C:\Program Files (x86)\apache-httpd\Apache24\conf\<Certificate key file>"
#SSLCertificateKeyFile "${SRVROOT}/conf/server-dsa.key"
#SSLCertificateKeyFile "${SRVROOT}/conf/server-ecc.key"

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
```

4. Repeat Step 2.
5. Search for the word 'SSLCertificateKeyFile' and replace the <Certificate key file> as per the certificate received from certification authority, as shown below:

```

httpd-ssl.conf - Notepad
File Edit Format View Help
# Enable/Disable SSL for this virtual host.
SSLEngine on

# Server Certificate:
# Point SSLCertificateFile at a PEM encoded certificate. If
# the certificate is encrypted, then you will be prompted for a
# pass phrase. Note that a kill -HUP will prompt again. Keep
# in mind that if you have both an RSA and a DSA certificate you
# can configure both in parallel (to also allow the use of DSA
# ciphers, etc.)
# Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
# require an ECC certificate which can also be configured in
# parallel.
SSLCertificateFile "C:\Program Files (x86)\apache-httpd\Apache24\conf\<Certificate file>"
#SSLCertificateFile "${SRVROOT}/conf/server-dsa.crt"
#SSLCertificateFile "${SRVROOT}/conf/server-ecc.crt"

# Server Private Key:
# If the key is not combined with the certificate, use this
# directive to point at the key file. Keep in mind that if
# you've both a RSA and a DSA private key you can configure
# both in parallel (to also allow the use of DSA ciphers, etc.)
# ECC keys, when in use, can also be configured in parallel
SSLCertificateKeyFile "C:\Program Files (x86)\apache-httpd\Apache24\conf\<Certificate key file>"
#SSLCertificateKeyFile "${SRVROOT}/conf/server-dsa.key"
#SSLCertificateKeyFile "${SRVROOT}/conf/server-ecc.key"

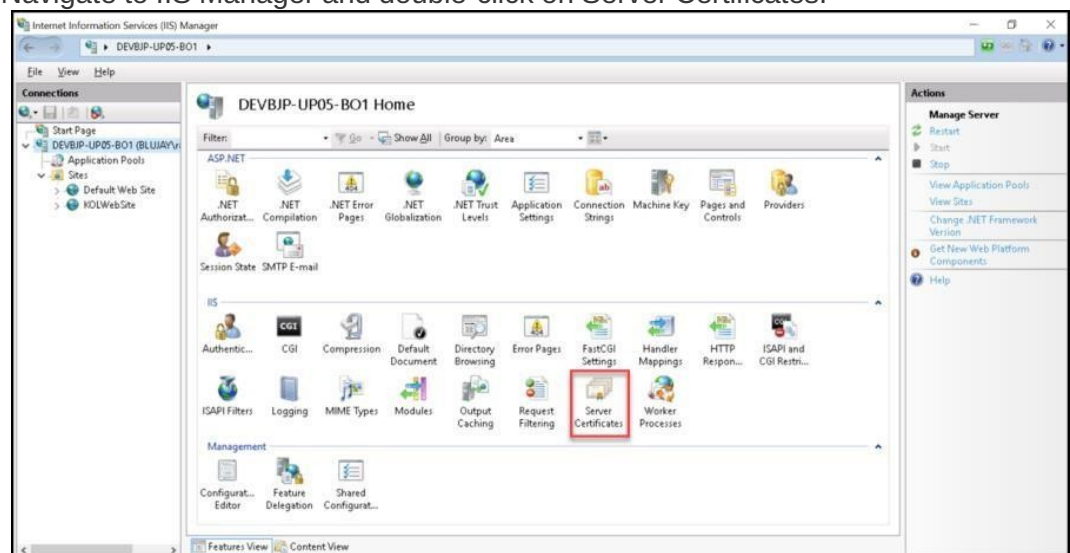
# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the

```

- Restart Apache2.4 Service.

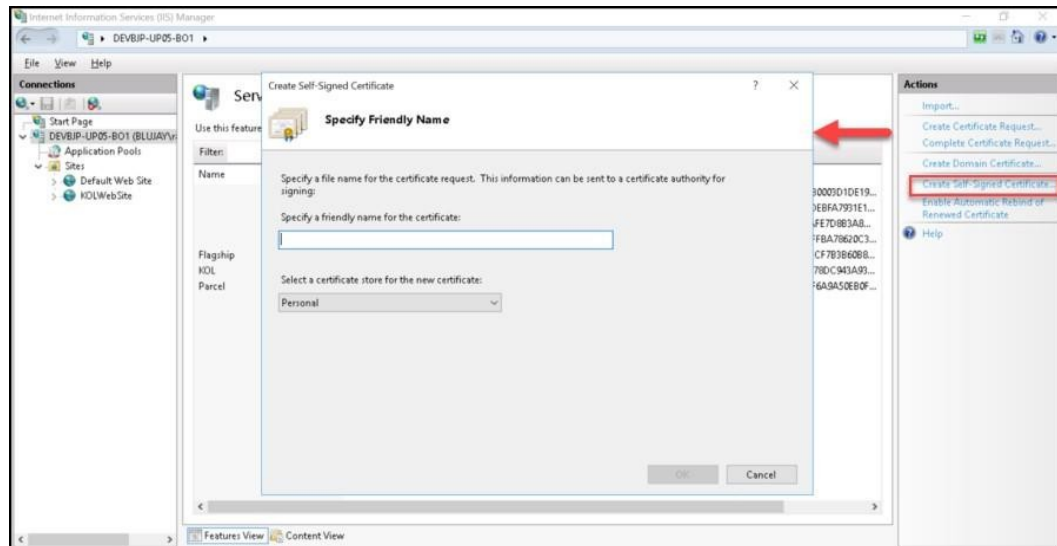
Enabling HTTPS on IIS Server

- Navigate to IIS Manager and double-click on Server Certificates.



- In the Actions panel, click **Create Self-Signed Certificate...**

The Create Self-Signed Certificate dialog box appears, as shown in following screen.

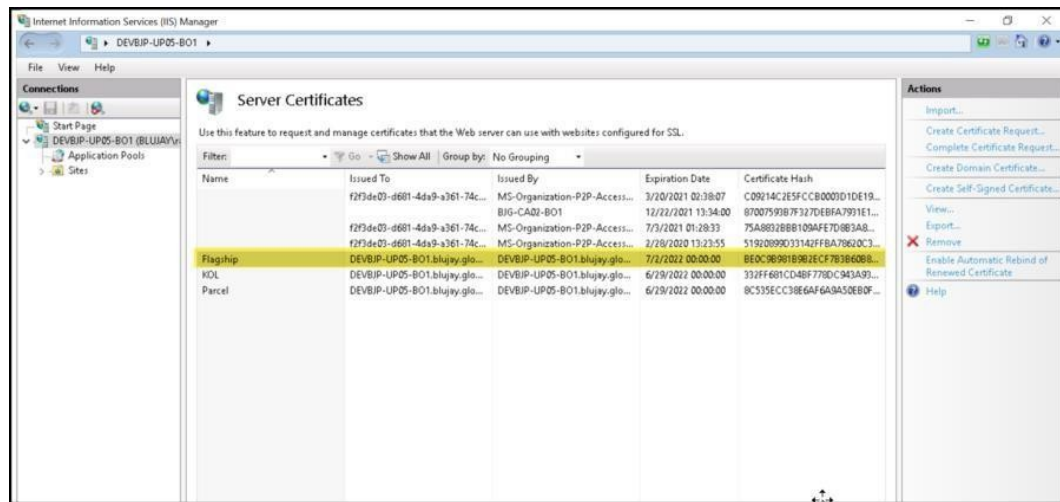


3. Specify a friendly name for the certificate

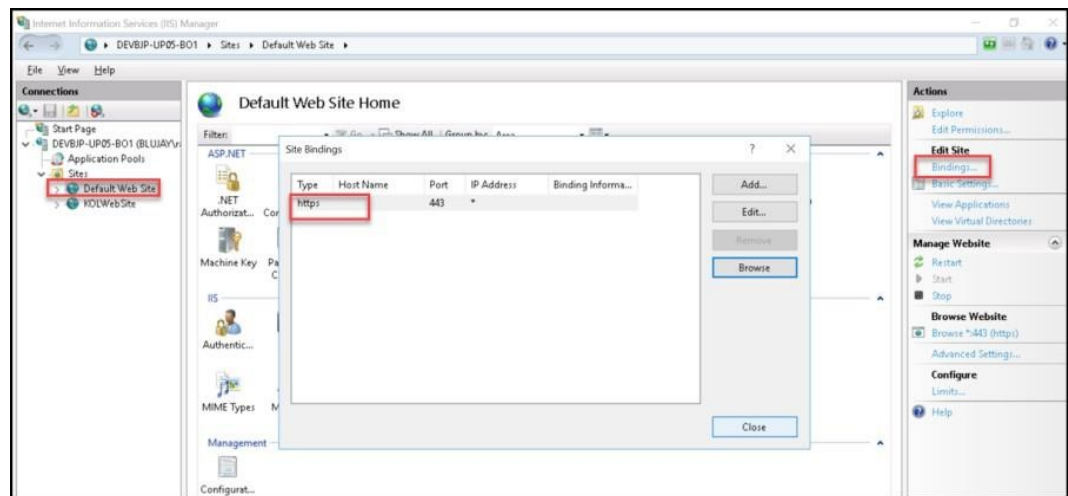
The Create Self-Signed Certificate dialog box appears, as shown in following screen.



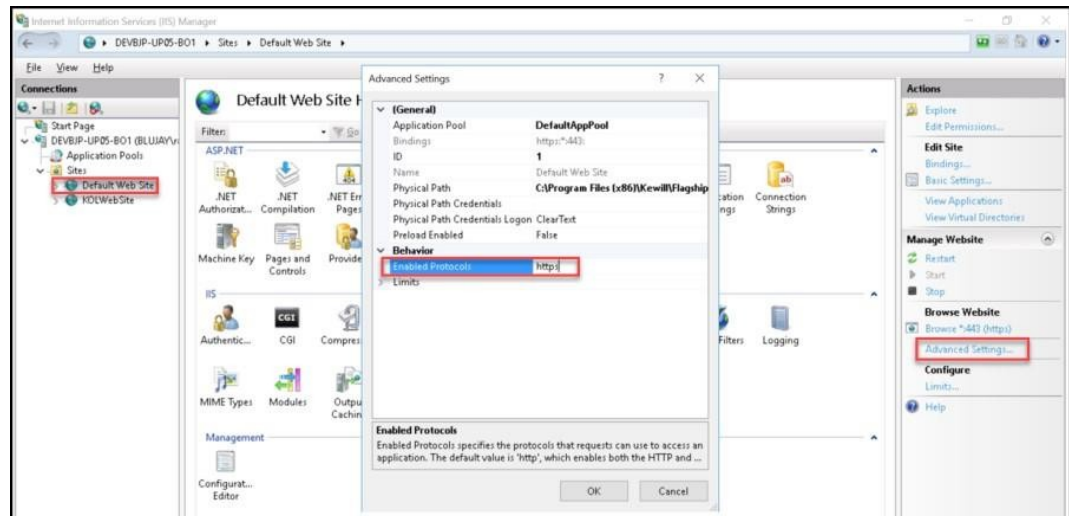
The Self-Signed Certificate is created as shown in following screen.



4. Navigate to Default Web Site, under Actions panel, click **Bindings...** and create new Binding with https, as shown in following illustration.



5. In the Actions panel, click **Advanced Settings** and make sure 'EnabledProtocols' is in https, as shown in following illustration.



- Restart Default Web Site on the IIS Manager.

Configuring HTTPS Certificate for UCM

Note: For testing, use the ucm.p12 (in Flagship Installation directory > ucm > META-INF) and ucm.pem (in Flagship Installation directory > WebGUI > ucm > internal). If not, copy the certificates from certification authority and follow the below steps:

- Update **certificateFilePath** and **certificatePassword** details in <Parcel Artifact Folder>\Flagship\ucm\java\META-INF\config.xml file, as shown below.

```
<https>
  <Enabled>Y</Enabled>
  <CertificateFilePath>./META-INF/ucm.p12</CertificateFilePath>
  <CertificatePassword>blujayucm</CertificatePassword>
</https>
```

- Update **pemFilePath** (Full Path to the certificate) and **pemPassPhrase** in <Parcel Artifact Folder>\Flagship\WebGUI\ucm\internal\pemFile.properties file, as shown below.

```
#If the pem file exists in a different folder then provide full path for the PEM file
#Ex:C:\certificates\ucm.pem (local path)
#\<machinename\IP>\certificates\ucm.pem (remote path)
pemFilePath=C:\Program Files (x86)\Kewill\Flagship\WebGUI\ucm\internal\ucm.pem
pemPassPhrase=blujayucm
```

- Restart BluJayUCMServer Service.

Configuring 64bit DSN

To configure 64bit DSN, follow these steps:

- Open command prompt as administrator.
- Navigate to the installer path. Navigate to \ThirdParty\MySQL folder (Example: C:\Parcel24.1.0_INST_4591\ThirdParty\MySQL).
- Execute "Call ODBC 64-bit.bat" file.

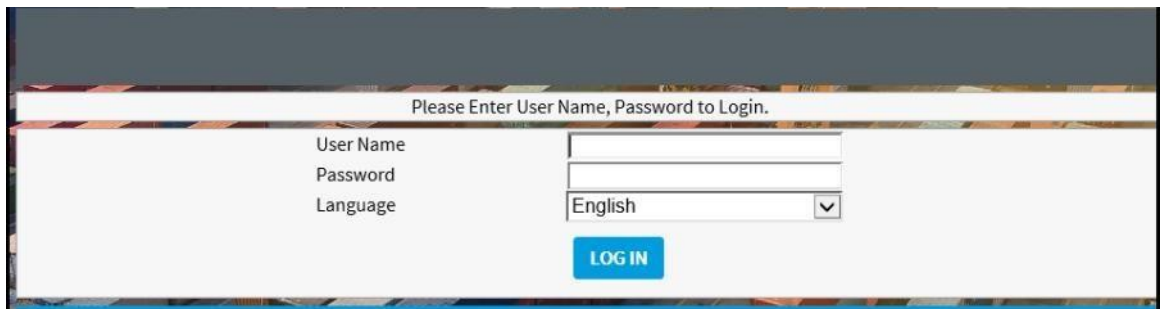
```
C:\Windows\System32\cmd.exe - "Call ODBC 64-bit.bat"
Microsoft Windows [Version 10.0.17763.3887]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\pvarre\Downloads\Parcel23.1.0_INST_4334\ThirdParty\MySQL>"Call ODBC 64-bit.bat"
C:\Users\pvarre\Downloads\Parcel23.1.0_INST_4334\ThirdParty\MySQL>pushd
C:\Users\pvarre\Downloads\Parcel23.1.0_INST_4334\ThirdParty\MySQL>cd "C:\Users\pvarre\Downloads\Parcel23.1.0_INST_4334\ThirdParty\MySQL\"
C:\Users\pvarre\Downloads\Parcel23.1.0_INST_4334\ThirdParty\MySQL>call odbc_64-bit.bat shipnowdb 64-bit
FIND: Parameter format not correct
Press any key to continue . . .
```

Accessing the Parcel Application

To access the Parcel Application, follow these steps:

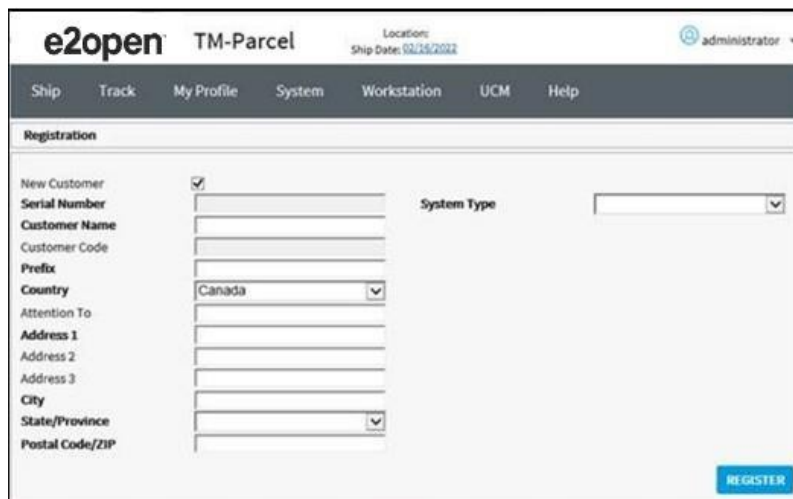
1. Open the Parcel Application using **<https://localhost/login/login.php>** URL.
2. Enter the credentials **User Name** and **Password** and then click LOG IN.



The Registration screen appears.

Registering Parcel

The first time you log in to Parcel, you need to register your installation of the Parcel product. On first login, the following 'Registration' screen is displayed:



To register Parcel, follow these steps:

1. On the 'Registration' screen, enter the following information:

In this field...	Do this...
New Customer	Select this checkbox, to enter the new customer details.
Serial Number	It is non-editable field.
Customer Name	Enter the customer name of the customer. It is mandatory field.
Customer Code	Enter the customer code if you already have one otherwise, leave it blank.
Prefix	Enter the prefix details of the customer. It is mandatory field.
Country	Select the country name of the customer. It is mandatory field.
Attention To	Enter the attention to details of the customer.
Address 1	Enter the address 1 details of the customer. It is mandatory field.
Address 2	Enter the address 2 details of the customer.
Address 3	Enter the address 3 details of the customer.
City	Enter the city details of the customer. It is mandatory field.
Postal Code/Zip	Enter the postal code/zip details of the customer. It is mandatory field.
System Type	Select the required system type: Test or Production of the customer from drop-down list. It is mandatory field.

- Click REGISTER. After you successfully register, a confirmation message **"Product Registered successfully"** appears with a 16 character Serial Number and Customer Code details, as shown in the following illustration:

The screenshot displays the e2open TM-Parcel web interface. At the top, the header includes the e2open logo, 'TM-Parcel', and user information: 'Location: Ship Date: 02/17/2022' and 'administrator'. A navigation bar contains links: Ship, Track, My Profile, System, Workstation, UCM, and Help. A green banner across the page reads 'Product Registered successfully.' Below this, a 'Registration' section contains the following details:

Serial Number	F41641A3C25EA3B4	System Type	Test
Customer Name	PARCEL_TEST		
Customer Code	MR. TEST180235293		
Country	United States		
Address 1	STREET 2		
Address 2	TEST LOCALE		
City	CHELMSFORD		
State/Province	Massachusetts		
Postal Code/ZIP	01824		

Now, the system is ready to use.

Note: Please save your registration details.

Importing UPS World Wide Validation Data

The UPS Worldwide Validation (WWV) Distribution is a set of data files distributed monthly by UPS that a customer can be import into Parcel.

To import the UPS Worldwide Validation files, carry out the following steps:

- Extract the files from the UPS-supplied zip file into a directory on your Application Server.
- In the Parcel Configuration (Web Admin) tool, under the UPS carrier for which you want to import these files, click Data Import to open the Import screen. (See illustration below.)
- Specify the information on this screen as follows:

In this field....	Type this....
Import Date	The World Wide Validation Effective Date in YYYYMMDD format; for example: April 06, 2022 is rendered as "20220406"– (without quotation marks). This is mandatory field for World Wide Validation import.
World Wide Validation Data Directory	The full (absolute) path to the folder to which you extracted the World Wide validation zip file. For Example: C:\WWV_Files

Keep previous World Wide Validation Data	Select this checkbox to keep previous World Wide Validation Data, otherwise it will be purged.
Billable Weight Determination Data Directory	The full (absolute) path to the folder to which you extracted the UPS file. For Example: C:\BW_Files
Peak/Demand Surcharge Data Directory	The full (absolute) path to the folder to which you extracted the UPS Peak Surcharge zip file. For Example: C:\PS_Files

4. Save to import the files or click CANCEL to cancel out of this screen.

Parcel UPS WW Validation Data Directory Import screen

The screenshot shows the e2open TM-Parcel interface. The top navigation bar includes 'Ship', 'Track', 'My Profile', 'System', 'Workstation', 'UCM', and 'Help'. The breadcrumb trail is 'System / US Smoke Test Location / Carriers / UPS / Data Import'. The left sidebar lists various settings, with 'Data Import' under the 'UPS' section highlighted. The main content area has the following fields:

- Import Date: [Text Field]
- World Wide Validation Data Directory: [Text Field]
- Keep previous World Wide Validation Data: ☐ Enable
- Billable Weight Determination Data Directory: [Text Field]
- Peak/Demand Surcharge Data Directory: [Text Field]
- VCI Type Data Directory: [Text Field]

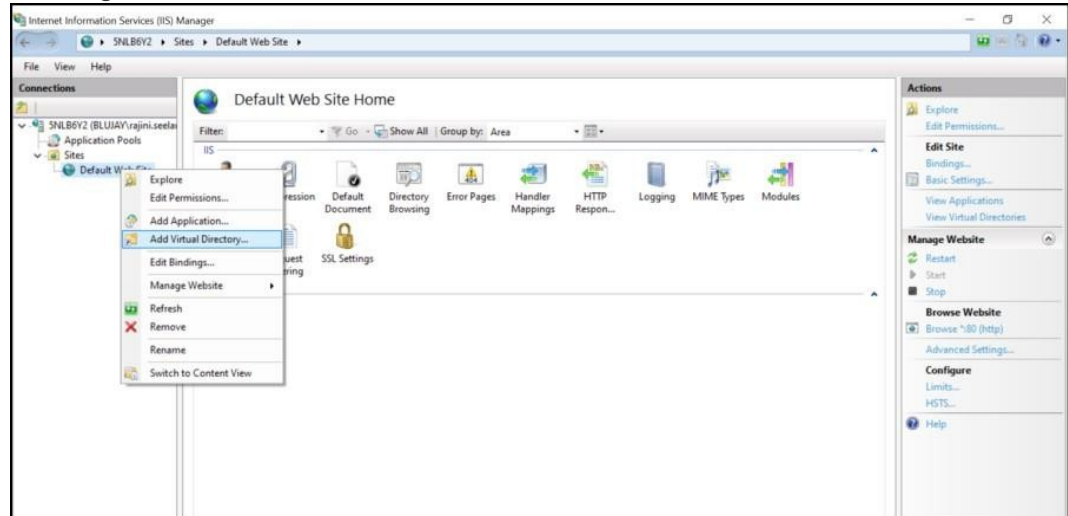
At the bottom right, there are 'CANCEL' and 'SAVE' buttons.

Add/Update Virtual Directory in IIS

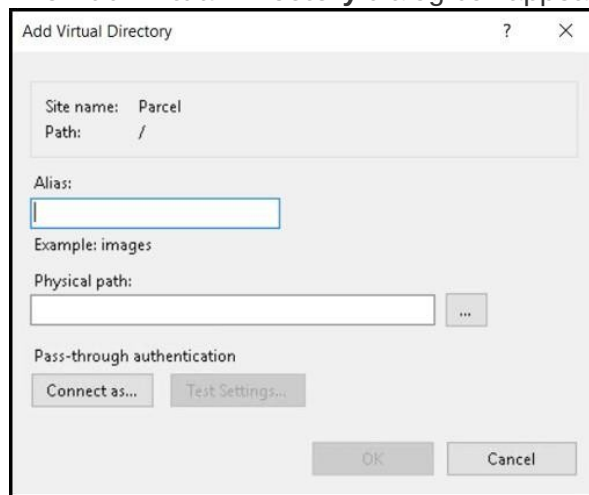
The Virtual Directory in IIS is used for viewing the labels and reports. This section describes about to how add and update the virtual directory in IIS. To add virtual directory in IIS, follow these steps:


1. Navigate to IIS Manager.

2. In the **Connections** pane, expand the Server Name, expand **Sites** node, click Default Web Site, as shown in following screen.
3. Right-click on the Default Web Site, and then click **Add Virtual Directory...** , as shown in following screen.



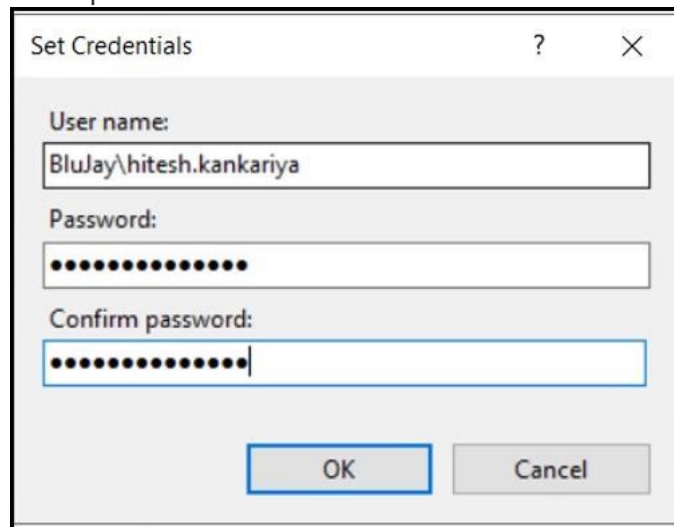
The **Add Virtual Directory** dialog box appears, as shown in following screen.



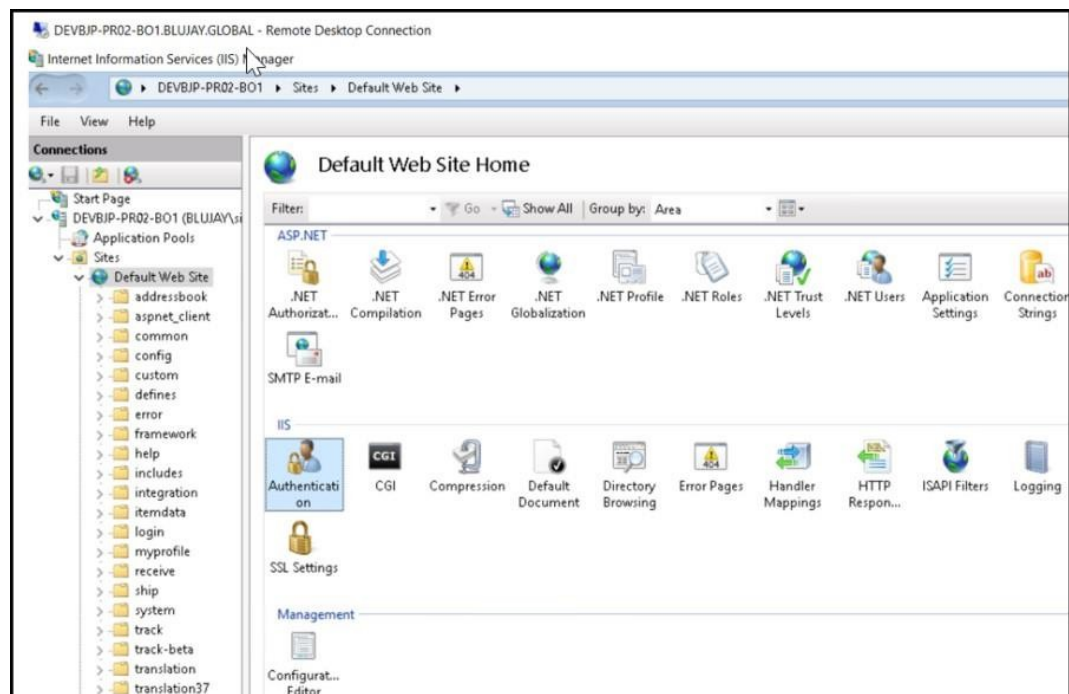
4. In **Alias:** field, enter "parceloptions".
5. In **Physical path:** field, click  and browse for Parcel Artifact Folder Path.
For Example: C:\Parcel Artifact Folder
6. Click Connect as
7. The Edit Anonymous Authentication Credentials dialog box appears, as shown in the following screen.



8. The Set Credentials dialog box appears.
9. In the Set Credentials dialog box, enter Username, Password and Confirm Password in the respective fields and then click OK

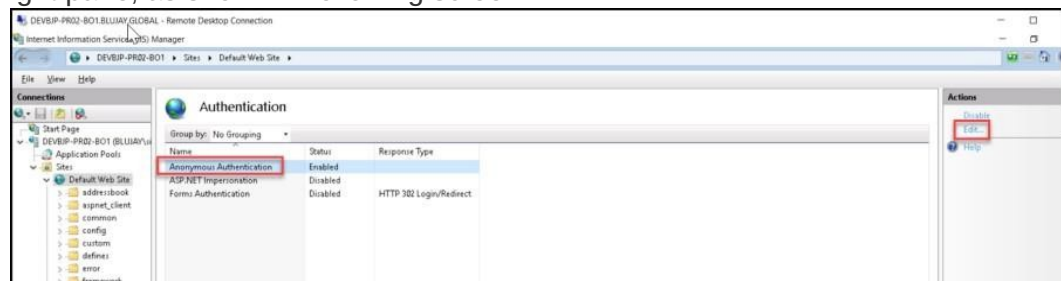


10. Click OK in the Add Virtual Directory dialog box.
11. Click Default Web Site and then double-click on **Authentication** on in the rightpane, as shown in following screen.



The Authentication screen displays.

12. In Authentication screen, select **Anonymous Authentication** and then click **Edit...** in the right pane, as shown in following screen.



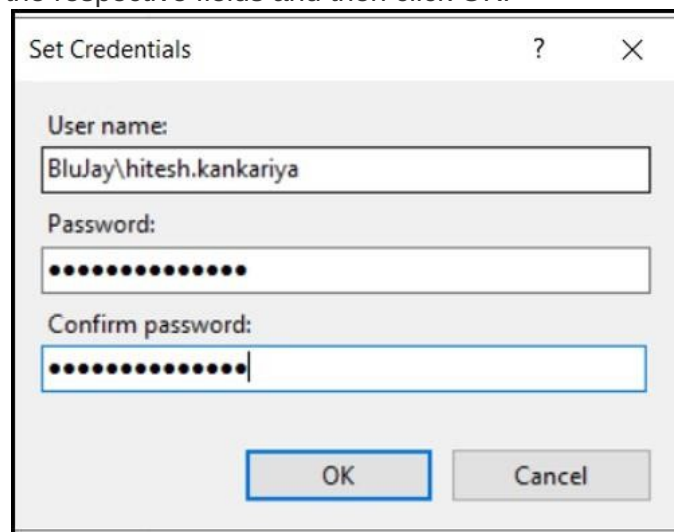
The Edit Anonymous Authentication Credentials dialog box appears.

13. In Edit Anonymous Authentication Credentials dialog box, select Specify user option and click Set and then click OK, as shown in following screen.



The Set Credentials dialog box appears.

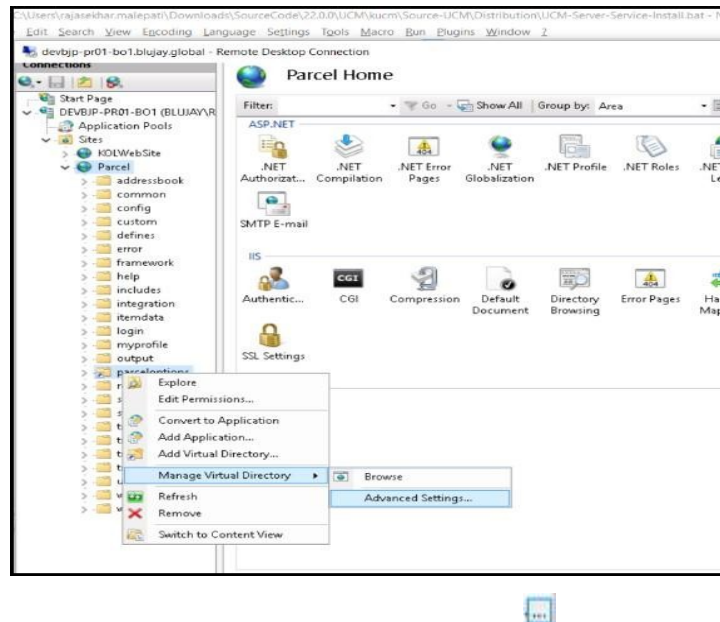
14. In the Set Credentials dialog box, enter Username, Password and Confirm Password in the respective fields and then click OK.



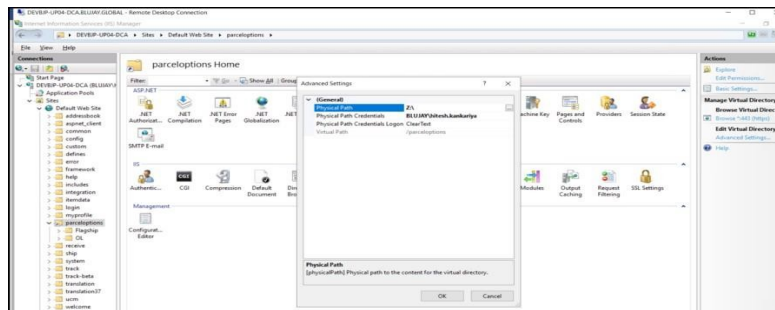
15. Click OK
16. Restart IIS Service.

To update virtual directory in IIS, follow these steps:

1. Right-click on the created virtual directory, click Manage Virtual Directory > Advanced Settings.
2. In the Advanced Settings window, click next to the **Physical Path** and choose the new Parcel Artifact Folder path and then click OK

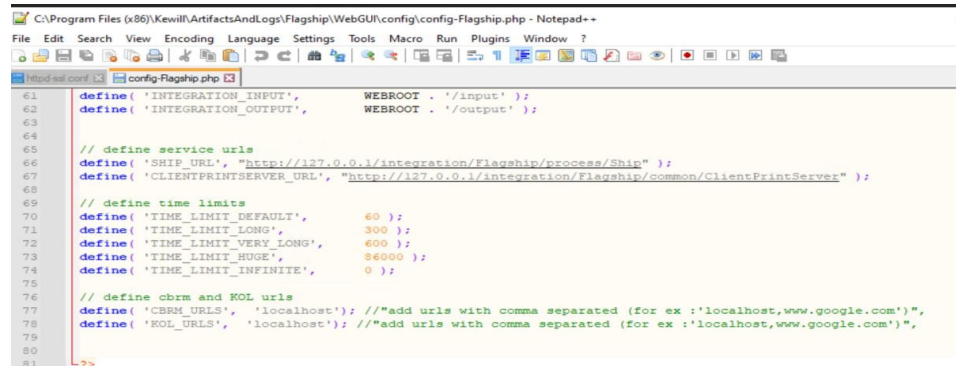


3. Restart IIS Service.



Add/Update KOL and CBRM URLs

1. By default 'localhost' value would be available in the file. The machine name and IP would be whitelisted and should work without adding in the file.
2. If user wants to add any other URL, they can add multiple machine name and IPs with comma separated in the file at path (Line # 77 and 78) -
 ./<Artifact location>/ Flagship/WebGUI/config/config-Flagship.php



Additional Optional Steps

Configuring an External Database

Overview - Running Batch Files & Scripts

Parcel uses a MySQL database for internal application purposes. However, you can also configure an external database to work with Parcel. You can then connect to this database from within Parcel to access corporate data on shipping history, events, addresses, and related matters. Currently, Parcel supports the following database types (in addition to MySQL, installed with Parcel):

- SQL Server (Microsoft)
- Oracle

Note: The size of the Carrier and Service columns in the SOR schema is increased to 20 characters. The appropriate upgrades must be applied for Oracle and Microsoft SQL Server SOR databases.

Note on Changing SOR Database Type

When changing a MySQL SOR database to an Oracle SOR database, you first need to place the Oracle ojdbc14.jar file in the local Java\lib\database folder.

When changing a MySQL SOR database to an MSSQL SOR 2019 database, you first need to place the mssql-jdbc-7.4.1.jre8.jar file in the local Java\lib\database folder.

Location and Function of Scripts and Batch Files

To configure a database other than MySQL, sets of SQL scripts provided with your Parcel installation needs to be run. There are two sets of these SOR scripts, one set for each database type, in separate folders labeled according to the database (see the following table). The code in the scripts is customized according to database type. These SQL scripts, together with the batch files for running them are installed into the following folders under your BluJay Solutions installation folders:

For Database Type...	Script folders location is...
Oracle	<Parcel Install Folder>\Flagship\DBUpdate\SOR\ORACLE\ For Example: C:\Program Files (x86)\Kewill\Flagship\DBUpdate\SOR\ORACLE\
SQL Server	<Parcel Install Folder>\Flagship\DBUpdate\SOR\MSSQL\ For example: C:\Program Files (x86)\Kewill\Flagship\DBUpdate\SOR\MSSQL\

These folders contain the following subfolders with the actual scripts for the respective Parcel versions (starting with 4.0 to 24.1.0) and databases:

- \UPGRADES\4.0.000
- \UPGRADES\4.1.000
- \UPGRADES\4.1.004

- \UPGRADES\4.1.006
- \UPGRADES\5.0.000
- \UPGRADES\5.2.000
- \UPGRADES\6.0.000
- \UPGRADES\6.0.001
- \UPGRADES\6.0.002
- \UPGRADES\7.0.000
- \UPGRADES\17.0.000
- \UPGRADES\19.2.000
- \UPGRADES\21.1.0
- \UPGRADES\21.2.0
- \UPGRADES\22.4.0
- \UPGRADES\23.4.0
- \UPGRADES\24.1.0

Note: The various Sequel scripts called by these batch files configure the database as follows:

- Create tables for audit history, Corporate Address book and groups, and event log.
- Create System of Record (SOR) tables for shipments and shipment headers, items, and packages.
- Create IData storage areas for shipments, packages, and items.
- Set the version stored in the database version table.

Using Batch Files to Run Scripts

The Oracle and SQL Server folders contain batch files that run this set of SQL scripts automatically:

For Database Type...	SOR Batch File Path Name (Relative) and Filename...
Oracle	.\DBUpdate\SOR\ORACLE\InstallDB_ORACLE_SOR.bat
SQL Server	..\DBUpdate\SOR\MSSQL\InstallDB_SOR.bat ..\DBUpdate\SOR\MSSQL\UpdateDB_SOR.bat

Notes:

- Each of these batch files in turn calls another batch file in a subfolder and directs that batch file to operate on the corresponding database. Thus, *before running these batch files, you must first customize* them to connect to the database as described in the following subsections.
- Note that there are both an Install and an Update batch files for SQL Server. *Run the Update file only when upgrading Parcel with a patch release.*

Customizing Installation batch file for Oracle

To customize the Installation batch file for Oracle, follow these steps:

1. In the `..\DBUpdate\SOR\ORACLE\FULL_41` folder, open the following file for editing by right-clicking on the filename, and then selecting Edit from the Pop-up menu:
Install_SOR_Oracle.bat file - InstallDB_ORACLE_SOR.bat
2. Find the following line: `CALL Install_SOR_ORACLE TNS USERNAME PASSWORD`
3. For the parameters TNS USERNAME PASSWORD (meant to serve as placeholders only) make the following substitutions:

```
CALL Install_SOR_ORACLE <Actual_TNS_Name_of_Oracle_instance>  
<Actual_User_Name> <Actual_Password>
```

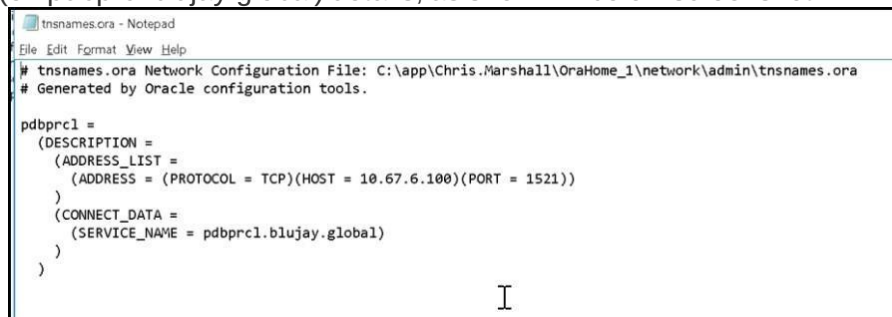
Changing SOR from MySQL to Oracle

To change the SOR from MySQL to Oracle, follow these steps:

1. Download **instantclient_19_9.zip** file from the Parcel Server and extract the contents from the zip file to a local system.

For Example: C:\ drive.

2. Set Environment Variables:
 - a. SET PATH=C:\instantclient_19_9;%PATH% for finding the executables.
 - b. SET TNS_ADMIN=C:\instantclient_19_9 for finding the tnsnames.ora file.
 - c. SET LD_LIBRARY_PATH=C:\instantclient_19_9 for finding the shared libraries shipped with Instant Client.
3. Navigate to C:\instantclient_19_9 path and open 'tnsnames.ora' in Notepad and update the HOST (ex: 10.67.6.100), PORT (ex:1521) and SERVICE_NAME (ex:pdbrcl.blujay.global) details, as shown in below screenshot.

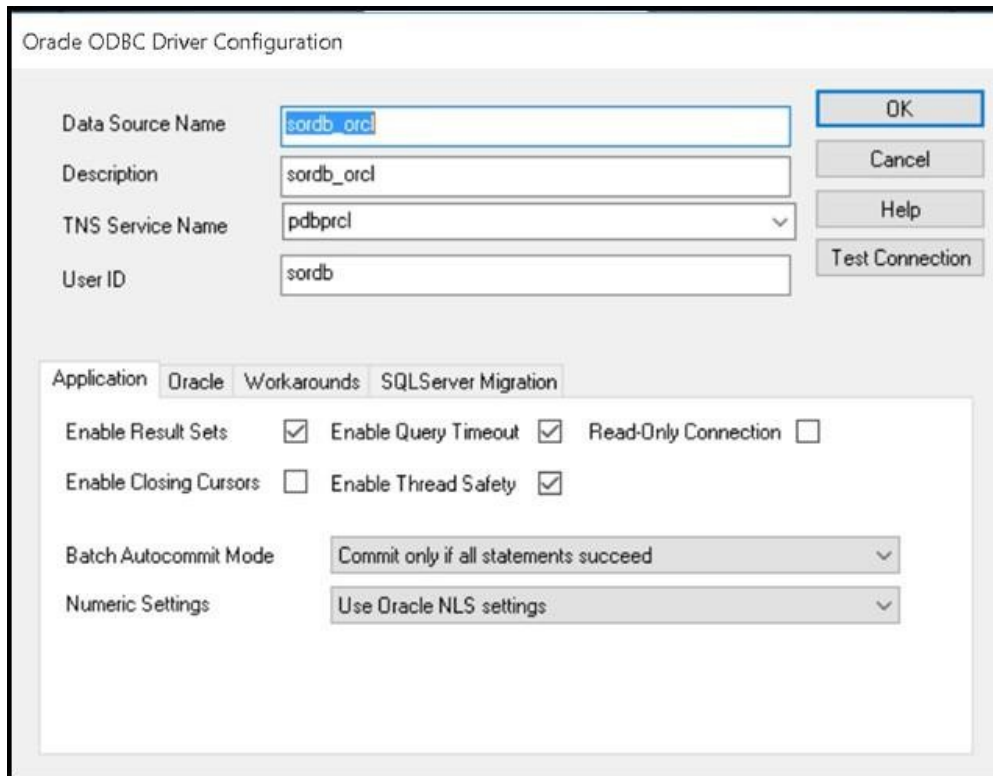


4. Navigate to C:\instantclient_19_9 path and run 'odbc_install.exe'.
5. Open the ODBC Data Source Administrator (32-bit) screen, select the **System DSN** tab and then click Add.

The Oracle ODBC Driver Configuration screen displays, as shown in following illustration.


6. In Oracle ODBC Driver Configuration screen, complete the fields as shown in following table for **sordb** and then click OK.

In this field...	Do this...
Data Source Name	Enter the data source name. For Example: sordb_orcl
Description	Enter the description. For Example: sordb_orcl
TNS Service Name	Select the TNS Service Name from drop-down list.
UserID	Enter the sordb User ID. For Example: sordb



The Oracle ODBC Driver Configuration dialog box is shown. It has a title bar 'Oracle ODBC Driver Configuration'. The 'Data Source Name' field contains 'sordb_orcl'. The 'Description' field contains 'sordb_orcl'. The 'TNS Service Name' dropdown menu is set to 'pdbprcl'. The 'User ID' field contains 'sordb'. On the right side, there are buttons for 'OK', 'Cancel', 'Help', and 'Test Connection'. Below these fields, there is a tabbed interface with 'Application', 'Oracle', 'Workarounds', and 'SQLServer Migration' tabs. The 'Application' tab is selected, showing options for 'Enable Result Sets' (checked), 'Enable Query Timeout' (checked), 'Read-Only Connection' (unchecked), 'Enable Closing Cursors' (unchecked), and 'Enable Thread Safety' (checked). The 'Batch Autocommit Mode' dropdown is set to 'Commit only if all statements succeed'. The 'Numeric Settings' dropdown is set to 'Use Oracle NLS settings'.

- Click Test Connection to test the sordb connectivity to the database, the Oracle ODBC Driver Connect dialog box appears, as shown in following illustration



The Oracle ODBC Driver Connect dialog box is shown. It has a title bar 'Oracle ODBC Driver Connect'. The 'Service Name' field contains 'pdbprcl'. The 'User Name' field contains 'sordb'. The 'Password' field is filled with 12 dots. On the right side, there are buttons for 'OK', 'Cancel', and 'About...'.

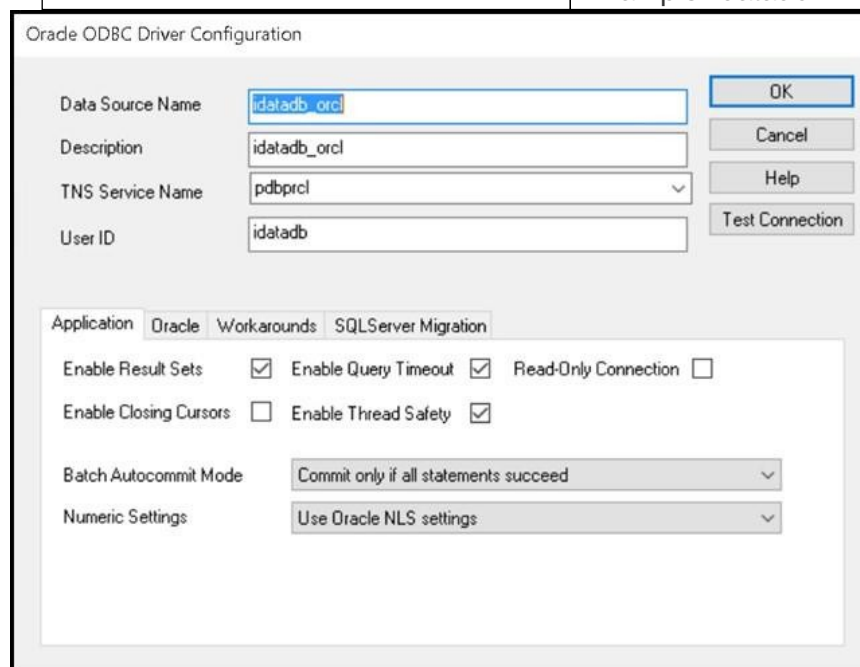
Note: By default, the **Service Name** and **User Name** fields are filled with details.

- Enter Password in *Password* field and then OK.
The 'Connection successful' message appears, as shown in following screen.



9. Similarly complete the fields for idatadb, as shown in following table and then click OK.

In this field...	Do this...
Data Source Name	Enter the data source name. For Example: idatadb_orcl
Description	Enter the description. For Example: idatadb_orcl
TNS Service Name	Select the TNS Service Name from drop-down list.
UserID	Enter the idatadb User ID. For Example: idatadb



10. Click Test Connection to test the idatadb connectivity to the database and enter password in the **Password** field and then click OK.
11. Do the changes in **didb.settings**, as shown in following table:

a. **SORDB**

domain	sub_domain	key_name	key_value
core	sor	dbtype	Change from mysql to oracle.
core	sor	dsn	Enter dsn name. For example: sordb_oracl
core	sor	user id	Enter the user id. For example: sordb
core	sor	password	Enter the password. For example: LyFva55hVGfPF56s
core	sordb	name	Enter the sordb name. For example: sordb
core	sordb	username	Enter the sordb username. For example: sordb
core	sordb	password	Enter the sordb password. For Example: LyFva55hVGfPF56s
core	sordb	driver	Change to oracle.jdbc.OracleDriver
core	sordb	url	Enter the URL in jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS=(PROTOCOL=tcps)(PORT=portnumber)(HOST=oracleserveripaddress))(CONNECT_DATA=(SERVICE_NAME=portnumber/servicename))) format. For Example: jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS=(PROTOCOL=tcps)(PORT=1525)(HOST=10.67.8.49))(CONNECT_DATA=(SERVICE_NAME=pdbprcl2.blujay.global))) Note: For SSL connection PROTOCOL should be tcps for non-SSL connection PROTOCOL should be tcp, port number also change based on ssl or non-ssl connection.

domain	sub_domain	key_name	key_value
dbconnection	sordb	trustStore_path	Enter the trustStore path. For Example: C:\client_wallet\client_wallet\cwallet.sso Note: trustStore_path should be the cwallet.sso file path, this is mandatory for ssl connection (tcps)
dbconnection	sordb	trustStore_password	Null Note: trustStore_password is not required for oracle ssl connection.
dbconnection	sordb	use_secure_encryption	Set this flag to 'y' to turn on for ssl connection (tcps). Valid values are: <ul style="list-style-type: none"> • y • n By default, this key is set to 'n'.

machine_name	domain	sub_domain	key_name	key_value
ALL	core	sor	dsn	#ordb_oracle
ALL	core	sor	user id	sordb
ALL	core	sor	password	LyFva5ShVGfPF56e
ALL	core	sor	enable_batch_log	n
ALL	core	sor	addparam	
ALL	core	sor	send_userpass_seperately	n
ALL	core	sor	dbtype	oracle
ALL	dba-connection	sordb	name	sordb
ALL	dba-connection	sordb	type	JDBC
ALL	dba-connection	sordb	uri	jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS=(PROTOCOL=tcps) (P...
ALL	dba-connection	sordb	username	sordb
ALL	dba-connection	sordb	password	LyFva5ShVGfPF56e
ALL	dba-connection	sordb	driver	oracle.jdbc.OracleDriver
ALL	dba-connection	sordb	dialect	
ALL	dba-connection	sordb	trustStore_path	C:\client_wallet\client_wallet\cwallet.sso
ALL	dba-connection	sordb	trustStore_password	
ALL	dba-connection	sordb	use_secure_encryption	y

b. IDATADB

domain	sub_domain	key_name	key_value
core	idata	dbtype	Change from mysql to oracle.
core	idata	dsn	Enter dsn name. For example: idatadb_oracle
core	idata	user id	Enter the user id. For example: idatadb

domain	sub_domain	key_name	key_value
core	idata	password	Enter the password. For example: uygSCupx9n7J56Av
core	idatadb	name	Enter the idatadb name. For example: idatadb
core	idatadb	username	Enter the idatadb username. For example: idatadb
core	idatadb	password	Enter the idatadb password. For Example: uygSCupx9n7J56Av
core	idatadb	driver	Change to oracle.jdbc.OracleDriver

domain	sub_domain	key_name	key_value
core	idatadb	url	<p>Enter the URL in</p> <p>For Example:</p> <p>jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(PORT=portnumber)(HOST=oracleserveripaddress))(CONNECT_DATA=(SERVICE_NAME=portnumber/servicename))) format.</p> <p>jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(PORT=1525)(HOST=10.67.8.49))(CONNECT_DATA=(SERVICE_NAME=pdbprcl2.blujay.global)))</p> <p>Note: For SSL connection PROTOCOL should be tcps for non-SSL connection PROTOCOL should be tcp, port number also change based on ssl or non-ssl connection.</p>
domain	sub_domain	key_name	key_value

db connection	db	trustStore_path	Enter the trustStore path. For Example: C:\client_wallet\client_wallet\cwallet.sso Note: trustStore_path should be the cwallet.sso file path, this is mandatory for ssl connection (tcps)
db connection	db	trustStore_password	Null Note: trustStore_password is not required for oracle ssl connection.
db connection	db	use_secure_encryption	Set this flag to 'y' to turn on for ssl connection (tcps). Valid values are: • y • n By default, this key is set to 'n'.

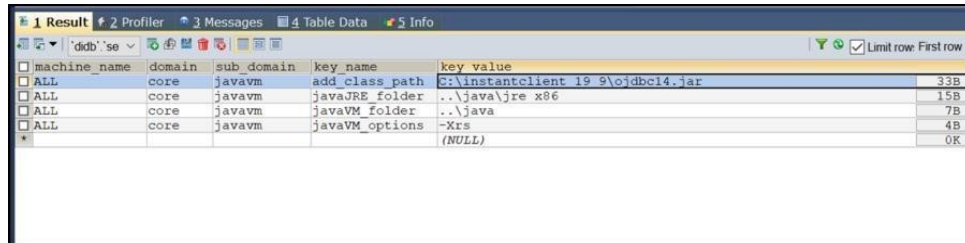
machine_name	domain	sub_domain	key_name	key_value
ALL	ui-app	idatadb	query_fromhold	N
ALL	core	idatadb	dsn	idatadb_oracle
ALL	core	idatadb	password	uygSCupx9n7J56Av
ALL	core	idatadb	user id	idatadb
ALL	core	idatadb	dbtype	oracle
ALL	core	idatadb	addparam	
ALL	core	idatadb	send_userpass_seperately	n
ALL	db connection	idatadb	name	idatadb
ALL	db connection	idatadb	type	JDBC
ALL	db connection	idatadb	url	jdbc:oracle:thin:@(DESCRIPTION= (ADDRESS= (PROTOCOL=tcps) (P...
ALL	db connection	idatadb	username	idatadb
ALL	db connection	idatadb	password	uygSCupx9n7J56Av
ALL	db connection	idatadb	driver	oracle.jdbc.OracleDriver
ALL	db connection	idatadb	dialect	
ALL	db connection	idatadb	trustStore_path	C:\client_wallet\client_wallet\cwallet.sso
ALL	db connection	idatadb	trustStore_password	
ALL	db connection	idatadb	use_secure_encryption	y

c. JAVAVM

Copy and place the ojdbc.14.jar file in C:\ drive and define the path in add_class_path

domain	sub_domain	key_name	key_value
--------	------------	----------	-----------


core	javavm	add_class_path	C:\instantclient_19_9\odbc14.jar
------	--------	----------------	----------------------------------



machine_name	domain	sub_domain	key_name	key_value	
ALL	core	javavm	add_class_path	E:\instantclient_19_9\odbc14.jar	33B
ALL	core	javavm	javaJRE_folder	..\java\jre x86	15B
ALL	core	javavm	javaVM_folder	..\java	7B
ALL	core	javavm	javaVM_options	-Xrs	4B
*				(NULL)	OK

12. Restart Kewill DiServer Service, KewillFlagshipConnectorFileService and KewillFlagshipDatabaseFileService Services.

Note: If Parcel is installed in IIS Environment, Restart IIS Service. **Configuring the didb.settings table**

1. You can use Parcel's Web Admin tool to update the Parcel didb.settings table for use with your external database. (This procedure assumes you are using the Parcel Web Admin tool. Alternatively, you can use SQLyog or another database administration tool to enter the values directly in the database.)
2. In Parcel, select System > Locations > Global Settings > Settings, and make the following entries in the Settings table by clicking the plus () icon in the upper left corner. Note that for all the entries, the value for machine_name is "ALL" (uppercase, no quotes). The display_name field is the description. The remaining column names and values (shown without quotes) are given in the following table:

domain	sub_domain	key_name	key_value	display_name
core	sor	dsn	Didb	SOR DSN Name
				ODBC DSN
				Setup in Windows]
domain	sub_domain	key_name	key_value	display_name

core	sor	user id	<User_ID> for example: sn_usr	SOR database user name User Name set up in external database]
core	sor	password	<Password> for example: shipnowdb	SOR database password Password set up in external database]
core	javavm	add_class_pa th		Class path for Java Virtual Machine

3. Add the class path for the Java Virtual Machine (.jar file) as follows:

domain: core **sub_domain:**

javavm **Key_name:**

add_class_path

key_value: ..\java\lib\database\<javavm_filename>.jar **For**

Example: ..\java\lib\database\mssql-jdbc-7.4.1.jre8.jar

Where the path name is the relative path under the BluJay Solutions installation folder.

Note: The Java Virtual Machine is not included in your BluJay Solutions installation. You must download this from the Sun Microsystems Java Web site separately.

4. If you have instances of the external database in addition to the default, add the URL for the database server and the instance name of the database as follows:

domain: dbs-connection

sub_domain: sordb

Key_name: url **key_value:**

jdbc:<database_type>://<server_IP_address>:<port_no.>;databaseName=sordb

For Example:

jdbc:sqlserver://localhost:1433;databaseName=sordb

5. When you have entered the Key Name, Key Value, and Display Name for each key, click SAVE at the bottom of the screen. Note that each key occupies one row in the Settings table.

Installing Oracle JDBC Driver for Parcel

To use an Oracle database as the IData/SOR for Parcel, you first need to install the Oracle JDBC Driver.

Caution: If you routinely ship a high volume of shipments and encounter timeouts with your Oracle ODBC connection, you need to increase the number of processes allowed by Oracle. **Notes:**

- The Parcel Java distribution includes the JDBC driver. For the version of Java that Parcel uses, the required driver is: ojdbc5.jar
- To check settings for steps 1-3, see the "Checking Settings" section in TM-Parcel – Upgrade Installation Guide

Installing Oracle JDBC Driver

To install the Oracle JDBC Driver, follow these steps:

Change the appropriate settings in the MySQL didb.settings table for the JavaVM and Database Server (DBS) Connection as follows:

- Add the path name to the ojdbc5.jar file for the key_value of the add_class_path entry. If there are any entries for this key_value already, separate the additional path name with a semicolon. **For Example:**

machine name	domain	sub_domain	key_name	key_value	display_name
ALL	core	javavm	javaJRE_folder	..\java\jre6_7_5_05	Java JRE root Folder
ALL	core	javavm	javaVM_folder	..\java	Java VM root Folder
ALL	core	javavm	add_class_path	..\java\lib\database\ojdbc5.jar	Additional Class Path information for JavaVM

- Change the settings for the SOR and/or the IData connection to the appropriate values for the JDBC connection. **For Example:**

machine name	domain	sub_domain	key_name	key_value	display_name
ORACLE	dba-connection	sor	dialect	Oracle	Hibernate SQL dialect used for connection
ORACLE	dba-connection	sor	driver	oracle.jdbc.OracleDriver	Database driver used to connect
ORACLE	dba-connection	sor	name	sor	Connection name used to connect to sor via Database S
ORACLE	dba-connection	sor	password	FS_DEV	Database Password
ORACLE	dba-connection	sor	type	JDBC	Connection type used to connect to sor via Database S
ORACLE	dba-connection	sor	url	jdbc:oracle:thin:@10.10.97.244:1521:occl	Connection URL used to connect to sor via Database S
ORACLE	dba-connection	sor	username	FS_DEV	Database User name

CAUTION

The value (in the key_value column) for key_name = "name" *must not be changed*.

- In order to access the SOR tables from the UI, you must set up an ODBC driver and modify the settings to use the DSN. **For Example:**

machine name	domain	sub_domain	key_name	key_value	display_name
ORACLE	core	sor	addparam		Additional ODBC Connection Parameters
ORACLE	core	sor	dbtype	oracle	The SOR database application MySQL, MSSQL, etc
ORACLE	core	sor	dsn	sor	SOR DSN Name
ORACLE	core	sor	enable_batch_log	n	Enable logging of batch events
ORACLE	core	sor	password	FS_DEV	SOR database password
ORACLE	core	sor	send_userpass_seperately	y	Send Username and Password seperately in ODBC Connect
ORACLE	core	sor	user id	FS_DEV	SOR database user name

Note: For additional information on SOR/IData Settings, refer to section *Updating DB Settings for SQL Server & Oracle SOR*

Customizing Installation batch file for SQL Server

To customize the Installation batch file for SQL Server, follow these steps:

- In the ..\DBUpdate\SOR\MSSQL\ folder, open the following file for editing by right-clicking on the filename, and then selecting Edit from the Pop-up menu: InstallDB_SOR.bat
- Find the following line: CALL Install_SOR_MSSQL DSN USER PASSWORD

- For the parameters DSN USER PASSWORD (meant to serve as an placeholders only) make the following substitutions:CALLInstall_SOR_MSSQL
<Actual_DNS_Name_of_ODBC_database>
<Actual_User_Name> <Actual_Password>

Note: For SQL Server, the parameters *DSN_Name*, *User_Name* and *Password* must be passed in exactly this sequence.

Customizing the Upgrade batch file for SQL Server

To customize the Upgrade batch file for SQL Server, follow these steps:

- In the MSSQL folder, open the UpdateDB_SOR.bat file for editing by rightclicking on the file, and then selecting Edit from the Pop-up menu.
- For the parameters FILENAME DSN USER PASSWORD (meant to serve as placeholders only) make the following substitutions:CALL
<Actual_Update_Batch_Filename>
<Actual_DNS_Name_of_ODBC_database><Actual_User_Name>
<Actual_Password>

Adding SOR Settings for SQL Server

To use a Microsoft SQL Server (SQL Server) database as the IData/SOR for Parcel, you first need to download and install the SQL Server JDBC Driver. **Notes:**

- The SQL Server JDBC driver is not included with Parcel. You need to download this driver separately. This driver is Open Source, and you do not need an account to download the required files. (See steps 1-2 of the following procedure.)
- To check settings for Step 3a and Step 3b, see the "Checking Settings" section in TM-Parcel - Upgrade Installation Guide.

Installing JDBC Drivers for SQL Server:

To install the JDBC Driver for SQL Server, follow these steps:

- Download the SQL Server JDBC Driver as follows: This driver is currently available from the following Sourceforge.net Web Page:
<https://docs.microsoft.com/en-us/sql/connect/jdbc/system-requirements-for-thejdbc-driver?view=sql-server-2019>
Note: For the version of Java that Parcel uses, the required driver is called jTDS - SQL Server and Sybase JDBC driver. The executable filename is: mssql-jdbc-7.4.1.jre8.jar
- Download the distribution zip file and unzip it to any folder. BluJay Solutions recommends the following path:...\Kewill\Flagship\java\lib\database
- Modify the appropriate settings in the MySQL didb.settings table for the JavaVM, Database Server (DBS) Connection, and class path as follows:

- Add the path name to the mssql-jdbc-7.4.1.jre8.jar file (see step 2) for the key_value of the add_class_path entry.

domain	sub_domain	key_name	key_value
--------	------------	----------	-----------

core	javavm	add_class_path	<Parcel Install Folder>\Flagship\java\lib\data base\mssqljdbc- 7.4.1.jre8.jar
------	--------	----------------	---

For Example:

The value for the machine column in the above example is ALL.

- b. Change the settings for the SOR and/or the IData connection to the appropriate values for the JDBC connection.

Note: In order to access the SOR tables from the UI, you must set up an ODBC driver and modify the settings to use the DSN. The following example displays all the settings in addition to the class path (see the example under step 3a. above) that need to be configured:

machine_name	domain	sub_domain	key_name	key_value	display_name
ALL	core	sor	dsn	sor-db-mssql	118 SOR DSN Name
ALL	core	sor	user id	sa_user	68 SOR database user name
ALL	core	sor	password	shipnowdb	98 SOR database password
ALL	core	sor	enable_batch_log	n	18 Enable logging of batch events
ALL	core	sor	addparam		08 Additional ODBC Connection Parameters
ALL	core	sor	send_username_password_separately	n	18 Send Username & Password separately in ODBC Connect
ALL	core	sor	dtype	mysql	98 The SOR database application MySQL / MSQ / etc
ALL	db	db	name	sordb	98 Connection name used to connect to sordb via Database Service
ALL	db	db	type	ODBC	48 Connection type used to connect to sordb via Database Service
ALL	db	db	url	jdbc:sqlserver://localhost:1433:databaseName=sordb	508 Connection URL used to connect to sordb via Database Service
ALL	db	db	username	sa_user	68 Database User name
ALL	db	db	password	shipnowdb	98 Database Password
ALL	db	db	driver	com.microsoft.sqlserver.jdbc.SQLServerDriver	48 Database driver used to connect
ALL	db	db	dialect	(NULL)	08 Hibernate SQL Dialect used for connection

Updating DB Settings for SQL Server & Oracle SOR

After completing your Parcel 24.1.0 installation, you need to update the didb.settings table if you are using one of the following database types for your SOR database:

- MS SQL Server
- Oracle

To update the Parcel database for a SQL Server SOR:

1. Stop the DIServer.
2. Edit the didb.settings table as follows: In the sor_subdomain, for the key_value of the dialect key_name, enter SQLServer, as shown in the following illustration:

machine_name	domain	sub_domain	key_name	key_value
ALL	db	sordb	dialect	SQLServer

To update the Parcel database for an Oracle SOR:

1. Stop the DIServer.
2. Edit the didb.settings table as follows: In the sor_subdomain, for the key_value of the dialect key_name, enter Oracle, as shown in the following illustration:

machine_name	domain	sub_domain	key_name	key_value
ALL	db	sordb	dialect	Oracle

After updating the Parcel database, to test your update:

1. Restart the DIServer.

2. Process a test shipment, and then Void the shipment.

Configuring LDAP User Authentication

Overview

Parcel supports user authentication using the Lightweight Directory Access Protocol (LDAP) and Windows Active Directory® as follows:

- LDAP - This software protocol enables users to locate organizations, individuals, and other resources such as files and devices in a network, including the Internet or a corporate intranet.
- Windows Active Directory - This directory service forms an integral part of the Windows 2000 architecture. Active Directory is a centralized and standardized system that automates network management of user data, security, and distributed resources, and enables interoperation with other directories. Active Directory is designed for distributed networking environments.

This section describes how to set up Parcel to use LDAP. **Requirements**

The following requirements must be met to use LDAP authentication with Parcel:

- An LDAP server must be installed and in operation.
- Parcel must be able to access the LDAP server.

Note: Parcel does not need to be in the same server with LDAP.

Configuring LDAP with Parcel

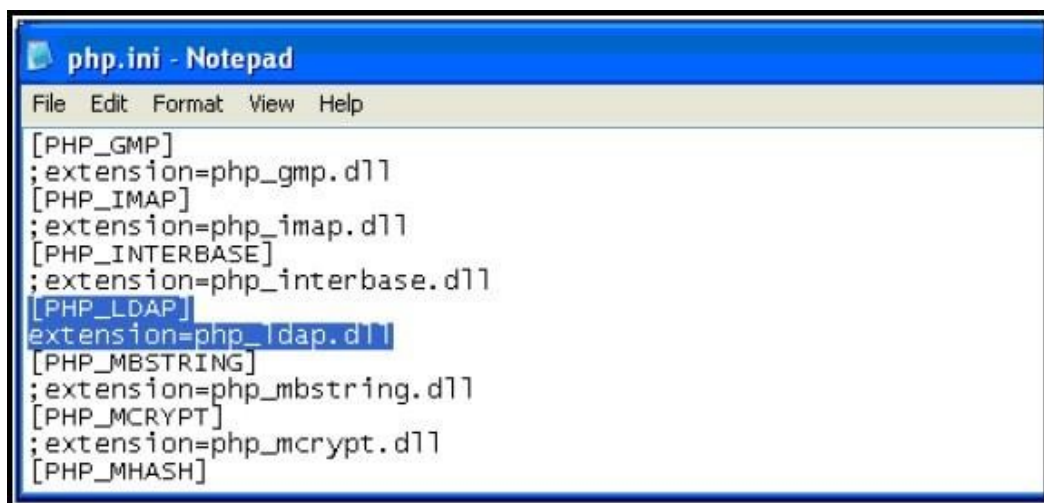
The following subsections describe how to configure LDAP with Parcel:

- Editing the php.ini file
- Configuring database settings
- Configuring the Parcel login

Editing the php.ini file

Check whether the php_ldap.dll extension is enabled in the php.ini file. If this extension is not currently enabled, you must edit the php.ini file to enable this extension. To check/edit the php.ini file:

1. Stop the Apache Web server.
2. In Windows Explorer, open the Windows folder and locate the php.ini file. Typically, this folder is located in the path:<Parcel Install Folder>\Flagship\php (or) <Parcel Install Folder>\Flagship\phpnts
3. Open the php.ini file in a text editor such as Notepad or WordPad, and then locate the line with the statement for the php_ldap.dll extension, as show in the following illustration:



4. If the line `extension=php_ldap.dll` is "commented out", that is, preceded by a semicolon at the start of the line, delete the semicolon. (The above illustration shows this line with the semicolon removed.)
5. Save and close the `php.ini` file.
6. Restart the Apache server.

Configuring Database Settings

You need to configure the Settings table in the Parcel `didb` database (`didb.settings`) for the LDAP server and other authorization settings. **To configure the settings table:**

1. Open Parcel and log in with Administrator privileges.
2. From the System menu, select Settings > Locations > Global Settings > Settings to display the `didb.settings` table.
3. Edit the settings for key names and values according to the following table:

machine_name	domain	sub_domain	key_name	key_value	Description
ALL	ui-auth	auth	authtype	ldap	Valid values for authentication type: <ul style="list-style-type: none"> LDAP server - ldap SSO - sso database - database

machine_name	domain	sub_domain	key_name	key_value	Description
--------------	--------	------------	----------	-----------	-------------

ALL	ui-auth	ldap	Role_default	usr	Parcel roles: <ul style="list-style-type: none"> usr-application user ead-Application Administrator eed-Enterprise Administrator toh-Default Ship to Hold user
ALL	ui-auth	ldap	basedn	<variable>	The Base DN as listed in the ldap_location table. (See the following example.)
ALL	ui-auth	ldap	port	389	The default port for the LDAP server is 389.
ALL	ui-auth	ldap	domain_controller	<variable>	The machine name or IP address of the LDAP server in the ldap_location table. (See the following example.)
machine_name	domain	sub_domain	key_name	key_value	Description

ALL	ui-auth	ldap	account_suffix	<variable >	The domain name of the LDAP server as listed in the ldap_location table. (See the following example.)
ALL	ui-auth	database	dsn	didb	The name of the Parcel database.
ALL	ui-auth	database	username	sn_usr	The script for this function requires this user name.
ALL		database	password	shipnow db	The script for this function requires this password.

didb.ldap_location Table Example

The following example of an ldap_location table in the Parcel didb database shows examples of values for the domain_controller, account_suffix, and basedn fields listed in the previous table:

domain_controller	user_friendly_name	portno	account_suffix	basedn
10.10.10.10	Satisfied Customer	389	saticus.local	satis
domcmrll.corpco.net	Corporate LDAP	389	corpco.net	corpco
*		389	(NULL)	(NULL)

Notes:

- The Parcel DI Server must be on the same network or have a VPN connection to the domain controller.
- You can use SQLyog or another database management tool to edit the Parcel didb database.

Configuring the Parcel Login

To configure the Parcel login to work with LDAP user authentication:

1. In the Windows Active Directory, create a user name and password for each LDAP domain controller that you specified in the ldap_location table. (See Windows documentation for this procedure.)

2. Open the Parcel application, so that the login screen for the Web GUI is displayed. Note that the login screen now includes a field called "Domain Controller" with a drop-down list containing all the configured LDAP servers listed in the didb.idap_location table (by user_friendly_name value), as in the previous example:

3. From the Domain Controller drop-down list, select the Domain Controller you want to use for this login, enter the **User Name** and **Password** that you set up in step 1 for this **Domain Controller**, and then click LOG IN to open the Welcome screen (Home page) of the Parcel Web GUI.
If the login is successful (everything has been configured correctly, Parcel carries out the following steps:
 - a. Authenticates the User Name and Password with the LDAP server.
 - b. If authentication is successful, checks that the User Name exists in the Parcel didb.login table.
 - c. If the User Name exists, Parcel opens the Welcome screen (Home page).
 - d. If the User Name does not exist Parcel adds a record for that User Name in the didb.login table, and then adds records for that user in the didb.user_shippers table for each location configured within Parcel. (This means that, by default, this user has access to ship from every location.)

Notes:

- Parcel determines a user's role by the group value returned as part of the LDAP response. This means that you need to assign LDAP users to groups within Parcel. (For information on how to do this, see the Parcel Help.)
- In addition, after a successful initial login, you need to set a default location for the LDAP user that you logged in as. (For information on how to do this, see the Parcel Help.)

Purge Utility

Since Parcel uses MySQL databases for internal configurations, carrier configurations, and shipping transactional history; maintenance needs to be performed on these databases to maintain data integrity.

Parcel is delivered with a utility named the Purge Utility. This utility is configured to purge data from specified schemas based on certain conditions. In addition, the Purge Utility can clean up files, database and both as part of the purging process.

The Purge Utility then performs extended create, repair and optimization on tables where data is purged. The data is placed into backup CSV files and can be used to restore data if necessary.

This Purge Utility can be run manually from the Flagship bin folder or it can be scheduled as a task to be run from the Windows Task Scheduler.

Note: It is recommended that the Purge Utility be run during non or low-impact business hours.

The Purge Utility uses several tables in MySQL for internal configuration and to determine what schemas need to be purged and under what conditions. For internal configuration, the Purge Utility uses the DADB.SETTINGS table. The records associated with the Purge Utility in this table are:

machine_name	domain	subdomain	key_name	key_value
ALL	Purging	database	backup_dir	<Parcel Install Folder>\Flagship\Purge_backup
ALL	Purging	database	repair	E
ALL	Purging	database	optimize	Y
ALL	Purging	database	create_backup_files	Y

The key_name = backup_dir specifies the location where the purged data will be placed. The key_name = repair specifies that extended repair will be done on the tables. Options are:

- N = perform no operations
- Y = perform standard repair
- E = perform extended repair (recommended)

The key_name = optimize specifies that the tables are optimized after a purge. Options are:

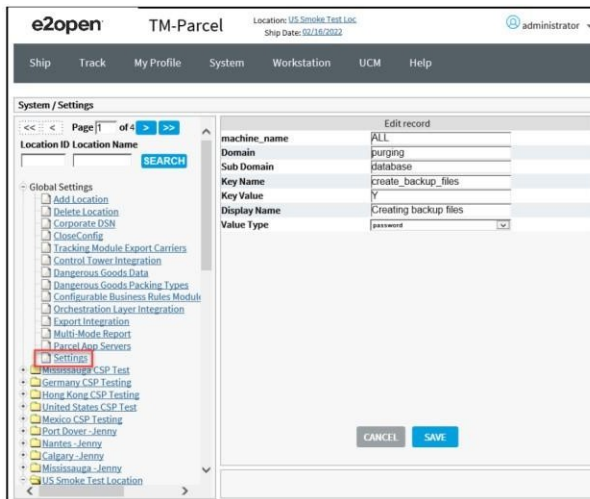
- N = perform no optimization
- Y = perform optimization (recommended)

The key_name = create_backup_files specifies the creation of backup files. Options are:

- Y = perform creation of backup files
- N = perform no creation of backup files

Note: You can also set the purge settings in Application under, Global Settings > Settings > search for Key Name: create_backup_files.

The purge settings displays, as shown in the following screen.



For database schema definition, the Purge Utility uses the following DIDB.DB_PURGE_SCHEMA table.

Samplings of the records in this table are:

Schema_id	Db_name	Table_name	dateformat	create_file	is_custom
10	didb	intl_detail	yyyymmdd	y	Y
11	didb	intl_master	yyyymmdd	y	Y
12	didb	preship_shipments	yyyymmdd	y	Y
13	didb	preship_packages	yyyymmdd	y	Y
14	didb	error_log	yyyymmdd	y	Y

The Schema_id is related to the Schema_id defined in the DIDB.DB_PURGE_CONDITIONS table.

The Db_name defines the schema that the table to be purged is found in.

The Table_name defines the table to be purged in the previously defined schema.

The dateformat defines the data format specified in the previous defined table name.

Please note that purging conditions are based on age of the records and specifically use dates based on the condition to purge.

The create_file flag specifies whether a backup file is created for a table that is purged.

Tables will always be purged, saving the data is optional.

The is_custom flag is used to prevent newer builds from overwriting these tables when upgrading to a newer version of Parcel.

For database purging conditions, the Purge Utility uses the DIDB.DB_PURGE_CONDITIONS table. Samplings of the records in this table are:

Condition_id	Schema_id	Column_type	Column_name	Condition	Value	is_custom
2000	10	DATE	pickupdate	<=	@31	y
2001	11	DATE	Pickupdate	<=	@31	y
2002	12	DATE	ship_date	<=	@31	y
2003	13	DATE	ship_date	<=	@31	y
2004	14	DATE	Date_format(log_time, %Y%m\$d')	<=	@31	y

The Condition_id is an auto incremental value for the records created in this table. It is not used with the Purge Utility.

The Schema_id is related to the Schema_id specified in the DIDB.DB_PURGE_SCHEMA table.

The Column_type denotes that the type of value contained in the defined column is a type of DATE.

The Column_name defines the name of the column found in the table specified in the DIDB.DB_PURGE_SCHEMA table.

The Condition is used to define the condition of the purge query.

The value specifies the number of days to be used for the purge query condition. The value can be 1 to n , where n is any value within reason. This value signifies days and must be specified with the '@' sign.

The is_custom flag is used to prevent newer builds from overwriting these tables when upgrading to a newer version of Parcel.

For file purging conditions, the Purge Utility uses the DIDB.FILE_PURGE_CONFIG table. Samplings of the records in this table are:

File_purge_id	Folder	File_mask	No_of_days	is_custom
2000	<Parcel Artifact Folder>\Flagship\bin	di_debug.log*	30	y
2001	<Parcel Artifact Folder>\Flagship\bin\di_logs\backup	di_debug.log*	30	y
2002	<Parcel Artifact Folder>\Flagship\bin\di_logs\backup	di_event.log*	30	y
2003	<Parcel Artifact Folder>\Flagship\bin\di_logs\backup	ns_debug.log*	30	y

The File_purge_id is an auto incremental value for the records created in this table. It is not used with the Purge Utility.

The Folder specifies where the purge utility is required to look for files to purge based on the File_mask and No_of_days specified.

The File_mask specifies the file(s) to be defined using wildcards so the purge utility can purge or delete these files. Backups are not created. If backups are needed, simply don't specify the file for purging.

The No_of_days specifies the age of the file to purged. This value is not unlike the value used in the conditions table. The value can be 1 to n , where n is any value within reason.

The is_custom flag is used to prevent newer builds from overwriting these tables when upgrading to a newer version of Parcel.

Updating the purge.ini file:

1. Navigate to the following location and open the purge.ini file in a text editor:
<Parcel Install Folder>\Flagship\bin\purge.ini

- In the purge.ini file, add a new setting for CONNECTSTRING under the DATABASE section. Note that this should have connection information to the MySQL database.

```
[DATABASE]
CONNECTSTRING
="DB_HOST=localhost;DB_USER=sn_usr;DB_PASSWORD=shipnowdb;DB_DATABASE=didb";
PURGE_FLAG value should be d/f/b or D/F/B (D/d ->database, f/F ->File, b/B ->Both);
if PURGE_FLAG value is d/D it will only do database purge; if
PURGE_FLAG value is f/F it will only do File purge;
if PURGE_FLAG value is b/B it will only do both (database and File) purge;
PURGE_FLAG=b
```

Supporting UCM Integration on HTTPS

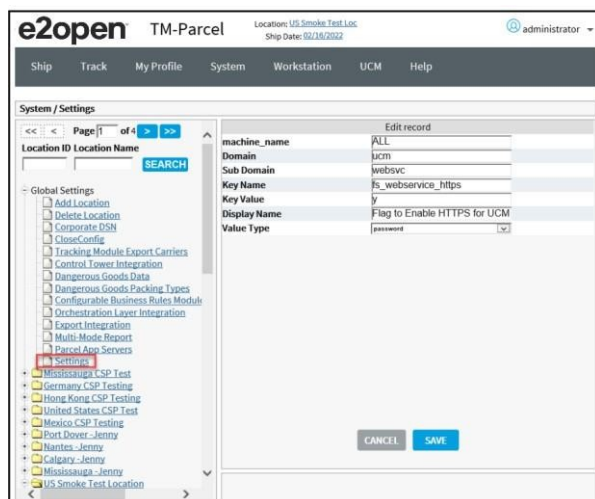
To support UCM Integration on HTTPS, update 'fs_webservice_https' under Global Settings > Settings

- Y = support UCM Integration on HTTPS

The record associated to support UCM Integration on HTTPS is in the following table:

machine_name	domain	sub-domain	key_name	key_value
ALL	ucm	websvc	fs_webservice_https	Y

The ucm integration layer settings displays, as shown in the following screen.



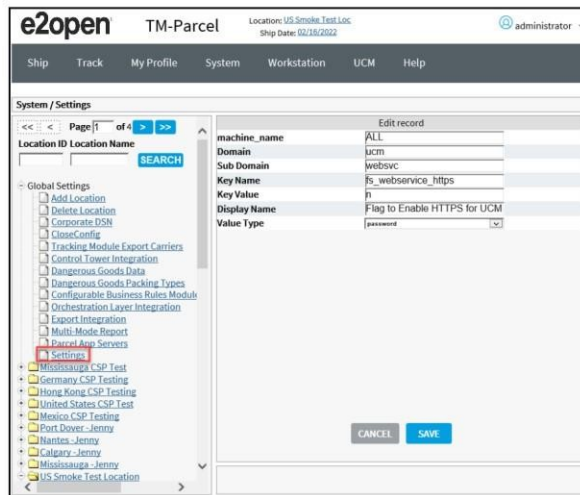
Converting UCM from HTTPS to HTTP

Note: Make sure Parcel is in http.

- Edit the setting for key_name and value according to the following table:

machine_name	domain	sub-domain	key_name	key_value
ALL	ucm	websvc	fs_webservice_https	N

The settings of **fs_webservice_https** key_name for **ucm** Domain in Parcel Application is shown in the following screen.



- Restart Kewill DiServer Service and Refresh the Application.
- Navigate to <Parcel Artifact Folder>\Flagship\ucm\java\META-INF\config.xml file and update "Enabled" tag to "N".

```
<https>
  <Enabled>N</Enabled>
  <CertificateFilePath>./META-INF/ucm.p12</CertificateFilePath>
  <CertificatePassword>blujayucm</CertificatePassword>
</https>
```

- Restart BluJayUCMServer Service.

Parcel Data Upload

Note: If you want to connect to Remote DB from Parcel Data Upload you have to update DB configuration in the following file:

<Parcel Artifact Folder>\Flagship\java\conf\parcel_data_upload\parcel-data-uploadconfig.properties

Modifying parcel-data-upload-config.properties file

- spring.datasource.url=jdbc:mysql:<change the localhost with respect to your DB IP:Port>/didb?characterEncoding=UTF-8
- spring.datasource.username=<change the username with respect to your DB>
- spring.datasource.password=<change the password with respect to your DB>

After updating the above property file, you need to restart the BluJayParcelDataUploadTool service.

Installing and Starting the SOR Updater Windows Service

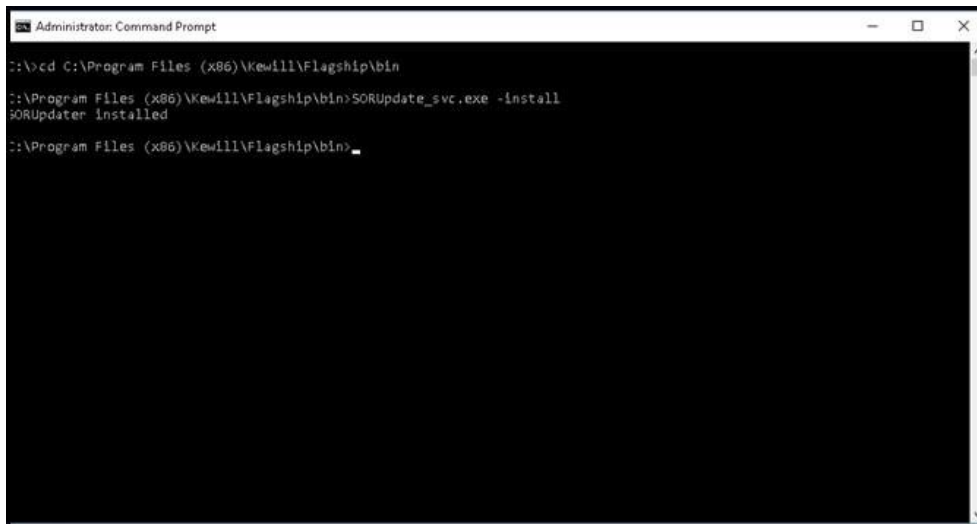
If you are using End of Day (EOD) Consolidation with carriers that support this option

(for example FedEx, UPS, etc.), you need to install and start the BluJay Solutions SOR Updater Windows service. This Windows service automatically updates consolidation rates in the Parcel SOR database.

To install and start the SOR Updater Windows Service:

1. On the computer running the Parcel DI Server, open the Windows Administrator Command Prompt window, and then navigate to the `..\Kewill\Flagship\bin` directory.
2. Select the `SORUpdate_svc.exe` file, and then type a space and the `-install` command as shown in the following example:<Parcel Install Folder>\Flagship\bin>`SORUpdate_svc.exe -install`

The following illustration shows the result of executing this command:



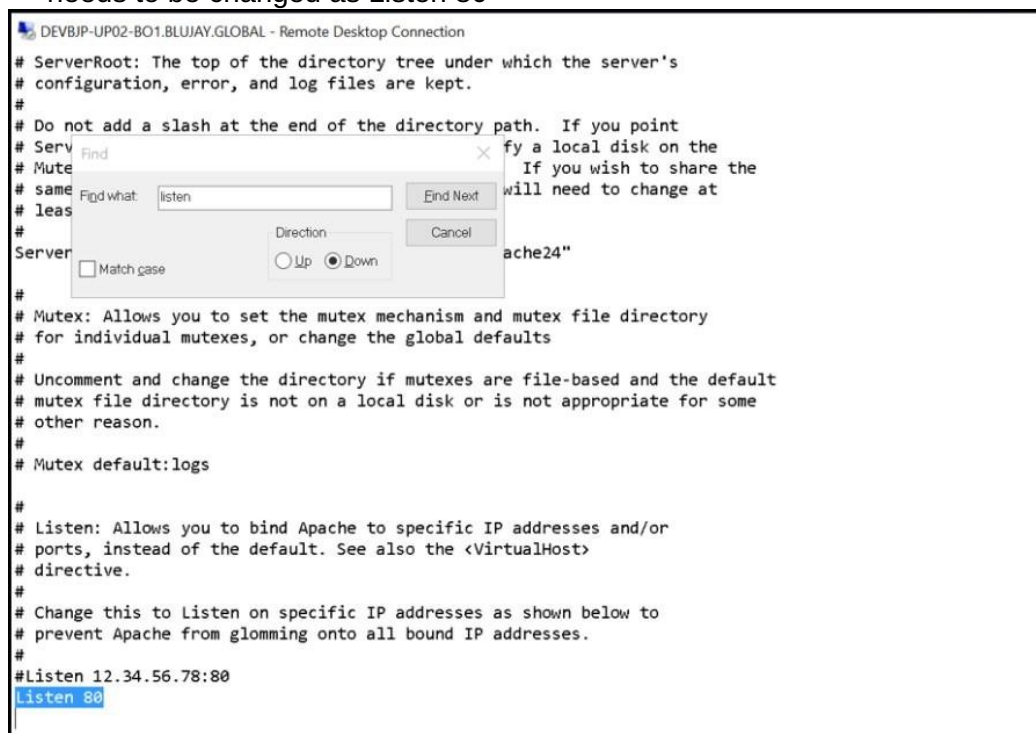
```
Administrator: Command Prompt
C:\>cd C:\Program Files (x86)\Kewill\Flagship\bin
C:\Program Files (x86)\Kewill\Flagship\bin>SORUpdate_svc.exe -install
SORUpdater installed
C:\Program Files (x86)\Kewill\Flagship\bin>
```

3. Open the Component Services window (Start > Control Panel > Administrative Tools > Component Services), and then select Service (Local) to display the list of Windows services.
4. Select the BluJay Solutions SOR Updater service, right click on this service, and then select **Start** from the Pop-up menu. **Note:** On subsequent restarts of the Parcel DI Server, this service starts automatically along with the other Kewill services, as shown in the following illustration:

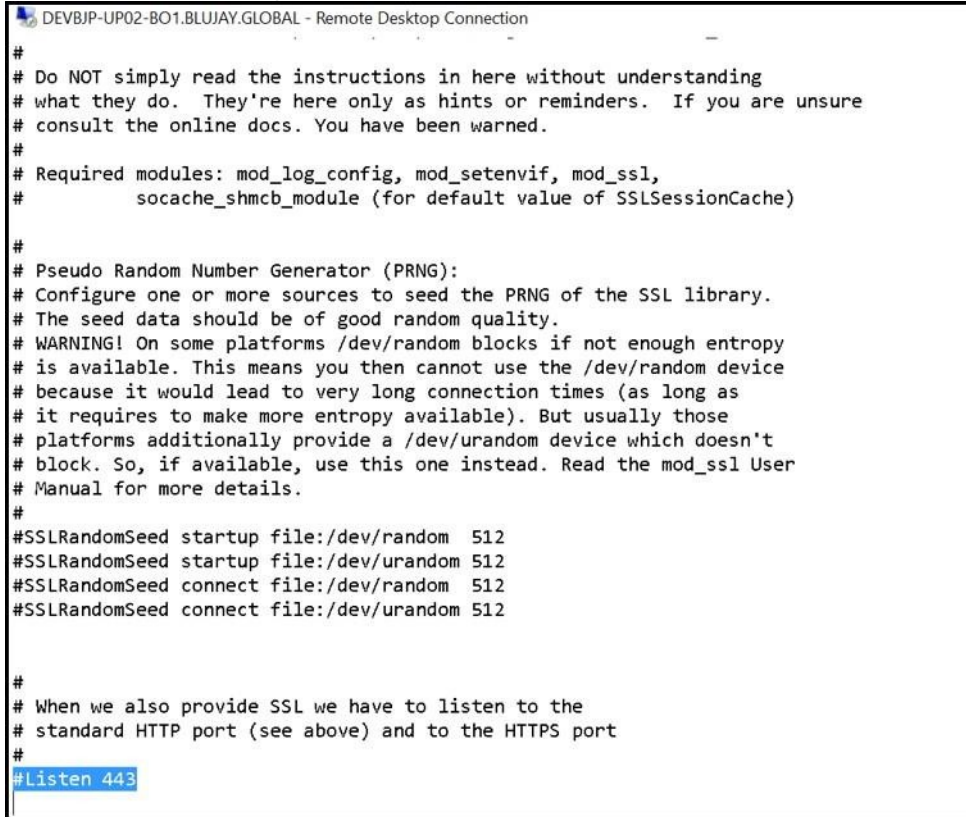
Name	Description	Status	Startup Type	Log On As
Hyper-V Volume Shadow C...	Coordinates...		Manual (Trig...	Local Syste...
IKE and AuthIP IPsec Keying...	The IKEEXT ...	Running	Automatic (T...	Local Syste...
Interactive Services Detection	Enables use...		Manual	Local Syste...
Internet Connection Sharin...	Provides ne...		Manual (Trig...	Local Syste...
IP Helper	Provides tu...	Running	Automatic	Local Syste...
IPsec Policy Agent	Internet Pro...	Running	Manual (Trig...	Network S...
KDC Proxy Server service (K...	KDC Proxy S...		Manual	Network S...
Kewill DiServer Service	Flagship Ser...	Running	Automatic	Local Syste...
Kewill Notification Service	Automatic ...	Running	Automatic	Local Syste...
Kewill Scheduler Service	Enables the ...	Running	Automatic	Local Syste...
Kewill SOR Updater	Kewill's con...		Automatic	Local Syste...
Kewill Tracking Service	Automatic ...	Running	Automatic	Local Syste...
KewillFlagshipConnectorFil...	Kewill Servi...	Running	Automatic	Local Syste...
KewillFlagshipDatabaseFileS...	Kewill Servi...	Running	Automatic	Local Syste...
KewillFlagshipServerBridgeS...	Kewill Servi...	Running	Automatic	Local Syste...
KewillReportingService	Kewill Servi...	Running	Automatic	Local Syste...

Converting Parcel from HTTPS to HTTP on Apache Server

1. Navigate to the following location and open the httpd.conf file in a text editor: C:\Program Files (x86)\Apache-httpd\Apache24\conf
2. Search for the word 'Listen' and update the comment, as shown below: #Listen 80 needs to be changed as Listen 80



3. Navigate to the following location and open the httpd-ssl.conf file in a text editor: C:\Program Files (x86)\Apache-httpd\Apache24\conf\extra
4. Search for the word 'Listen' and update the comment, as shown below: Listen 443 needs to be changed as #Listen 443



```
#
# Do NOT simply read the instructions in here without understanding
# what they do. They're here only as hints or reminders. If you are unsure
# consult the online docs. You have been warned.
#
# Required modules: mod_log_config, mod_setenvif, mod_ssl,
#                   socache_shmcb_module (for default value of SSLSessionCache)
#
# Pseudo Random Number Generator (PRNG):
# Configure one or more sources to seed the PRNG of the SSL library.
# The seed data should be of good random quality.
# WARNING! On some platforms /dev/random blocks if not enough entropy
# is available. This means you then cannot use the /dev/random device
# because it would lead to very long connection times (as long as
# it requires to make more entropy available). But usually those
# platforms additionally provide a /dev/urandom device which doesn't
# block. So, if available, use this one instead. Read the mod_ssl User
# Manual for more details.
#
#SSLRandomSeed startup file:/dev/random 512
#SSLRandomSeed startup file:/dev/urandom 512
#SSLRandomSeed connect file:/dev/random 512
#SSLRandomSeed connect file:/dev/urandom 512
#
# When we also provide SSL we have to listen to the
# standard HTTP port (see above) and to the HTTPS port
#
#Listen 443
```

5. Restart Apache2.4 Service.

Configuring Stunnel Settings for Encryption of Data in Motion

Parcel supports Encryption of Data in Motion between client and server for data security and protection as follows:

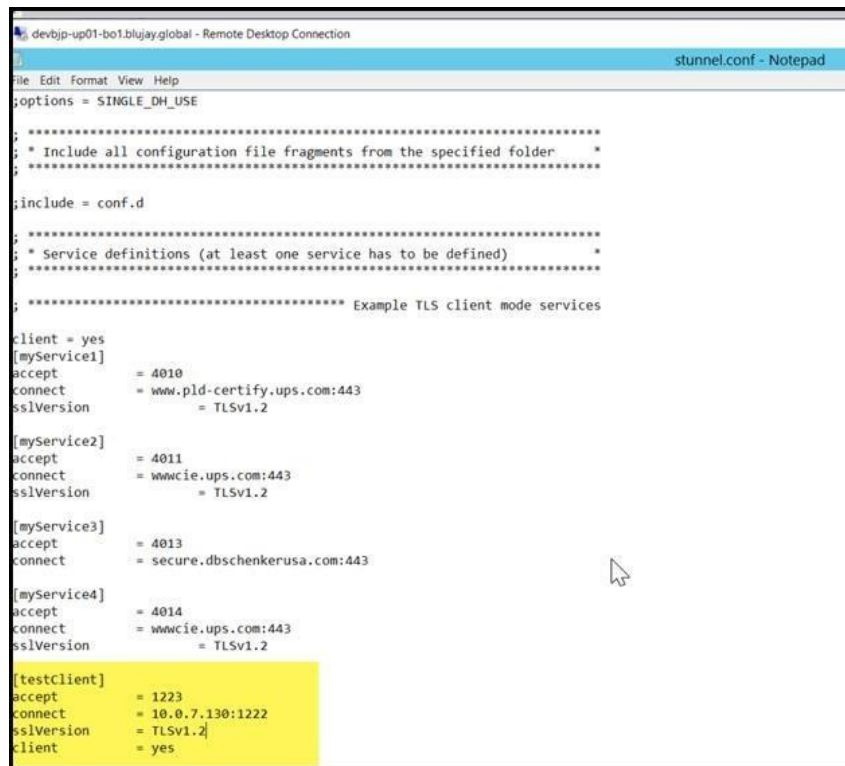
- Configuring the Stunnel Settings in Client Machine
- Configuring the Stunnel Settings in Server Machine

Configuring the Stunnel Settings in Client Machine

Note: Make sure to install Stunnel with openssl in client machine which has Parcel Web Admin Tool (Javalin Tool).

To configure the Stunnel settings in Client Machine:

1. Navigate to the following location and open stunnel.conf file in a text editor:<Drive>:<Parcel Install Folder>\Flagship\STunnelService\config For Example:
<Parcel Install Folder>\Flagship\STunnelService\config
2. In the stunnel.conf file, add below service, as shown in following screen.
testClient accept = 1223 connect = Server IP Address:1222
sslVersion = TLSv1.2 client
= yes



```

devbjp-up01-bo1.blujayglobal - Remote Desktop Connection
stunnel.conf - Notepad
File Edit Format View Help
;options = SINGLE_DH_USE
;
; *****
; * Include all configuration file fragments from the specified folder *
; *****
;include = conf.d
;
; *****
; * Service definitions (at least one service has to be defined) *
; *****
; ***** Example TLS client mode services *****
client = yes
[myService1]
accept      = 4010
connect     = www.pld-certify.ups.com:443
sslVersion  = TLSv1.2

[myService2]
accept      = 4011
connect     = www.ups.com:443
sslVersion  = TLSv1.2

[myService3]
accept      = 4013
connect     = secure.dbschenkerusa.com:443

[myService4]
accept      = 4014
connect     = www.ups.com:443
sslVersion  = TLSv1.2

[testClient]
accept      = 1223
connect     = 10.0.7.130:1222
sslVersion  = TLSv1.2
client      = yes

```

3. Save stunnel.conf file.
4. Restart stunnel service.
5. Set **Host** as Client Hostname/IP Address/localhost and **Port** as 1223 in Javalin tool on the Client Machine.
6. Run any API Request on the Client Machine.

Configuring the Stunnel Settings in Server Machine

Note: Make sure to install Stunnel with openssl in Parcel server machine. To configure the Stunnel settings in Parcel Server Machine:

1. Navigate to the following location and open stunnel.conf file in a text editor:<Drive>:<Parcel Install Folder>\Flagship\STunnelService\config For Example:<Parcel Install Folder>\Flagship\STunnelService\config
2. In the stunnel.conf file, add below service, as shown in following screen.

```
testServerclient = no
accept = 1222
connect = 1200 cert
= stunnel.pem
```

```
;options = SINGLE_ECDH_USE
;options = SINGLE_DH_USE

; *****
; * Include all configuration file fragments from the specified folder *
; *****

;include = conf.d

; *****
; * Service definitions (at least one service has to be defined) *
; *****

; ***** Example TLS client mode services *****

client = yes
[myService1]
accept      = 4010
connect     = www.pld-certify.ups.com:443
sslVersion  = TLSv1.2

[myService2]
accept      = 4011
connect     = wwwcie.ups.com:443
sslVersion  = TLSv1.2

[myService3]
accept      = 4013
connect     = secure.dbschenkerusa.com:443

[myService4]
accept      = 4014
connect     = wwwcie.ups.com:443
sslVersion  = TLSv1.2

; ***** Example TLS server mode services *****

[testServer]
client      = no
accept      = 1222
connect     = 1200
cert        = stunnel.pem
```

3. Save stunnel.conf file.
4. Restart stunnel service.

Encryption of Stored Data

Transparent Data Encryption (TDE) is employed to encrypt data at rest. This enables you to encrypt sensitive data stored in tables and table spaces.

After the data is encrypted, this data is transparently decrypted for authorized users or applications when they access this data.

Parcel supports TDE to encrypt data stored in MySQL Server. If you wish to enable encryption of data stored in the databases, please refer to the following sections to configure the servers to use TDE.

Configuring Transparent Data Encryption in MySQL Server

This section describes how to configure Transparent Data Encryption (TDE) in MySQL Server.

Prerequisite:

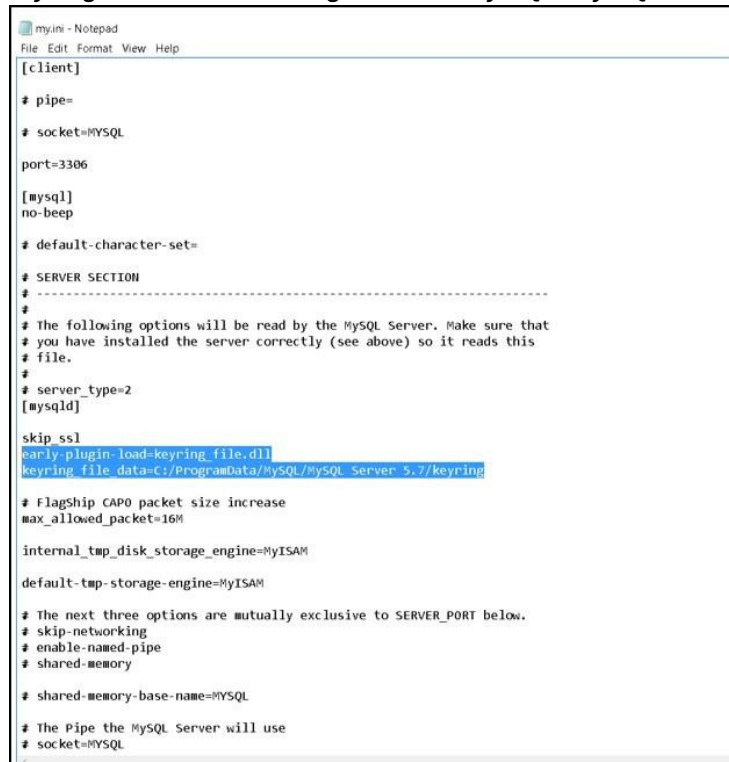
- TDE for MySQL is only supported with InnoDB engine. Please refer to "Parcel – Instructions Document – Converting MyISAM to InnoDB to change the engine type."

To configure Transparent Data Encryption in MySQL Server, follow these steps:

1. Navigate to the MySQL Configuration file (my.ini) location and open the my.ini in a text editor.**For Example:** C:\ProgramData\MySQL\MySQL Server 8.0\my.ini
2. Modify the my.ini file, as shown in the following figures.

Add the below lines under `mysqld` section.*early-plugin-load=keyring_file.dll***Note:** Keyring file can be placed in any location. However, please ensure the MySQL application (mysqld.exe) has access to this file in the location it is placed. New keyring flat file will be created in the below mentioned path:

keyring_file_data=C:/ProgramData/MySQL/MySQL Server 8.0/keyring



```

my.ini - Notepad
File Edit Format View Help

[client]

# pipe=
# socket=MySQL

port=3306

[mysql]
no-beep

# default-character-set=

# SERVER SECTION
# -----
#
# The following options will be read by the MySQL Server. Make sure that
# you have installed the server correctly (see above) so it reads this
# file.
#
# server_type=2
[mysqld]

skip_ssl
early-plugin-load=keyring_file.dll
keyring_file_data=C:/ProgramData/MySQL/MySQL Server 8.0/keyring

# FlagShip CAP0 packet size increase
max_allowed_packet=16M

internal_tmp_disk_storage_engine=MyISAM
default_tmp_storage_engine=MyISAM

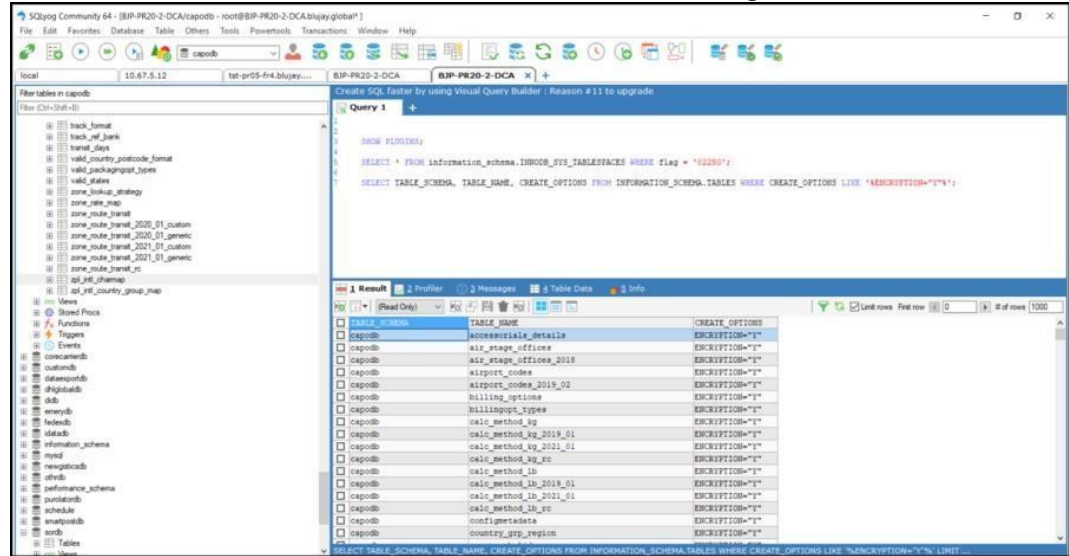
# The next three options are mutually exclusive to SERVER_PORT below.
# skip-networking
# enable-named-pipe
# shared-memory

# shared-memory-base-name=MYSQL

# The Pipe the MySQL Server will use
# socket=MySQL
  
```

3. Restart the MySQL Service.**Note:** For 'EncryptDBatRest.php' file, please contact BluJay Solutions Technical Support Team.
4. Place 'EncryptDBatRest.php' file in ...\\Kewill\\Flagship\\WebGUI path.
5. Open a command prompt using Administrative privileges and then navigate to ..\\Kewill\\Flagship\\WebGUI directory. Execute the below command: php EncryptDBatRest.php Now, the data in .ibd files gets encrypted.**Note:** To ensure the data are encrypted in tables, run the following query: SELECT TABLE_SCHEMA, TABLE_NAME, CREATE_OPTIONS FROM INFORMATION_SCHEMA.TABLES WHERE CREATE_OPTIONS LIKE

'%ENCRYPTION="Y"%'; The results are shown in following screen.



Configuring Transparent Data Encryption in MSSQL Server

This section describes how to configure Transparent Data Encryption (TDE) in MSSQL Server.

Prerequisite:

- Create a new folder <BackupPath> in MSSQL Server for backup. **For Example:** C:\TDE

Note: The TDE configuration in MSSQL Server is needed only if MSSQL SOR is used. To configure Transparent Data Encryption in MSSQL Server, you need to execute the below command in MSSQL Server, as shown in the following steps:

1. Create a Master Key

The master key is a symmetric key used to protect the private keys of certificates and asymmetric keys.

You must create the Master Key. It must be created within the master database with the USE MASTER command.

USE Master;

CREATE MASTER KEY ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>'; **For**

Example:

USE Master;

CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'Ace3289\$@12';

2. Create or Obtain a Certificate Protected by the Master Key. Once the master key is created along with the strong password (that you should remember or save in a secure location), now create the actual certificate and name it.

Execute the below command:

USE Master; CREATE CERTIFICATE '<CertificateNameHere>' WITH SUBJECT = '<GenericSubject>'; **For Example:**

```
USE Master;CREATE CERTIFICATE '<TDECert>'
WITH SUBJECT = '<TDE Certificate>';
```

3. Create a Database Encryption Key. Now, utilize the USE command to switch to the database that you wish to encrypt. Then create a connection between the certificate that you just created and the actual database. Then indicate the type of encryption algorithm.

Execute the below command:

```
USE '<DB Name>';
CREATE DATABASE ENCRYPTION KEY WITH
ALGORITHM = '<Encryption Algorithm>'
ENCRYPTION BY SERVER CERTIFICATE '<CertificateNameHere>'; For
```

sordb:

```
USE sordb;
CREATE DATABASE ENCRYPTION KEY WITH
ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE TDECert; For
```

idatadb:

```
USE idatadb;
CREATE DATABASE ENCRYPTION KEY WITH
ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE TDECert;
```

4. Backup the Private Encryption Key and Certificate Now, backup the private encryption key and certificate you created and store it in a secure location.

Execute the below command:

```
BACKUP CERTIFICATE '<CertificateNameHere>'
TO FILE ='<BackupPath>'
WITH PRIVATE KEY ( FILE = '<BackupPath>\<PrivateKey>',
ENCRYPTION BY PASSWORD = '<UseStrongPasswordHere>'); For
```

Example:

```
BACKUP CERTIFICATE TDECert
TO FILE ='C:\TDE\TDE_Cert'
WITH PRIVATE KEY (FILE ='C:\TDE\TDE_CertKey.pvk',
ENCRYPTION BY PASSWORD = 'Ace3289$@12');
```

5. Turn TDE On

Finally, you need to enable encryption on the database.

Execute the below command: USE

```
'<DB Name>';
ALTER DATABASE '<DB Name>'
SET ENCRYPTION ON; For
```

sordb:

```
USE sordb;
ALTER DATABASE sordb
SET ENCRYPTION ON;
```

For idatadb:

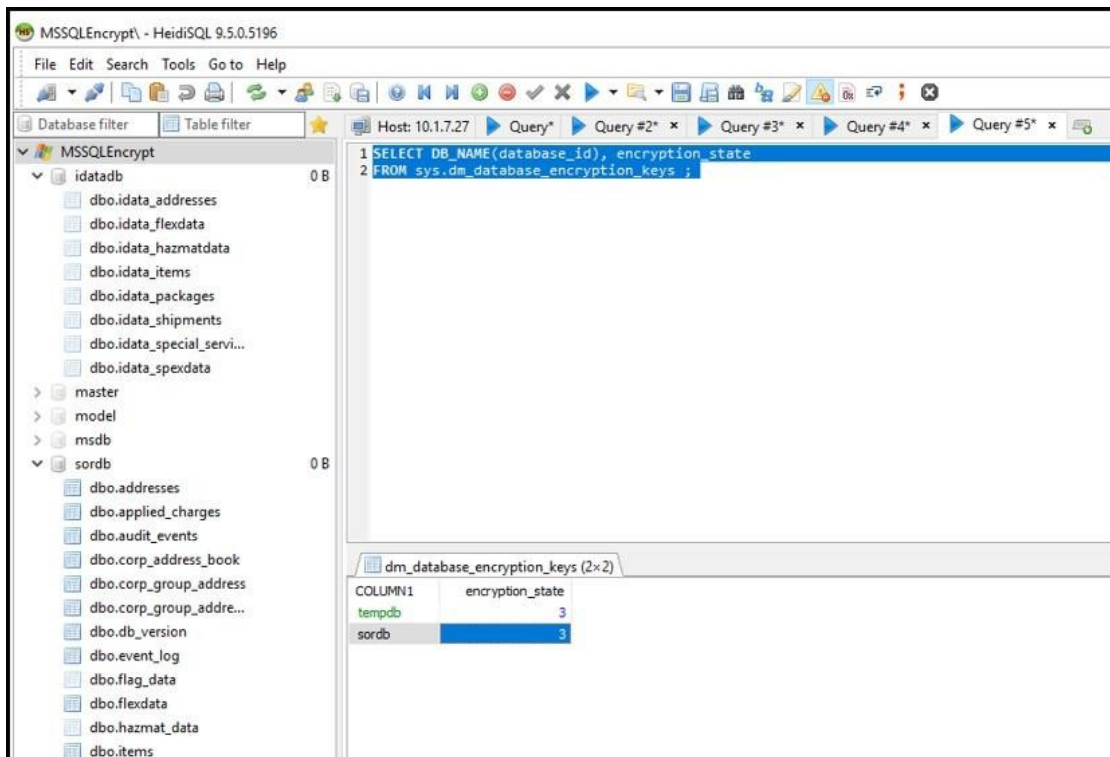
```
USE idatadb;
ALTER DATABASE idatadb
SET ENCRYPTION ON;
```

Now, if you want to check the progress of the database encryption on the MSSQL Server, execute the below command.

```
SELECT DB_NAME(database_id) AS '<DB Name>', encryption_state FROM
sys.dm_database_encryption_keys;
```

For sordb:

```
SELECT DB_NAME(database_id) AS sordb, encryption_state FROM
sys.dm_database_encryption_keys;
```



For idatadb:

```
SELECT DB_NAME(database_id) AS idatadb, encryption_state FROM
sys.dm_database_encryption_keys;
```

Database Encryption Status Details

The following table shows the encryption status details of the database displayed in Results grid.

Database Encryption Status	Description
0	No database encryption key present, no encryption
1	Unencrypted
2	Encryption in progress
3	Encrypted
4	Key change in progress
5	Decryption in progress

6	Protection change in progress (The certificate or asymmetric key that is encrypting the database encryption key is being changed.)
---	--

Configure Encrypted Connections to Database

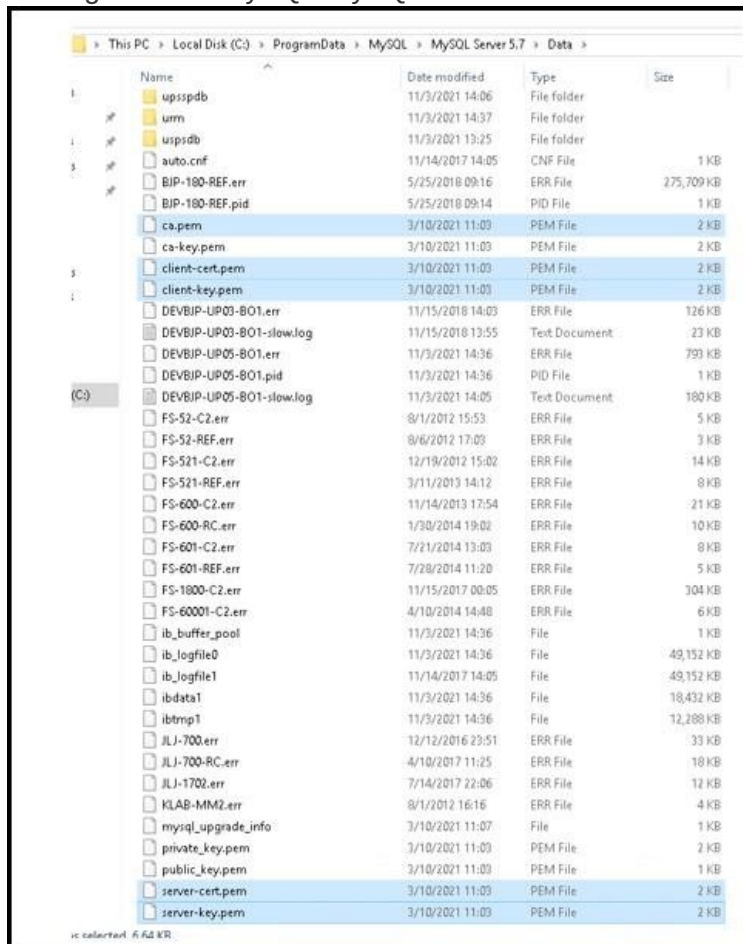
Parcel supports encrypted connections to the database. This is available for connections to MySQL, MSSQL and Oracle in this release.

In-order to set up encrypted connections, configuration changes are required to both the database server and, in the Application (Modules).

Configuring MySQL to Use Encrypted Connection

To configure the MySQL to use encrypted connections, follow these steps:

1. For encrypted connection SSL Certificates are required. These can be generated in any of the following methods: Get SSL Certificates from Certificate Authority (CA). These certificates should be in PEM format. Use default MySQL SSL Certificates which can be found in MySQL Installation path. **For Example:** C:\ProgramData\MySQL\MySQL Server 8.0\Data



2. Navigate to the MySQL Configuration file (my.ini) location and open the my.ini in a text editor. **For Example:** C:\ProgramData\MySQL\MySQL Server 8.0\my.ini
3. Search for the property 'skip_ssl' if it is available, and comment the line, as shown below: skip_ssl needs to be changed as #skip_ssl

4. Add the below keys in the my.ini file, as shown in following table.

Keys	Description
ssl_ca	Provide the path of the server Certificate Authority (CA) certificate file in PEM format.
ssl_cert	Provide the path of the server public key certificate file in PEM format.
ssl_key	Provide path of the server private key file in PEM format.
ssl_cipher	Provide the cipher algorithm supported by MySQL. Note: Use Cipher "DHE-RSA-AES128-GCM-SHA256:AES128-SHA". This should be also used in Application (Modules).
Keys	Description
require_secure_trasnport	Set this key to allow SSL connection only. Valid values are: <ul style="list-style-type: none"> • ON • OFF
tls_version	Set the tls_version to 'TLSv1.2'.

The SSL settings in my.ini file is shown in following screen.

```
#skip_ssl

ssl_ca=ca.pem
ssl_cert=server-cert.pem
ssl_key=server-key.pem
ssl_cipher="DHE-RSA-AES128-GCM-SHA256:AES128-SHA"
require_secure_transport=ON
tls_version=TLSv1.2
```

5. Restart the MySQL Service.

Configuring the Application (Modules) to Use Encrypted Connections to the Databases – MySQL

To configure the Application (Modules) to use encrypted connection to MySQL Server, follow these steps: **Prerequisite:**

- MySQL Server should be enabled for accepting encrypted connections.

For information on the above setting, see [Configuring MySQL to Use Encrypted Connection](#) section.

1. On Application Server, navigate to the parcel configuration file (shipnow.ini) location and open the shipnow.ini in a text editor.

For Example:

<Parcel Artifact Folder>\Flagship\bin\shipnow.ini

2. Add the below string in the shipnow.ini file and save the file.

```
ENCRYPT_DB_COMMUNICATION=ENABLE_ENCRYPTION=y;SSL_CA=ca.pem;SSL_CAPATH=<Client SSL Certificates Directory Path>;SSL_CERT=clientcert.pem;SSL_KEY=client-key.pem;SSL_CIPHER=DHE-RSA-AES128-GCM-
```

```
SHA256:AES128-SHA; SSL_TLS_VERSION=TLSv1.2
```

The description of the string to add in the shipnow.ini file, is shown in following table.

String	Description
ENCRYPT_DB_COMMUNICATION	ENCRYPT_DB_COMMUNICATION is the header of the string.
String	Description
ENABLE_ENCRYPTION	Set this flag to 'y' to turn on encrypted connection to MySQL Server. Valid values are: <ul style="list-style-type: none"> • y • n By default, this key is set to 'n'.
SSL_CA	Provide the path of the MySQL Server Certificate (ca.pem) file used in the server. For more information, see Configuring MySQL to Use Encrypted Connection section, Step 1.
SSL_CAPATH	Provide the path of the client certificate files. Note: In case of Remote MySQL configuration copy all client SSL certificates from MySQL Server to Application Server and provide the path.
SSL_CERT	Provide the path of the client SSL public key certificate file in PEM format.
SSL_KEY	Provide the path of the client SSL private key file in PEM format.
SSL_CIPHER	Provide the cipher algorithm supported by MySQL. Note: Use Cipher "DHE-RSA-AES128-GCM SHA256:AES128-SHA". This should be also used in MySQL Server.
TLS_VERSION	Set the TLS_VERSION to 'TLSv1.2'.

3. For KewillFlagshipConnectorFileService, KewillFlagshipDatabaseFileService, KewillFlagshipServerBridgeService, KewillReportingService, BluJayParcelCensusTool and BluJayParcelDataUploadTool Services:

Navigate to the <Parcel Artifact Folder>/Flagship/java/conf/configuration.properties file and update the fields as shown in Step 6.

4. For UCM:

Navigate to the <Parcel Artifact Folder>Flagship/ucm/java/META-INF/config.xml file and update the fields as shown in Step 6.

5. For UCMPurge:

Navigate to UCM Purge Property file (shown below) and update the fields under #DB SSL properties as shown in Step 6.

<Parcel Artifact Folder>Flagship/ucm/java/META-INF/UCMPurge.properties.xml

6. Update the fields, as shown in following table.

Fields	Description
useSSL	Set this field to allow the SSL settings on the services. Valid values are: <ul style="list-style-type: none"> • true • false

Fields	Description
requireSSL	Set this field to allow the connection between MySQL and the Services. Valid values are: <ul style="list-style-type: none"> • true • false • The 'requireSSL' settings should be 'true' at Java Services and SSL settings should be configured at MySQL.
verifyServerCertificate	Set this field to verify the MySQL Server certificate. Valid values are: <ul style="list-style-type: none"> • true • false If verifyServerCertificate is set to true, then you need to configure trustCertificateKeyStoreUrl and trustCertificateKeyStorePassword fields.
trustCertificateKeyStoreUrl	Provide the path of the truststore file, which is created by executing the command from <u>Creating and Importing Truststore</u> section. For Example: file:/C:/mysql/truststore
trustCertificateKeyStorePassword	Provide the password to the certificate, which is created by executing the command from <u>Creating and Importing Truststore</u> section. For Example: testmysql

clientCertificateKeyStoreUrl	<p>Provide the path of the keystore file, which is created by executing the command from Creating and Importing Client Keystore section.</p> <p>For Example: file:/C:/mysql/keystore</p> <p>This is optional field. If the credentials which you are using to connect to mysql has been configured with ssl_type as x509 then you need to import client certificate to keystore.</p> <p>You can check with the below query: SELECT ssl_type FROM mysql.user WHERE USER='<user name which is used to connect to database>';</p>
Fields	Description
clientCertificateKeyStorePassword	<p>Provide the password to the keystore certificate which is created by executing the command from Creating and Importing Client Keystore section.</p> <p>For Example: mypassword</p> <p>This is optional field. If the credentials which you are using to connect to mysql has been configured with ssl_type as x509 then you need to import client certificate to keystore.</p>
tlsVersion	Set the tlsVersion to 'TLSv1.2'.

7. On Application Server, navigate to the dbdefines.php file in a text editor and update the fields, as shown in following table. **For Example:** <Parcel Artifact Folder>\Flagship\WebGUI\defines\dbdefines.php

String	Description
ENABLE_ENCRYPTION	<p>Set this flag to 'y' to turn on encrypted connection to MySQL Server. Valid values are:</p> <ul style="list-style-type: none"> • y • n <p>By default, this key is set to 'n'.</p> <p>Note: The flag value is case sensitive, and user has to set it with lower case 'y' or 'n'.</p>
SSL_CA	<p>Provide the path of the MySQL Server Certificate (ca.pem) used in the server.</p> <p>For more information, see Configuring MySQL to Use Encrypted Connection section, Step 1.</p>

SSL_CAPATH	Provide the path of the Certificate Authority (CA) certificate file where we placed in the client.
SSL_CERT	Provide the path of the client SSL public key certificate file in PEM format.
SSL_KEY	Provide the path of the client SSL private key file in PEM format.
SSL_CIPHER	Provide the cipher algorithm supported by MySQL. Note: Use Cipher "DHE-RSA-AES128-GCM-SHA256:AES128-SHA". This should be also used in MySQL Server.
SSL_TLS_VERSION	Set the SSL_TLS_VERSION to 'TLSv1.2'.

8. Restart the following services:

- Kewill DiServer Service
- Kewill IA Service
- Kewill Notification Service
- Kewill Scheduler Service
- Kewill Tracking Service
- KewillFlagshipConnectorFileService
- KewillFlagshipDatabaseFileService
- KewillFlagshipServerBridgeService
- KewillReportingService
- BluJayParcelCensusTool
- BluJayParcelDataUploadTool
- For UCM: Restart BluJayUCMServer Service.
- For UCM Purge: Restart BluJayUCMPurgeService Service.

Creating and Importing Truststore

To create and import Truststore, follow these steps:

1. Open a command prompt using Administrative privileges, and then Navigate to the %jre%\bin folder: For KewillFlagshipConnectorFileService, KewillFlagshipDatabaseFileService, KewillFlagshipServerBridgeService, KewillReportingService, BluJayParcelCensusTool and BluJayParcelDataUploadTool Services: Navigate to Flagship\jre_x86\bin folder.

For Example: cd <Parcel Install Folder>\Flagship\java\jre_x86\bin For UCM and UCM Purge: Navigate to UCM %jre%\bin

For Example:
cd <Parcel Install Folder>\Flagship\ucm\java\jre\bin

2. To import the MySQL server certificate (ca.pem) into keystore, execute the below command: `keytool -importcert -alias <alias-name> -file <path to ca.pem> -keystore <truststore path> -storepass <password>`

For Example: `keytool -importcert -alias MySQLCACert -file "C:\ProgramData\MySQL\MySQL Server 8.0\Data\ca.pem" -keystore "c:/mysql/truststore" -storepass testmysql` • `keytool`: This is the main tool to import the MySQL server certificate into keystore.

- `<alias-name>` : Provide the name of the certificate file.

For Example:
MySQLCACert.

- - `<path to ca.pem>`: Provide the path of ca.pem that server uses.

For Example:

C:\ProgramData\MySQL\MySQL Server 8.0\Data\ca.pem

- - <truststore path>: Provide the path where you want to create the truststore file.

Note: Make sure there are no spaces in the path.

For Example:

c:/mysql/truststore

- - <password>: Provide the password to the certificate file.

For Example:

testmysql

3. For 'Trust this certificate? no:' Type 'yes' or 'y' and then click <Enter> from your keyboard.

Now, the truststore file will get created.

Configure the created truststore file and password from the above command in trustCertificateKeyStoreUrl and trustCertificateKeyStorePassword fields.

Creating and Importing Client Keystore

To create and import Client Keystore, follow these steps:

Note: Make sure that OpenSSL is installed on the Application Server. If it is not installed, please click below link to download and install: <https://www.openssl.org/source/>

1. On Application Server, open a command prompt using Administrative privileges, and then Navigate to OpenSSL \bin folder.

Note: If users copy certificates to Application Machine, they can execute the below command in Application Machine.

2. To convert client-cert.pem, client-key.pem to client-keystore.p12 file, execute the below command:

```
openssl pkcs12 -export -in <client-cert.pem path> -inkey <client- key.pem path> -name <name>
-passout pass:<password> -out <client- keystore.p12 path>
```

For Example: openssl pkcs12 -export -in "C:\ProgramData\MySQL\MySQL Server 8.0\Data\clientcert.pem" -inkey "C:\ProgramData\MySQL\MySQL Server 8.0\Data\client-key.pem" -name "mysqlclient" passout pass:mypassword -out "c:\mysql\client-keystore.p12"

- <client-cert.pem path>: Provide the path of client certificate.

For Example:

C:\ProgramData\MySQL\MySQL Server 8.0\Data\client-cert.pem

- <client-key.pem path>: Provide the path of client-key.pem.

For Example:

C:\ProgramData\MySQL\MySQL Server 8.0\Data\client-key.pem

- <name>: Provide the client certificate keystore name. For Example: mysqlclient
- <password>: Provide the password to the client-keystore.p12 file.

Note: Same password should be used while importing with keytool for Step 3.

For Example: mypassword

- <client-keystore.p12 path>: Provide the path of client-keystore.p12 file.

For Example:

c:\mysql\client-keystore.p12

3. To import client-keystore.p12 file to keystore, open command prompt using Administrative privileges in Application (Modules), and then Navigate to \jre\bin folder.

For Example: cd <Parcel Install

Folder>\Flagship\java\jre_x86\bin Execute the

below command:

```
keytool -importkeystore -srckeystore <client-keystore.p12 path> - srcstoretype pkcs12
srcstorepass
<p12 file password>-destkeystore
<keystore path> -deststoretype JKS -deststorepass <password>
```

For Example:

```
keytool -importkeystore -srckeystore c:\mysql\client-keystore.p12 - srcstoretype pkcs12
-srcstorepass mypassword -destkeystore c:\mysql\keystore -deststoretype JKS
deststorepass mypassword
```

- keytool: To import keystore.p12 to keystore.
 - <client-keystore.p12 path>: Provide the path of client keystore.
- For Example:
- c:\mysql\client-keystore.p12
- <p12 file password>: Provide the password of client keystore. For Example: mypassword
 - <keystore path>: Provide the client certificate keystore path. Note: Make sure there are no spaces in the path.

For Example: c:\mysql\keystore

- <password>: Provide the password to the client certificate key store.

For Example: mypassword

Now, the keystore file will get created.

Configure the created keystore file and password from the above command in clientCertificateKeyStoreUrl and clientCertificateKeyStorePassword fields.

Configuring SSL Settings in MySQL Connector/ODBC

To configure the SSL Settings in MySQL Connector/ODBC, follow these steps:

1. Open ODBC Data Source Administrator window (for both 32-bit and 64-bit).

2. Click **System DSN** tab, select the **didb** Data Source from the System Data Sources list and click Configure.
The MySQL Connector/ODBC Data Source Configuration dialog box appears.
3. In the MySQL Connector/ODBC Data Source Configuration dialog box, complete the fields as described in **Configuring a Connector/ODBC DSN for 32-bit Windows** section under Step 4.
4. Click Details >> to expand the MySQL Connector/ODBC Data Source Configuration dialog and then click **SSL** tab, as shown in following screen.

The screenshot shows the 'MySQL Connector/ODBC Data Source Configuration' dialog box. The 'Connection Parameters' section is at the top, with fields for Data Source Name (didb), Description (MySQL ODBC 8.0 Unicode Driver DSN), TCP/IP Server (127.0.0.1), Port (3306), User (sn_usr), Password (masked), and Database (didb). Below this is the 'SSL' tab, which contains fields for SSL Key, SSL Certificate, SSL CA File, SSL CA Path, SSL Cipher, SSL Mode, and RSA Public Key. The SSL Key field is highlighted with a blue border. At the bottom are buttons for Details, OK, Cancel, and Help.

5. In the **SSL** tab, complete the fields as shown in the following table.

Fields	Description
SSL Key	Enter the path of SSL Client Private Key in PEM format. For Example: <SSL Certificates Path>\<client-key.pem>
SSL Certificate	Enter the path of SSL Client Public Certificate file in PEM format. For Example: <SSL Certificates Path>\<client-cert.pem>
SSL CA File	Enter the Certificate Authority (CA) certificate file in PEM format. For Example: <SSL Certificates Path>\<ca.pem>
Fields	Description

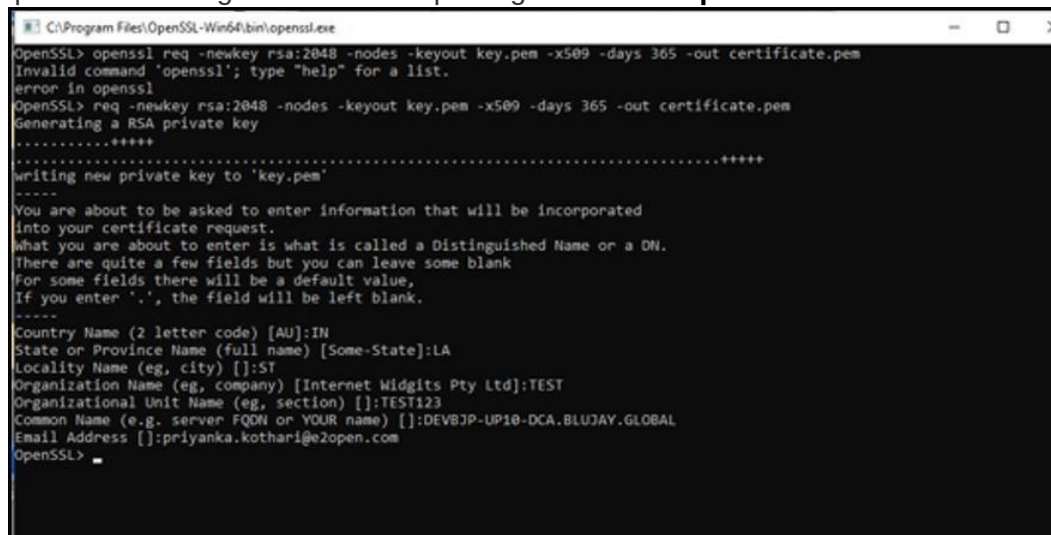
SSL CA Path	Enter the path name of the Certificate Authority (CA) certificate file where we placed in the client. For Example: <SSL Certificates Path>
SSL Cipher	Provide the cipher algorithm supported by MySQL. Note: Use Cipher "DHE-RSAAES128-GCM-SHA256:AES128-SHA". This should be also used in Application (Modules).

- Click OK.

Generating a Self-Signed SSL Certificate using OpenSSL

To generate a Self-Signed SSL Certificate using OpenSSL, follow these steps:

- On Application Server, navigate to OpenSSL\bin folder and launch the openssl.exe using Administrative privileges.**For Example:**



```

C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem
Invalid command 'openssl'; type "help" for a list.
error in openssl
OpenSSL> req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem
Generating a RSA private key
.....+++++
writing new private key to 'key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:LA
Locality Name (eg, city) []:ST
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TEST
Organizational Unit Name (eg, section) []:TEST123
Common Name (e.g. server FQDN or YOUR name) []:DEVBJP-UP10-DCA.BLUJAY.GLOBAL
Email Address []:priyanka.kothari@e2open.com
OpenSSL>

```

- To generate private key and self-signed certificate, execute the below command: `req -newkey rsa:2048 -nodes -keyout <private key> -x509 -days 365 out <self-signed certificate>`
For Example: `req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 out certificate.pem`
-newkey rsa:2048: This specifies that the key should be 2048-bit, which is generated using the RSA algorithm.-nodes: This specifies that the private key should not be encrypted with a pass phrase.<private key>: Provide the name of the private key.<self-signed certificate>: Provide the name of the self-signed certificate.-x509: This specifies req to create a self-signed certificate.-days 365: This specifies that the certificate is valid for 365 days.
- You are now prompted to provide certificate information, as shown in the following table:

In this field...	Do this...
------------------	------------

Country Name	Enter the country name in 2 letter code. For Example: US
State or Province Name	Enter the state or province name. For Example: Massachusetts
Locality Name	Enter the city name. For Example: Chelmsford
Organization Name	Enter the organization name (i.e., company name.) For Example: CA Solutions Ltd.
Organization Unit Name	Enter the company unit name. (i.e., section) For Example: Engineering
Common Name	Enter the Fully Qualified Domain Name (FQDN) of the host that you intend to use the certificate. For Example: localhost

- To view the contents of a certificate in plain text, execute the below command:
`x509 -text -noout -in <self-signed certificate>`
For Example: `x509 -text -noout -in certificate.pem`
 <self-signed certificate>: Provide the name of the self-signed certificate name.
- To combine your private key and self-signed certificate into a PKCS12 file, execute the below command:
`pkcs12 -inkey <private key> -in <self-signed certificate> -export -out <PKCS12 file>`
For Example: `pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12`
 <PKCS12 file>: Provide the name of the PKCS12 file. You will be prompted for export password, which you can leave blank.
- To view and verify the certificate, execute the below command:
`pkcs12 -in <PKCS12 file> -noout -info`
For Example: `pkcs12 -in certificate.p12 -noout -info`
 The certificate file is now created, it can be uploaded to Keystore.

Configuring MSSQL to Use Encrypted Connection

To configure the MSSQL to use encrypted connections, follow these steps:

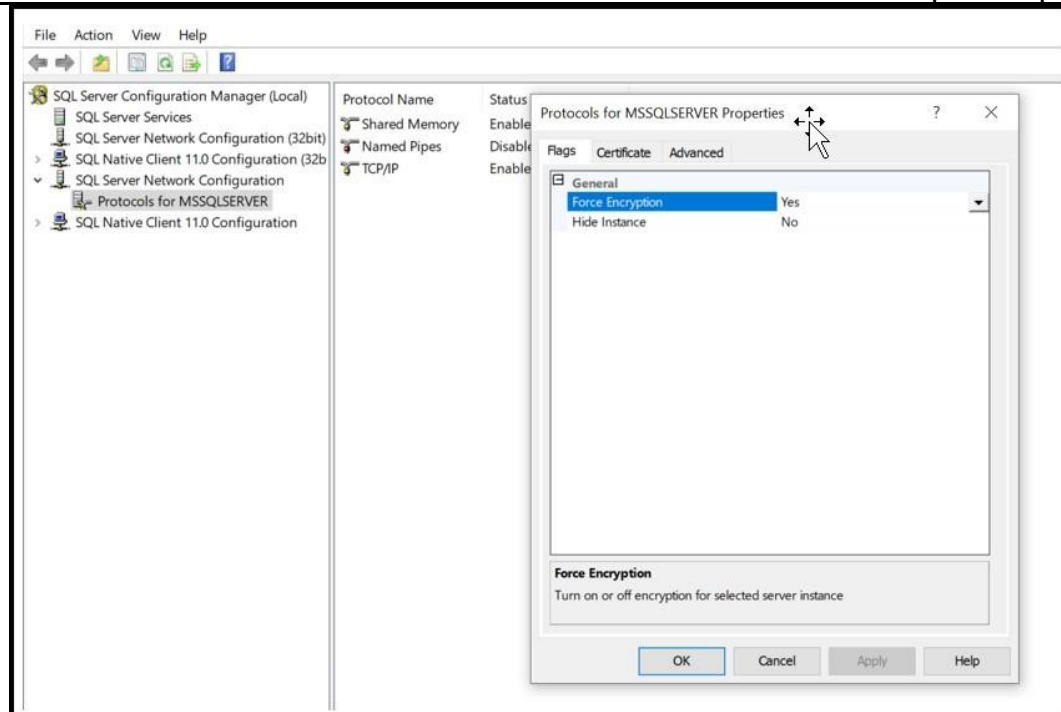
- For encrypted connection SSL Certificates are required. These can be generated in any of the following methods: Get SSL Certificates from Certificate Authority (CA). These certificates should be in PEM format. Get SSL Certificates using openssl, as shown in **Generating a Self-Signed SSL Certificate** using OpenSSL section. Now, import it to the certificate store on MSSQL using Microsoft Management Console.
- Open the Microsoft Management Console (MMC), click **Start**, then **Run** and in the dialog box type 'mmc' and click OK.
- The MMC Console window appears.
- From the **File** menu, select **Add/Remove Snap-in...** The Add/Remove Snap-in dialog box appears.

5. In Add/Remove Snap-in dialog box, under Available snap-ins section, select **Certificate** and then click Add.
The Certificates snap-in dialog box appears.
In Certificates snap-in dialog box, click **Computer account**, and then click Next.
6. Select **Local computer**, and then click Finish.
7. Click OK.
The Add/Remove Snap-in dialog box gets closed.
Your installed certificates are located in the Certificates folder in the Personal container.
8. Expand Certificates, expand Personal, and then right-click Certificates, point to **All Tasks**, and then click Import....
The Certificate Import Wizard window displays.
9. Click Next to continue importing the certificates to a computer.
10. Click Browse.. and select the file to import and then click Next.
11. Enter the password for the private key and then click Next.
12. Select 'Place all certificates in the following store' option and click Browse...
13. In 'Select Certificate Store' dialog box, select 'Trusted Root Certification Authorities', click OK and then click Next.
14. Click Finish to add certificate to the computer.
15. Click X (Close) in the upper right corner of the MMC console to close MMC console screen.

Enabling Encryption at the MSSQL

To enable encryption at the MSSQL, follow these steps:

1. Open the SQL Server Configuration Manager.
2. In SQL Server Configuration Manager, expand SQL Server Network Configuration, right-click Protocols for <server instance>, and then select Properties.
In the Protocols for <instance name> Properties dialog box, on the **Certificate** tab, select the desired certificate from the *Certificate* drop-down menu, and then click OK.
On the **Flags** tab, select **Yes** in the **Force Encryption** box, and then click OK, as shown in following illustration.



3. Restart the SQL Server service.

Configuring the Application (Modules) to Use Encrypted Connections to the Databases – MSSQL

To configure the Application (Modules) to use encrypted connection to MSSQL Server, follow these steps: **Prerequisite:**

- MSSQL Server should be enabled for accepting encrypted connection.

For information on the above setting, see *Generating a Self-Signed SSL Certificate using OpenSSL* section.

To generate a Self-Signed SSL Certificate using OpenSSL, follow these steps:

1. On Application Server, navigate to OpenSSL\bin folder and launch the openssl.exe using Administrative privileges.

```

C:\Program Files\OpenSSL-Win64\bin>openssl.exe
OpenSSL> openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem
Invalid command 'openssl'; type 'help' for a list.
error in openssl
OpenSSL> req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem
Generating a RSA private key
.....+++++
writing new private key to 'key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:IN
State or Province Name (full name) [Some-State]:LA
Locality Name (eg, city) []:ST
Organization Name (eg, company) [Internet Widgits Pty Ltd]:TEST
Organizational Unit Name (eg, section) []:TEST123
Common Name (e.g. server FQDN or YOUR name) []:DEV83P-UP10-DCA.BLUJAY.GLOBAL
Email Address []:priyanka.kothari@e2open.com
OpenSSL>

```

2. To generate private key and self-signed certificate, execute the below command: `req -newkey rsa:2048 -nodes -keyout <private key> -x509 -days 365 out <self-signed certificate>`
For Example: `req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 out certificate.pem`
 -newkey rsa:2048: This specifies that the key should be 2048-bit, which is generated using the RSA algorithm.
 -nodes: This specifies that the private key should not be encrypted with a pass phrase.
 <private key>: Provide the name of the private key.
 <self-signed certificate>: Provide the name of the self-signed certificate.
 -x509: This specifies req to create a self-signed certificate.
 -days 365: This specifies that the certificate is valid for 365 days.
3. You are now prompted to provide certificate information, as shown in the following table:

In this field...	Do this...
Country Name	Enter the country name in 2 letter code. For Example: US
State or Province Name	Enter the state or province name. For Example: Massachusetts
Locality Name	Enter the city name. For Example: Chelmsford
Organization Name	Enter the organization name (i.e., company name.) For Example: CA Solutions Ltd.
Organization Unit Name	Enter the company unit name. (i.e., section) For Example: Engineering
In this field...	Do this...
Common Name	Enter the Fully Qualified Domain Name (FQDN) of the host that you intend to use the certificate. For Example: localhost

4. To view the contents of a certificate in plain text, execute the below command: `x509 -text -noout -in <self-signed certificate>`
For Example: `x509 -text -noout -in certificate.pem`
 <self-signed certificate>: Provide the name of the self-signed certificate name.
5. To combine your private key and self-signed certificate into a PKCS12 file, execute the below command: `pkcs12 -inkey <private key> -in <self-signed certificate> -export -out <PKCS12 file>`
For Example: `pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12`
 <PKCS12 file>: Provide the name of the PKCS12 file.
6. You will be prompted for export password, which you can leave blank. To view and verify the certificate, execute the below command: `pkcs12 -in <PKCS12 file> -noout -info`
For Example: `pkcs12 -in certificate.p12 -noout -info`
 The certificate file is now created, it can be uploaded to Keystore.
 Configuring MSSQL to Use Encrypted Connection section.

Generating a Keystore and Truststore

To generate a keystore and truststore, follow these steps:

1. Open a command prompt using Administrative privileges, and then Navigate to the keystore.exe file in `\ucm\java\jre\bin` folder:
For Example:
`C:\Program Files (x86)\Kewill\Flagship\ucm\java\jre\bin` o `keytool`: This is the main tool to generate the certificate in the keystore file.
 o <Keystore file>: Provide the name of the Keystore file. To generate the certificate in the keystore file, execute the below command:
`keytool -keystore <Keystore file> -genkey -alias client` **For Example:**
`keytool -keystore keystore -genkey -alias client`
2. Once prompted, enter the information required to generate a CSR. A sample key generation section is shown in following screen.

```
C:\WINDOWS\system32>keytool -keystore keystore -genkey -alias client
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: 5VJQ4D3.blujay.global
What is the name of your organizational unit?
[Unknown]: dev
What is the name of your organization?
[Unknown]: blujay
What is the name of your City or Locality?
[Unknown]: hyd
What is the name of your State or Province?
[Unknown]: ts
What is the two-letter country code for this unit?
[Unknown]: in
Is CN=5VJQ4D3.blujay.global, OU=dev, O=blujay, L=hyd, ST=ts, C=in correct?
[no]: yes

Enter key password for <client>
(RETURN if same as keystore password):

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an industry standard format
using "keytool -importkeystore -srckeystore keystore -destkeystore keystore -deststoretype pkcs12".
```

3. To convert keystore to PKCS12 format, execute the below command `keytool -importkeystore -srckeystore <Source keystore name> -destkeystore <Destination keystore name> -deststoretype <Destination keystore type>` **For Example:**
`keytool -importkeystore -srckeystore keystore -destkeystore myKeystore -deststoretype pkcs12`
 - o `-importkeystore`: To import a single entry or all entries from a source keystore to a destination keystore.

o `<Source keystore name>`: Provide the Source keystore name.

For Example: keystore o `<Destination keystore name>`: Provide the Destination keystore name.

For Example: myKeystore o `<Destination keystore type>`: Provide the type of Destination keystore.

For Example: pkcs12

A sample import section is shown in following screen.

```
C:\WINDOWS\system32>keytool -importkeystore -srckeystore keystore -destkeystore myKeystore -deststoretype pkcs12
Importing keystore keystore to myKeystore...
Enter destination keystore password:
Re-enter new password:
Enter source keystore password:
Entry for alias client successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled
```

4. To export the client certificate and import it to the keystore, execute the below command:`keytool -import -keystore <Keystore File Name> -file <Path to client certificate>\clientCer.cer -alias clientCer` **For Example:**
`keytool -import -keystore myKeystore -file <C:\Users\Abc\Desktop\1004\sqlServerPat>\clientCer.cer -alias clientCer` **Note:**
 If clientCer.cer file is not available, use certificate.pem file to add to KeyStore.
 "myKeystore" is the keystore file that is generated.
5. To create the truststore file and add the server certificate to the truststore, execute the below command:

`keytool -import -file <Path to Server certificate>\serverCertificate.cer -alias serverCertificate -keystore <Truststorefile>`

For Example:`keytool -import -file <Path to Server certificate>\serverCertificate.cer -alias serverCertificate -keystore <truststore file>`
`<Path to Server certificate>`: Provide the path of the server certificate.
`<truststore file>`: Provide the name of truststore file.

1. Enter the password to the truststore file.
2. For 'Trust this certificate? no:' Type 'yes' or 'y' and then click <Enter> from your keyboard.

Now, the truststore file will get created.

Configure the created truststore file path and truststore password from the above command in the **didb.settings** tables for SORDDb and IDATADB, see "**Adding DSN for MSSQL Database Connection**" section, **Step 6**.

Configuring SSL Settings in MSSQL

To configure the SSL Settings in MSSQL, follow these steps:

[Enabling TLS 1.2 in Windows Registry Editor](#)

To enable TLS 1.2 in windows registry editor, follow these steps:

1. Open the Registry Editor (Start > Run > regedit).
2. In the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols directory:
3. Create the new key called "TLS 1.2" (Protocols > New > Key TLS 1.2)
4. Right-click the "TLS 1.2" Key and create subkeys:"Client" "Server"
5. Right-click the "Client" and "Server" subkeys and create a new DWORD (32-bit) Value called 'DisabledByDefault'. (New > DWORD (32-bit) Value > DisabledByDefault).
6. Leave the default value as '0'.
7. Right-click the "Client" and "Server" subkeys and create a new DWORD (32-bit) Value called 'Enabled'. (New > DWORD (32-bit) Value > Enabled).
8. Set the default value as '1'.
9. Close the Registry Editor.
10. Restart the Server Machine.

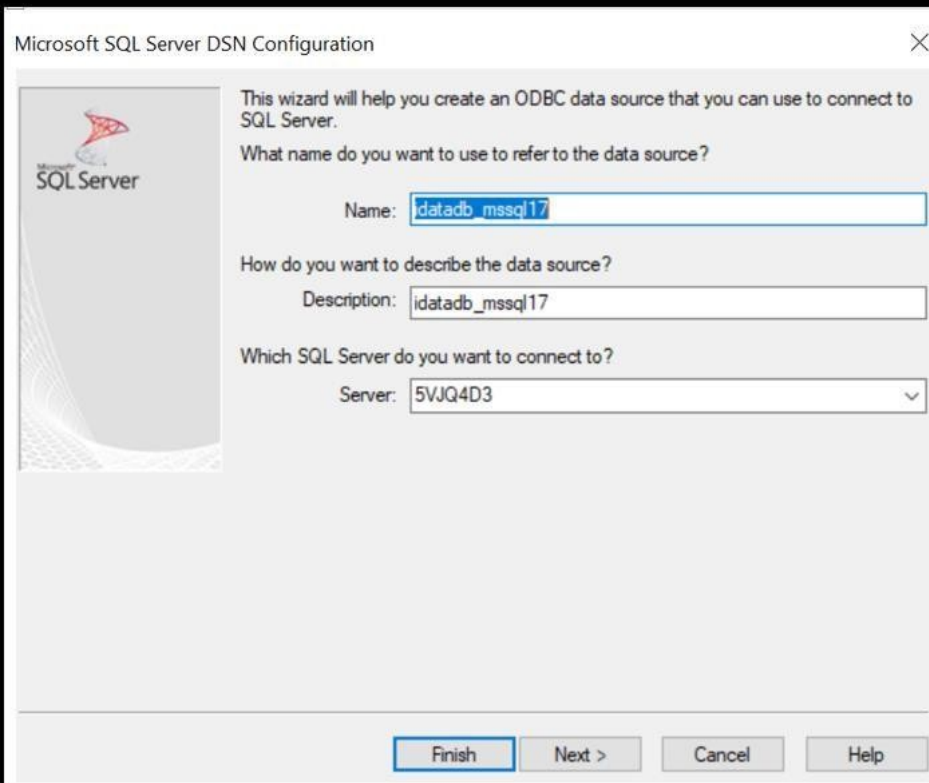
Adding DSN for MSSQL Database Connection

Prerequisite:

- Application Server should be installed with 'ODBC Driver 17 for SQL Server' driver and above.

To add DSN for MSSQL Database Connection, follow these steps:

1. Open ODBC Data Source Administrator (32-bit) window.
2. Select the *System DSN* tab, click Add... and select 'ODBC Driver 17 for SQL Server' drive or later and then click Finish.
Note: For secure encryption only 'ODBC Driver 17 for SQL Server' driver and above are supported.
The Microsoft SQL Server DSN Configuration screen displays.
3. In the Microsoft SQL Server DSN Configuration screen, complete the fields as follows, and then click Next.
4. Select the SQL Server you want to connect from the drop-down list.



Microsoft SQL Server DSN Configuration

This wizard will help you create an ODBC data source that you can use to connect to SQL Server.

What name do you want to use to refer to the data source?

Name:

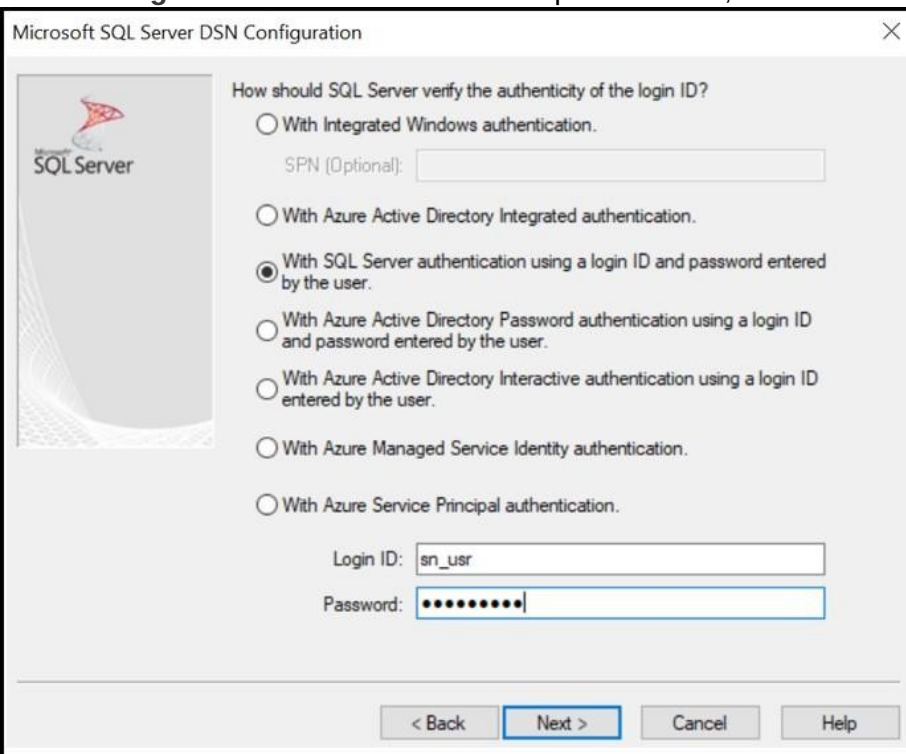
How do you want to describe the data source?

Description:

Which SQL Server do you want to connect to?

Server:

5. In Microsoft SQL Server DSN Configuration screen, select 'With SQL Server authentication using a login ID and password entered by the user.' option and enter **Login ID** and **Password** in the respective fields, and then click Next.



Microsoft SQL Server DSN Configuration

How should SQL Server verify the authenticity of the login ID?

☐ With Integrated Windows authentication.
SPN (Optional):

☐ With Azure Active Directory Integrated authentication.

☒ With SQL Server authentication using a login ID and password entered by the user.

☐ With Azure Active Directory Password authentication using a login ID and password entered by the user.

☐ With Azure Active Directory Interactive authentication using a login ID entered by the user.

☐ With Azure Managed Service Identity authentication.

☐ With Azure Service Principal authentication.

Login ID:

Password:

6. Select the appropriate database from the drop-down list and complete the configuration as shown in following illustration and then click Test Data Sources.. to test the connectivity to that database.

- o idatadb o

- sordb

Microsoft SQL Server DSN Configuration

☒ Change the default database to:
idatadb

Mirror server:
SPN for mirror server (Optional):

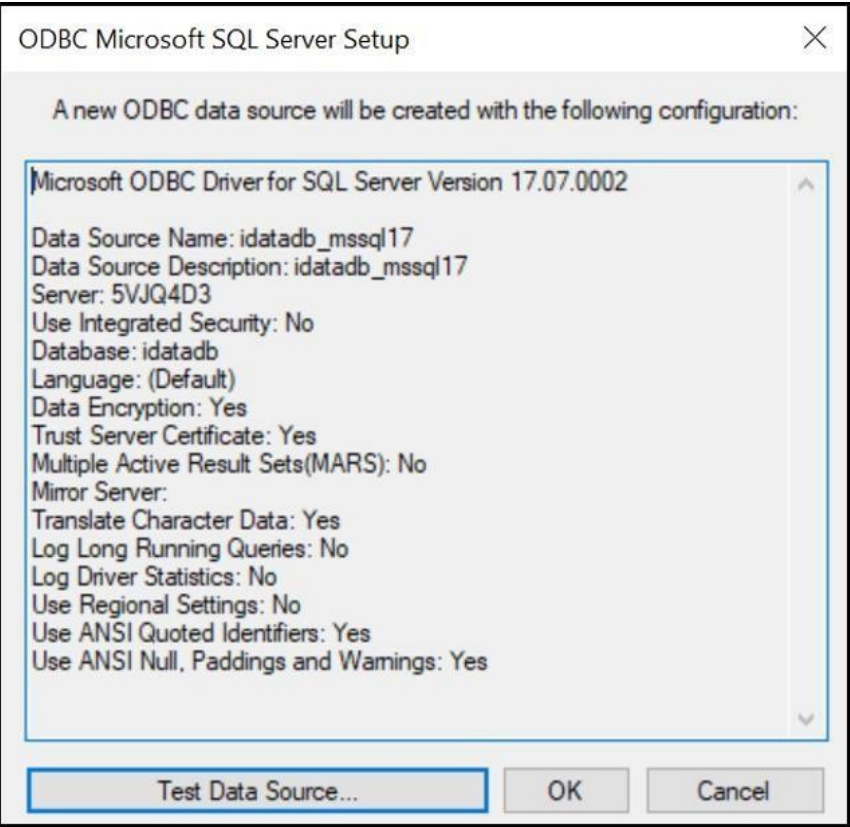
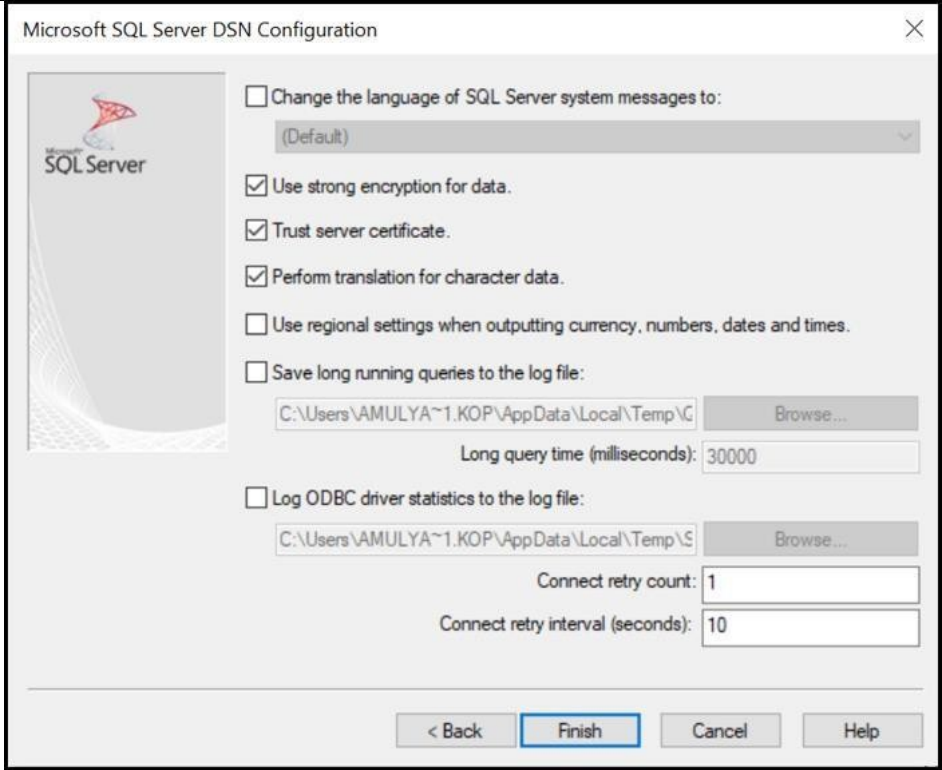
☐ Attach database filename:

☒ Use ANSI quoted identifiers.
☒ Use ANSI nulls, paddings and warnings.
Application intent:
READWRITE

☐ Multi-subnet failover.
☒ Transparent Network IP Resolution.
☐ Column Encryption.
Enclave Attestation Info:

☐ Use FMONLY metadata discovery.

< Back Next > Cancel Help



After adding DSN, do the changes in **didb.settings**, as shown in following table:

SORDB

domain	sub_domain	key_name	key_value
core	sor	dbtype	Change from mysql to mssql
core	sor	dsn	Enter dsn name. For example: sordb_mssql
core	sor	user id	Enter the user id. For example: sn_usr
core	sor	password	Enter the password. For example: shipnowdb
dbconnection	sordb	name	Enter the sordb name. For example: sordb
dbconnection	sordb	username	Enter the sordb username. For example: sn_usr
dbconnection	sordb	password	Enter the sordb password. For Example: shipnowdb
dbconnection	sordb	driver	Change to com.microsoft.sqlserver.jdbc.SQLServerDriver
domain	sub_domain	key_name	key_value
dbconnection	sordb	url	Enter the URL in jdbc:sqlserver://localhost:1433;databaseName=sordb format. For Example: jdbc:sqlserver://5VJQ403.blujay.global:1433;databaseName=sordb
dbconnection	sordb	trustStore_path	Enter the trustStore path. For Example: C:\Users\Blujay\myTrustStore
dbconnection	sordb	trustStore_password	Enter the trustStore password. For Example: test123
dbconnection	sordb	use_secure_encryption	Set this flag to 'y' to turn on encrypted connection to MSSQL Server. Valid values are: • y • n By default, this key is set to 'n'.

machine_name	domain	sub_domain	key_name	key_value
ALL	core	sor	dsn	sordb_mssql
ALL	core	sor	user id	sn_usr
ALL	core	sor	password	shipnowdb
ALL	core	sor	enable_batch_log	n
ALL	core	sor	addparam	
ALL	core	sor	send_userpass_seperately	n
ALL	core	sor	dbtype	mssql
ALL	dbconnection	sordb	name	sordb
ALL	dbconnection	sordb	type	JDBC
ALL	dbconnection	sordb	url	jdbc:sqlserver://5VJQ4D3.blujay.global:1433;Data
ALL	dbconnection	sordb	username	sn_usr
ALL	dbconnection	sordb	password	shipnowdb
ALL	dbconnection	sordb	driver	com.microsoft.sqlserver.jdbc.SQLServerDriver
ALL	dbconnection	sordb	dialect	
ALL	dbconnection	sordb	trustStore_path	C:\Users\Amulya.Koppula\myTrustStore
ALL	dbconnection	sordb	trustStore_password	test123
ALL	dbconnection	sordb	use_secure_encryption	y

IDATADB

domain	sub_do main	key_name	key_value
core	idata	dbtype	Change from mysql to mssql.
core	idata	dsn	Enter dsn name. For example: idatadb_mssql17
core	idata	user id	Enter the user id. For example: sn_usr
core	idata	password	Enter the password. For example: shipnowdb
domain	sub_do main	key_name	key_value
dbconnection	idatadb	name	Enter the idatadb name. For example: idatadb
dbconnection	idatadb	username	Enter the idatadb username. For example: sn_usr
dbconnection	idatadb	password	Enter the idatadb password. For Example: shipnowdb
dbconnection	idatadb	driver	Change to com.microsoft.sqlserver.jdbc.SQLServe rDriver
dbconnection	idatadb	url	Enter the URL in jdbc:sqlserver:///localhost:1433;databas eName=idatadb format For Example: jdbc:sqlserver:10.0.8.47:1433;database Name=idatadb
dbconnection	idatadb	trustStore_path	Enter the trustStore path. For Example: C:\myTrustStore

dbconnect ion	idatadb	trustStore_pass word	Enter the trustStore password. For Example: test123
dbconnect ion	idatadb	use_secure_enc ryption	Set this flag to 'y' to turn on encrypted connection to MSSQL Server. Valid values are: <ul style="list-style-type: none">• y• n By default, this key is set to 'n'.

machine_name	domain	sub_domain	key_name	key_value
ALL	core	global	document_in_response_part_size	
ALL	ui-app	idata	query_fromhold	N
ALL	core	idata	dsn	idatadb_mssql17
ALL	core	idata	password	shipnowdb
ALL	core	idata	user id	sn_usr
ALL	core	idata	dbtype	mssql
ALL	core	idata	addparam	
ALL	core	idata	send_userpass_seperately	n
ALL	dbconnect	idatadb	name	idatadb
ALL	dbconnect	idatadb	type	JDBC
ALL	dbconnect	idatadb	url	jdbc:sqlserver://10.0.8.47:1433;databaseName=idatadb
ALL	dbconnect	idatadb	username	sn_usr
ALL	dbconnect	idatadb	password	shipnowdb
ALL	dbconnect	idatadb	driver	com.microsoft.sqlserver.jdbc.SQLServerDriver
ALL	dbconnect	idatadb	dialect	
ALL	dbconnect	idatadb	trustStore_path	C:\myTrustStore
ALL	dbconnect	idatadb	trustStore_password	test123
ALL	dbconnect	idatadb	use_secure_encryption	y

Configuring Oracle to Use Encrypted Connection

To configure the Oracle to use encrypted connections, follow these steps:

1. Log in to the machine where the Oracle database is installed.
2. To create a directory where you want to store all the wallets, execute the below commands:

```
mkdir wallets
```

For Example: `oracle@parcel-orcl02-fr4 bin$ mkdir Wallets`

```
cd Wallets
```

For Example: `oracle@parcel-orcl02-fr4 bin$ cd Wallets`
3. To create an empty wallet with auto-login enabled for the Oracle server, execute the below command:

```
orapki wallet create -wallet ./server_wallet -auto_login -pwd <server_wallet_password>
```

For Example:

```
oracle@parcel-orcl02-fr4 Wallets$ orapki wallet create -wallet ./server_wallet auto_login -pwd oracle123
```

Two files are created under the server_wallet directory:

```
server_wallet/cwallet.sso server_wallet/ewallet.p12
```
4. To add a self-signed certificate in the wallet with a distinguished name as CN=Server, OU= Engineering, O=XYZ, and C=US, execute the below command:

```
orapki wallet add -wallet ./server_wallet -dn "CN=server,O=XYZ,OU=Engineering,C=US" -keysize 1024 -self_signed -validity 365 -pwd <server_wallet_password>
```
5. You will find a new pair of private or public keys is created.
For Example:

```
oracle@parcel-orcl02-fr4 Wallets$ orapki wallet add -wallet ./server_wallet -dn "CN=server" -keysize 1024 -self_signed -validity 365 -pwd oracle123
```

6. To export the server certificate to a file, execute the below command:
`orapki wallet export -wallet ./server_wallet -dn "CN=server,O=XYZ,OU=Engineering,C=US" -cert ./server_wallet/cert.txt`
 For Example:
`oracle@parcel-orcl02-fr4 Wallets$ orapki wallet export -wallet ./server_wallet -dn "CN=server" -cert ./server_wallet/cert.txt`
7. To create a wallet for Oracle client with auto login enabled, execute the below command: (proceed the same way as for the server).
`orapki wallet create -wallet ./client_wallet -auto_login -pwd <client_wallet_password>`
 For Example:
`oracle@parcel-orcl02-fr4 Wallets$ orapki wallet create -wallet ./client_wallet auto_login -pwd oracle123`
8. To add a self-signed certificate in the wallet with a distinguished name as CN=Client, OU= Engineering, O=XYZY, and C=US, execute the below command:
`orapki wallet add -wallet ./client_wallet -dn "CN=client,O=XYZ,OU=Engineering,C=US" -keysize 1024 -self_signed -validity 365 -pwd < client_wallet_password >`
 For Example:
`oracle@parcel-orcl02-fr4 Wallets$ orapki wallet add -wallet ./client_wallet -dn "CN=client" -keysize 1024 -self_signed -validity 365 -pwd oracle123`
9. To export the client certificate to a file, execute the below command:
`orapki wallet export -wallet ./client_wallet -dn "CN=client,O=XYZ,OU=Engineering,C=US" -cert ./client_wallet/cert.txt`
 For Example:
`oracle@parcel-orcl02-fr4 Wallets$ orapki wallet export -wallet ./client_wallet -dn "CN=client" -cert ./client_wallet/cert.txt`
10. To exchange the server and client their public keys, execute the below commands:
`orapki wallet add -wallet ./server_wallet -trusted_cert -cert ./client_wallet/cert.txt -pwd <server_wallet_pwd >`
 For Example:
`oracle@parcel-orcl02-fr4 Wallets$ orapki wallet add -wallet ./server_wallet trusted_cert -cert ./client_wallet/cert.txt -pwd oracle123`
`orapki wallet add -wallet ./client_wallet -trusted_cert -cert ./server_wallet/cert.txt -pwd < client_wallet_pwd >`
 For Example:
`oracle@parcel-orcl02-fr4 Wallets$ orapki wallet add -wallet ./client_wallet trusted_cert -cert ./server_wallet/cert.txt -pwd oracle123`

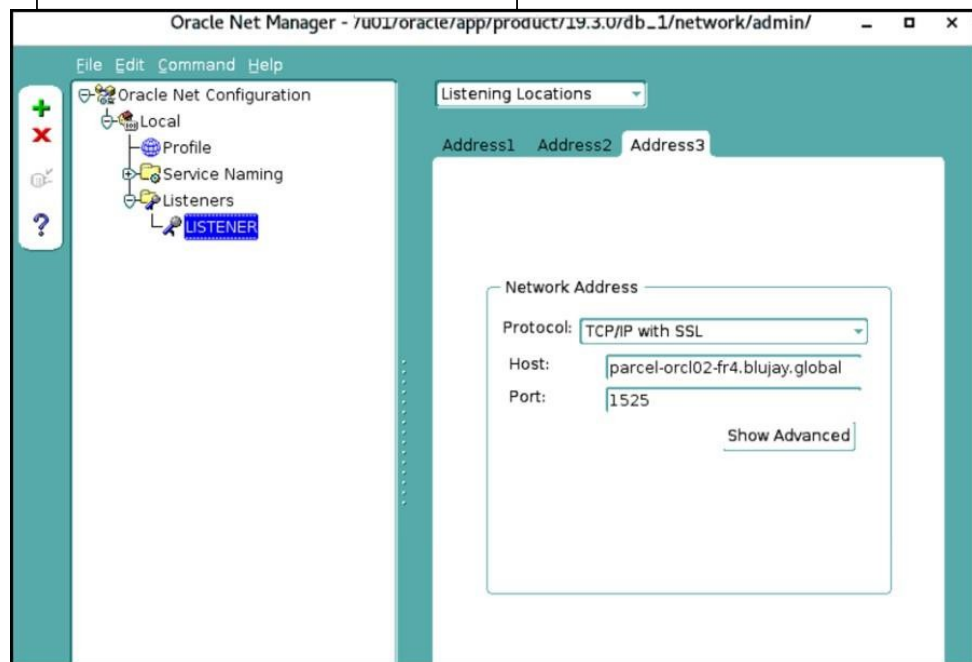
Configuring Database to Use TCPS with Server Key

To configure the network to activate SSL using Oracle Network Manager, follow these steps on the Oracle Database server.

1. Configure the listener.ora file.
 - a. Launch the Net Manager tool. To open network manager, execute the below command: `netmgr`
 - b. Navigate to Local > Listeners > Listener.
 - c. Click Add Address to add Listening Location addresses, as shown in the following table.

In this field...	Do this...
------------------	------------

Protocol	Select the 'TCP/IP with SSL' as protocol from drop-down list.
Host	Enter the database host name. For Example: parcel-orcl02-fr4.blujay.global
Port	Enter the TCPS Port For Example: 1525



- d. Click File > Save Network Configuration to save the configuration settings. The listener.ora network configuration file that you created looks as show below:

For Example:

/u01/app/oracle/product/19.3.0/db_1/network/admin/listener.ora

LISTENER =

(DESCRIPTION_LIST =

(DESCRIPTION =

(ADDRESS = (PROTOCOL = TCP)(HOST = <HostName>)(PORT = <PortNumber>))

)

(DESCRIPTION =

(ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1521))

)

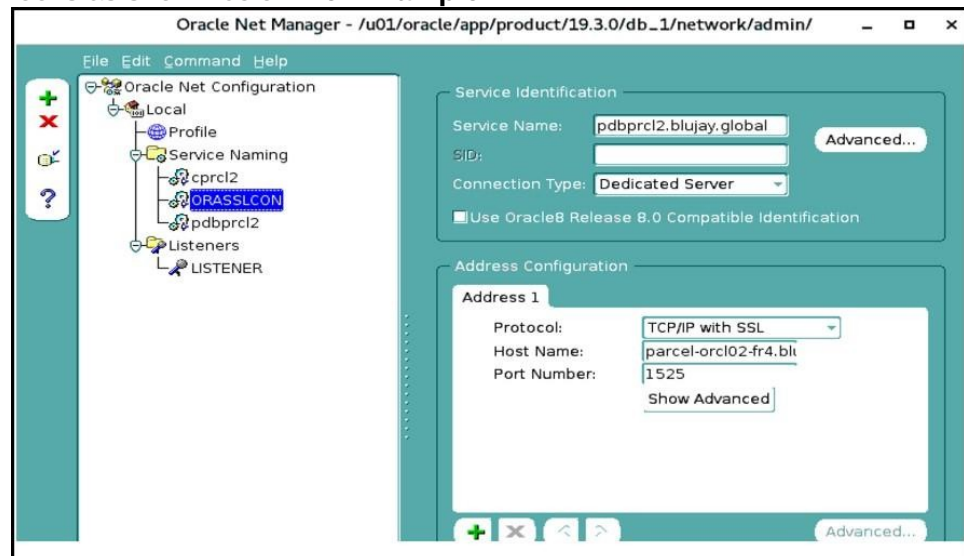
(DESCRIPTION =

(ADDRESS = (PROTOCOL = TCPS)(HOST = <HostName>)(PORT = <PortNumber>))

))

2. Configure the tnsnames.ora file.
 - a. Navigate to Local > Service Naming.

- b. Click Edit > Create. The Net Service Name Wizard: Welcome screen displays.
- c. Enter the name that you want to use to access the database or service in the **Net Service Name** field and click Next.
- d. Select the 'TCP/IP with SSL (Secure Internet Protocol)' protocol used for the database you want to access.
- e. Enter the TCP/IP host name for the computer where the database is located in the **Host Name** field.
- f. Enter the TCP/IP port number for Oracle database in the **Port Number** field and click Next.
- g. Enter the service name of the database that you want to access in the **Service Name** field.
- h. Select the database connection type as 'Dedicated Service' from **Connection Type** drop-down list and click Next.
- i. Click Test... if you want to test the connection of the wizard or else click Finish to create the net service name.
- j. Click File > Save Network Configuration to save the network configuration settings. The tnsnames.ora network configuration file that you created looks as shown below: **For Example:**



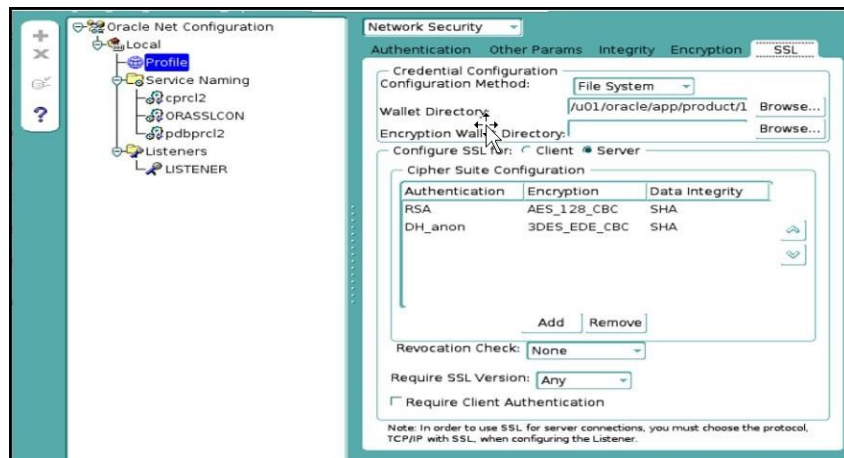
```

ORASSLCON =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCPS)(HOST = <HostName>)(PORT =
<PortNumber>))
)
(CONNECT_DATA =
(SERVER = dedicated)
(SERVICE_NAME= <ServiceName>)
)
)

```

3. Configure the sqlnet.ora file.

- a. Navigate to Local > Profile.
- b. Select 'Network Security' from the drop-down list.
- c. Click **SSL** tab and then select **Server** option, if you do not have an SSL form.
- d. In the Credential Configuration panel, select 'File System' from the *Configure Method* drop-down list and click Browse... and specify the Sever Wallet Directory.
- e. In the Cipher Suite Configuration panel, leave the default settings in **Revocation Check**, **Require SSL Version** and **Require Client Authentication** fields.
- f. Select Cipher Suite as RSA AES_128_CBC_SHA.
- g. Click File > Save Network Configuration to save the network configuration settings. The sqlnet.ora network configuration file that you created looks as show below: **For Example:**



```

SQLNET.AUTHENTICATION_SERVICES= (BEQ, TCPS, NTS)
SSL_VERSION = 0
SSL_CLIENT_AUTHENTICATION = FALSE
WALLET_LOCATION =
(SOURCE =
(METHOD = FILE)
(METHOD_DATA =
(DIRECTORY = /u01/oracle/app/product/19.3.0/db_1/Wallets/server_wallet)
)
)
SSL_CIPHER_SUITES = (SSL_RSA_WITH_AES_128_CBC_SHA,
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA)

```

Configuring the Application (Modules) to Use Encrypted Connections to the Databases – Oracle

To configure the Application (Modules) to use encrypted connection to Oracle, follow these steps:

1. Copy the cwallet.sso file from client wallet present in server to the client where you want to connect to SSL DB Server.
2. Add the below tns entry in tnsnames.ora file present in client location.

```
ORASSLCON =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = TCPS)(HOST = <HostName>)(PORT =
<PortNumber>))
)
(CONNECT_DATA =
(SERVER = dedicated)
(SERVICE_NAME = <ServiceName>)
)
)
```
3. Run Oracle SQL Developer locally.

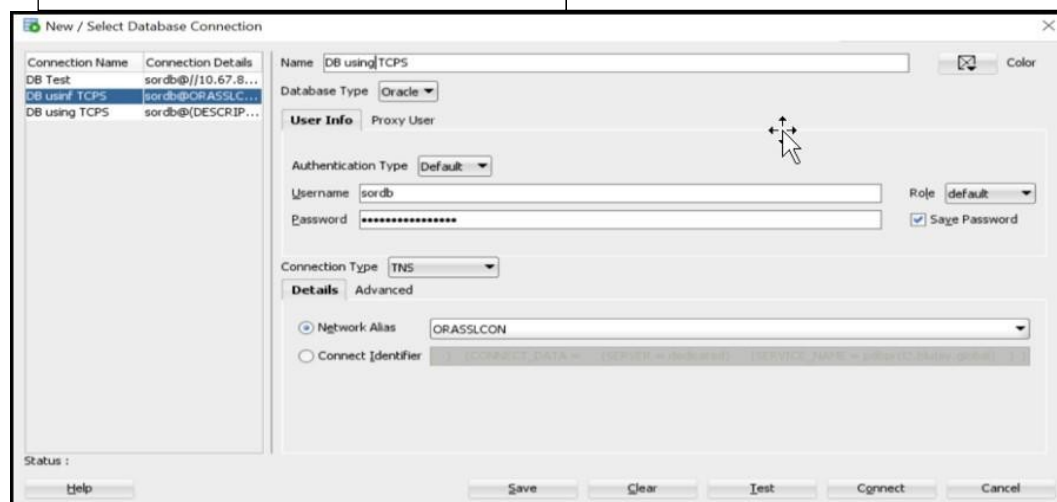
The Oracle SQL Developer home page displays.

1. In the **Connections** pane, right-click and select **New Connection**.

The New / Select Database Connection dialog box appears.

2. In the New / Select Database Connection dialog box, enter the database connection details as shown in the following table.

In this field...	Do this...
Name	Enter the name of the connection.
User Info	Username: Enter the database username. For Example: sordb
	Password: Enter the database password.
Connection Type	Select TNS from the drop-down list.
Details	



3. Click Save to save the configurations.

Configuring SSL DSN Settings in Oracle

To configure the SSL DSN Settings in Oracle, follow these steps:

1. Create sqlnet.ora file in C:\instantclient_19_9 path.
2. Add below details in sqlnet.ora file and save the file.

```
SQLNET.AUTHENTICATION_SERVICES = (BEQ,TCPS,NTS)
SSL_VERSION = 0
SSL_CLIENT_AUTHENTICATION=FALSE
WALLET_LOCATION =
(SOURCE =
(METHOD = FILE)
(METHOD_DATA =
(DIRECTORY = <<ADD wallet path without file name>>)
)
)
```

```
SSL_CIPHER_SUITES= (SSL_RSA_WITH_AES_128_CBC_SHA,
SSL_DH_anon_WITH_3DES_EDE_CBC_SHA)
```

The sqlnet.ora file that you added looks as shown below:

For Example:

```
SQLNET.AUTHENTICATION_SERVICES = (BEQ,TCPS,NTS)

SSL_VERSION = 0

SSL_CLIENT_AUTHENTICATION=FALSE

WALLET_LOCATION =
(SOURCE =
(METHOD = FILE)
(METHOD_DATA =
(DIRECTORY = C:\Users\Srikar.Medathati\Documents\oracle_wallet\client_wallet\client_wallet)
)
)

SSL_CIPHER_SUITES= (SSL_RSA_WITH_AES_128_CBC_SHA, SSL_DH_anon_WITH_3DES_EDE_CBC_SHA)
```

1. Open ODBC Data Source Administrator (32-bit) window.
2. Select the **System DSN** tab, click Add... and select 'Oracle in instantclient_19_9' drive and then click Configure.
The Oracle ODBC Driver Configuration screen displays.
3. In the Oracle ODBC Driver Configuration screen, complete the fields as shown in following table for **sordb** DSN configuration and then click OK.

In this field...	Do this...
Data Source Name	Enter the data source name. For Example: sordb_orcl2
Description	Enter the description. For Example: sordb_orcl2
TNS Service Name	Select the TNS service name related to TCPS service present in tnsnames.ora file.
UserID	

4. Click Test Connection to test the sordb connectivity to the database and enter password in the **Password** field and then click OK.
5. Similarly complete the fields for **idatadb** DSN configuration and then click OK.

In this field...	Do this...
Data Source Name	Enter the data source name. For example: idatadb_orcl2
Description	Enter the description. For Example: idatadb_orcl2
TNS Service Name	Select the TNS service name related to TCPS service present in tnsnames.ora file.
UserID	Enter the idatadb User ID. For Example: idatadb

6. Click Test Connection to test the idatadb connectivity to the database and enter password in the **Password** field and then click OK.
7. Do the changes in **didb.settings** table for SORDB and IDATADB, see "**Changing SOR from MySQL to Oracle**" section, **Step 11**.

Configure Edge in IE Mode

Parcel supports running the UI on the Edge browser in Internet Explorer mode. Please follow instructions in the link below to enable and open the UI on Edge in IE mode.

Internet Explore mode in Microsoft Edge

Change Log On user for all Kewill / BluJay Services

By default, Windows Services run with Local System account which means Local System account should have full access to the configured remote folder location. Instead of allowing system account to access configured Parcel Artifact folder, we can change Log On user for each service by following below steps:

1. Open the Windows Services screen.
2. From the Services list, right-click on "Kewill DiServer Service" and then click Properties.
3. Click **Log On** tab.
4. Select **This account:** option, enter the username and password details in the respective fields that the service is to run under.
5. Click OK.
6. Restart the service.
7. Repeat the Step 2-6 for all Kewill/BluJay services.

Changing Parcel Artifact Folder Location

If user prefers to change configured Parcel Artifact folder location after Parcel Installation is completed, then user needs to follow below steps:

1. Stop all Kewill/BluJay/Apache services.
2. Open a command prompt using Administrative privileges and then navigate to `..\Kewill\Flagship\bin` directory.
3. Select `MoveArtifactsAndLogs.bat` file, and then pass 2 command line arguments, such as :

First Param: Source Path directory where Flagship path is resided. Second Param: Destination Path directory where you want to move the Parcel Artifacts.

The `MoveArtifactsAndLogs.bat` batch file is used to move all log/artifacts/configuration files from existing Parcel Artifact location to the newly configured remote folder location.

Note: Make sure the destination path directory already exists and it has all required privileges.

For Example:

```
>MoveArtifactsAndLogs.bat "C:\Program Files (x86)\Kewill\ArtifactsAndLogs"  
"C:\Blujay\ArtifactsAndLogs"
```

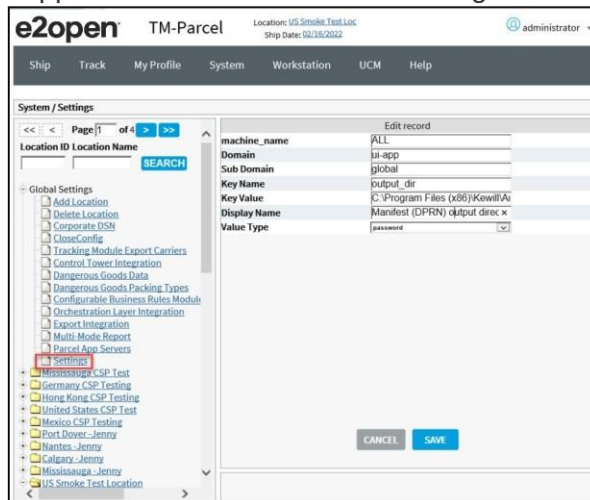
1. Click <Enter> from your keyboard.
The Parcel Artifacts are now moved from one location to another location. After the Parcel Artifacts moved to the required destination path directory, you need to update the below changes.
2. Update Parcel Artifact Folder in `..\Kewill\Flagship\bin` directory.
 - a. Navigate to `..\Kewill\Flagship\bin` directory.
3. Open `ParcelSystem.ini` file and set the value for 'RemoteFileRepository' to defined Destination Path directory where you moved the Parcel Artifacts.

For Example:

C:/Blujay/ArtifactsAndLogs

Note: It is recommended to use forward slash in the path. If using backward slash, use double slashes in the path like "C:\\Blujay ArtifactsAndLogs"

4. Save and close the ParcelSystem.ini file.
5. Open a command prompt using Administrative privileges and navigate to the <Parcel Install Folder>\\Flagship\\ucm\\java folder and then run 'UCM-ServerService-Install.bat' file by passing DBUsername and DBPassword as command line arguments.
For Example: UCM-Server-Service-Install.bat <DBUsername> <DBPassword>
6. Update the settings of output_dir key_name for ui-app Domain in Parcel Application is shown in the following screen.



Notes:

- o Make sure to append Parcel Artifact Folder with "/Flagship/WebGUI/output" directory.
- o Use backward slash in given path.

7. Update PHP.INI File.
For Apache –
..\Kewill\\Flagship\\php\\php.ini For
IIS –
..\Kewill\\Flagship\\phpnts.php.ini
 - a. Navigate to the following location and open the php.ini file in a text editor:
 - b. Search for the word include_path and append new given Parcel Artifact Folder separated by ';'
For Example:
include_path = ".;C:\\php\\includes;C:\\Blujay ArtifactsAndLogs"
Note: Use two backward slashes in given path.
 - c. Save and close the php.ini file.
8. Update httpd.conf file (For Apache only) Navigate to the following location and open the httpd.conf file in a text editor:
..\\Apache-httpd\\Apache24\\conf

- a. Search for <IfModule alias_module> and add the below lines under <IfModule alias_module> section.
Alias/parceloptions/"<add new custom path>" **For Example:**

```
<IfModule alias_module>
ScriptAlias /cgi-bin/"C:/Apache24/cgi-bin/"
Alias/parceloptions/"C:\\Blujay
ArtifactsAndLogs"
</IfModule>
```
 - b. At the end of </IfModule> add the below lines<Directory "<add new custom>">

```
Allow from all
AllowOverride None
Options Indexes FollowSymLinks MultiViews
Require all granted </Directory>
```

For Example:

```
<Directory "C:\\Blujay
ArtifactsAndLogs">
Allow from all
AllowOverride None
Options Indexes FollowSymLinks MultiViews
Require all granted
</Directory>
```

Note: Use two backward slashes in given path, in case of network drive, use four backward slashes at the starting.
 - c. Save and close the httpd.conf file.
9. Update Parcel options in Virtual Directory (For IIS Machine only)For information, see [Add/Update Virtual Directory in IIS](#) section.
 10. Restart all Kewill/BluJay/Apache services.

Supporting UMS and E2Proxy Integration

To support UMS and E2Proxy Integration, update the following keys under Global Settings

machine_name	domain	subdomain	key_name	key_value
ALL	integration	etwoproxy	enable_ums_integration	y

- y = support UMS Integration

The UMS integration layer settings displays, as shown in the following screen.

TM-Parcel

Location: Kewill Chelmsford

Ship Date: 04/18/2022

administrator

Ship

Track

My Profile

System

Workstation

UCM

Help

System / Settings

Page 1 of 4

Location ID Location Name

SEARCH

Global Settings

Add Location

Delete Location

Corporate DSN

CloseConfig

E2NET Watermill Integration

Tracking Module Export Carriers

Control Tower Integration

Dangerous Goods Data

Dangerous Goods Packing Types

Configurable Business Rules Module

Orchestration Layer Integration

Export Integration

Multi-Mode Report

Parcel App Servers

Settings

UMS/E2Proxy Integration

Mississauga CSP Test

Germany CSP Testing

Hong Kong CSP Testing

United States CSP Test

Mexico CSP Testing

Port Dover - Jenny

Nantes - Jenny

Edit record

machine_name

ALL

Domain

integration

Sub Domain

etwoproxy

Key Name

enable_ums_integration

Key Value

y

Display Name

JMS Integration

Value Type

password

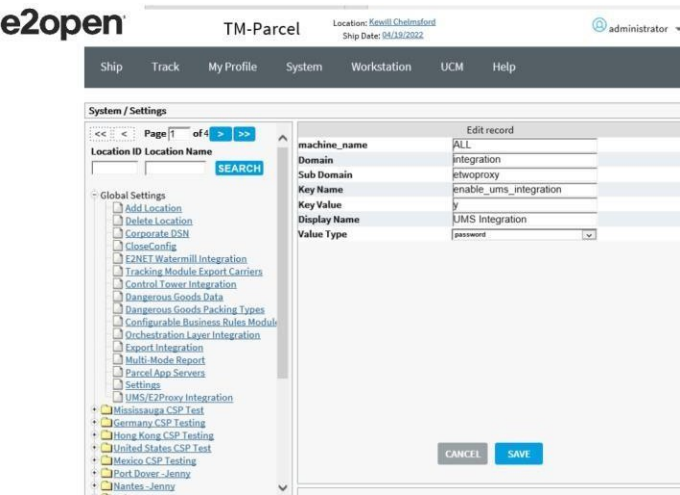
CANCEL

SAVE

machine_name	domain	subdomain	key_name	key_value
ALL	integration	etwoproxy	enable_e2proxy_integration	y

- y = support E2Proxy Integration

The E2Proxy integration layer settings displays, as shown in the following screen.



Configuring IIS 10.0 on Windows Server 2019

Installing IIS 10.0

If you are installing Parcel with Windows Server 2019, you first need to have Microsoft Internet Information Services version 10.0 (IIS 10.0) installed on the server where you install Parcel. To ensure this capability, carry out one of the following procedures:

- If IIS 10.0 is not installed on the server, carry out the following procedure to install and configure IIS 10.0
- If IIS 10.0 is already installed on the server, carry out the configuration procedure in the following sections:
- **Configuring PHP for IIS 10.0**
- **Configuring Bindings**

Notes:

- IIS 10.0 is only available in Windows Server 2019 and Windows Server 10.0.
- You must have System Administrator privileges in Windows to install and/or configure IIS 10.0

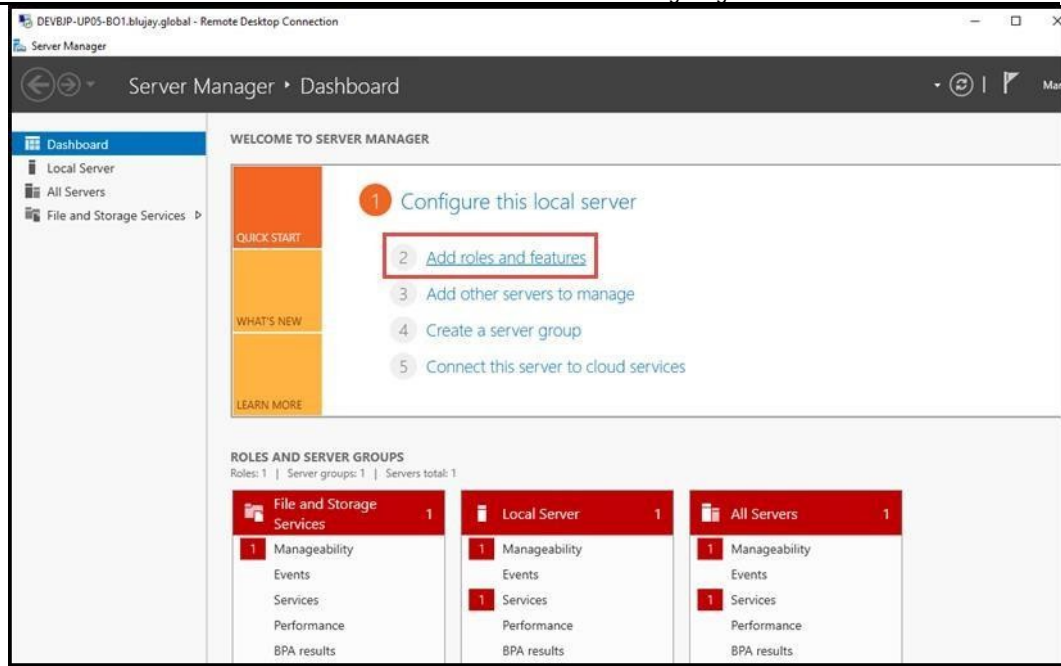
IIS 10 Installation

To install IIS 10.0, follow these steps:

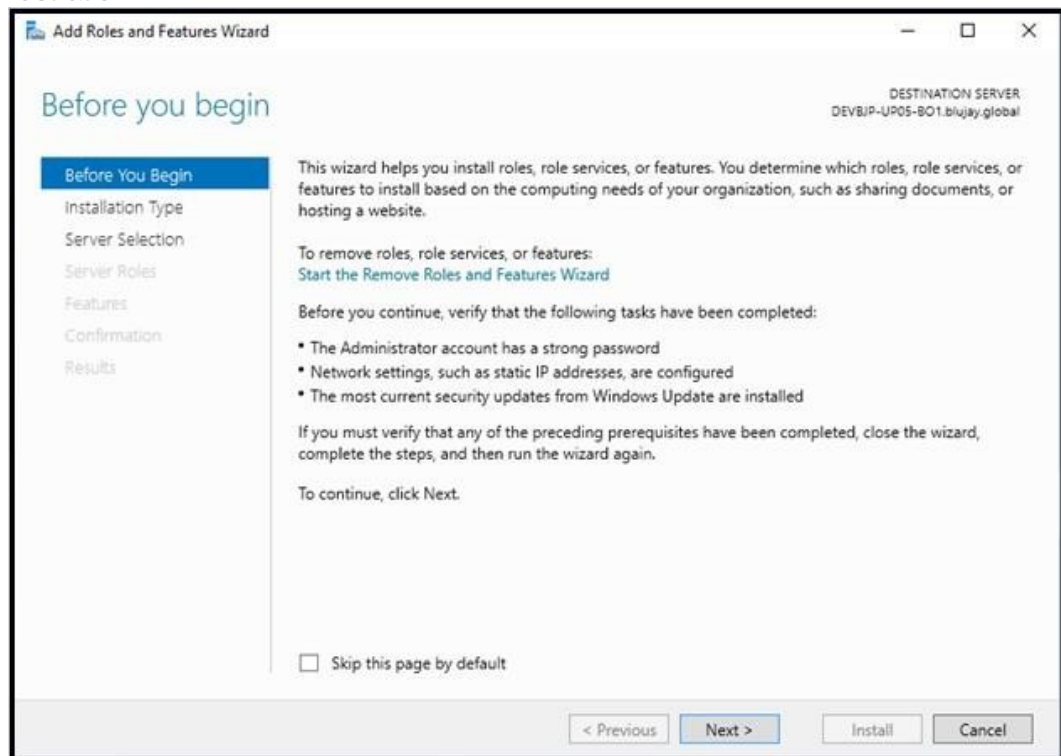
1. Click the Server Manager icon on the desktop or select *Server Manager* using the Start menu to open the Server Manager screen.



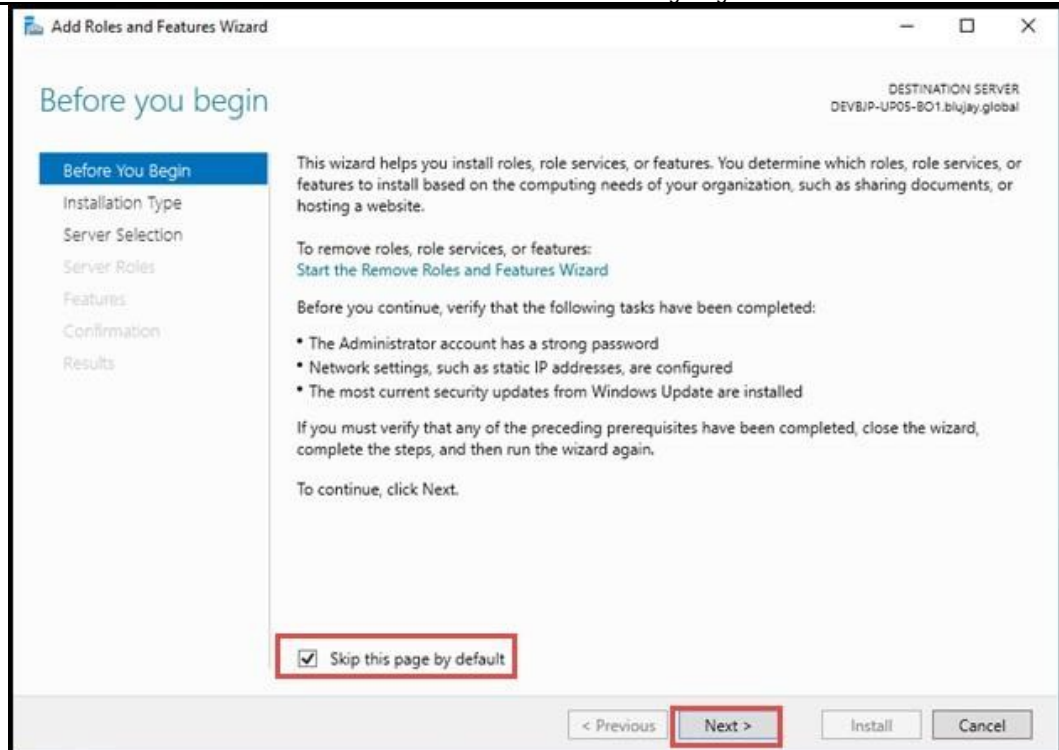
2. In the Server Manager > Dashboard screen, click **Add roles and features**, as shown in following illustration.



The Add Roles and Features Wizard screen displays, as shown in the following illustration.

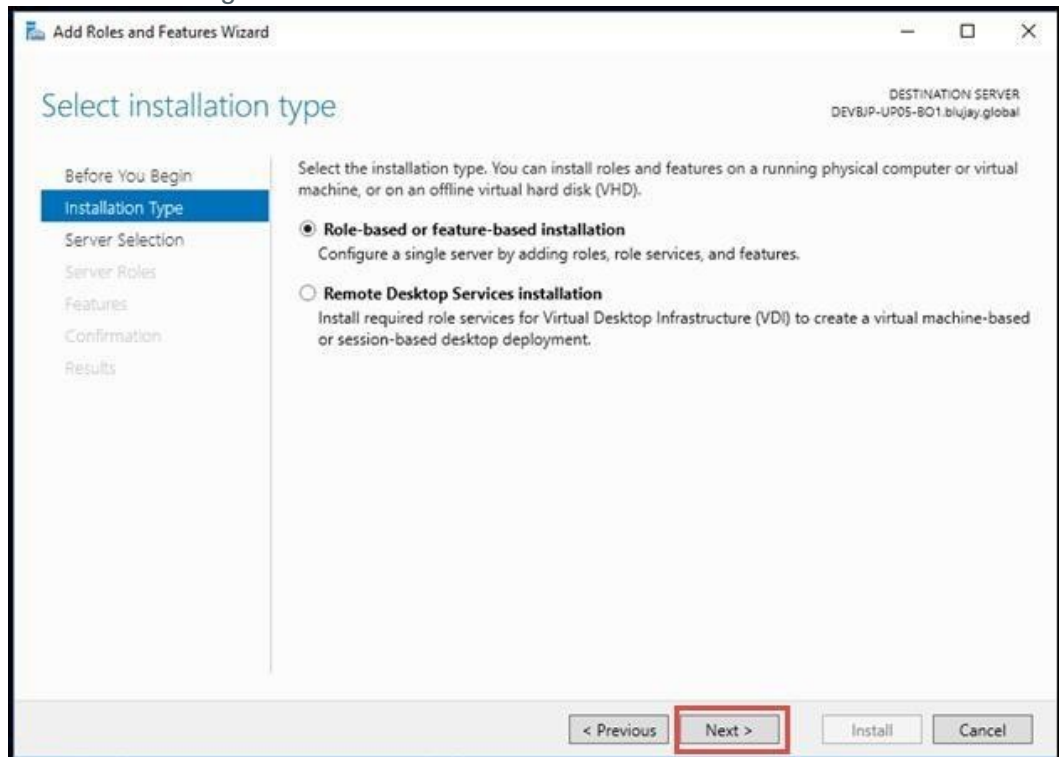


3. In the Add Roles and Features Wizard screen, select *Skip this page by default* checkbox and then click Next, as shown in following illustration.



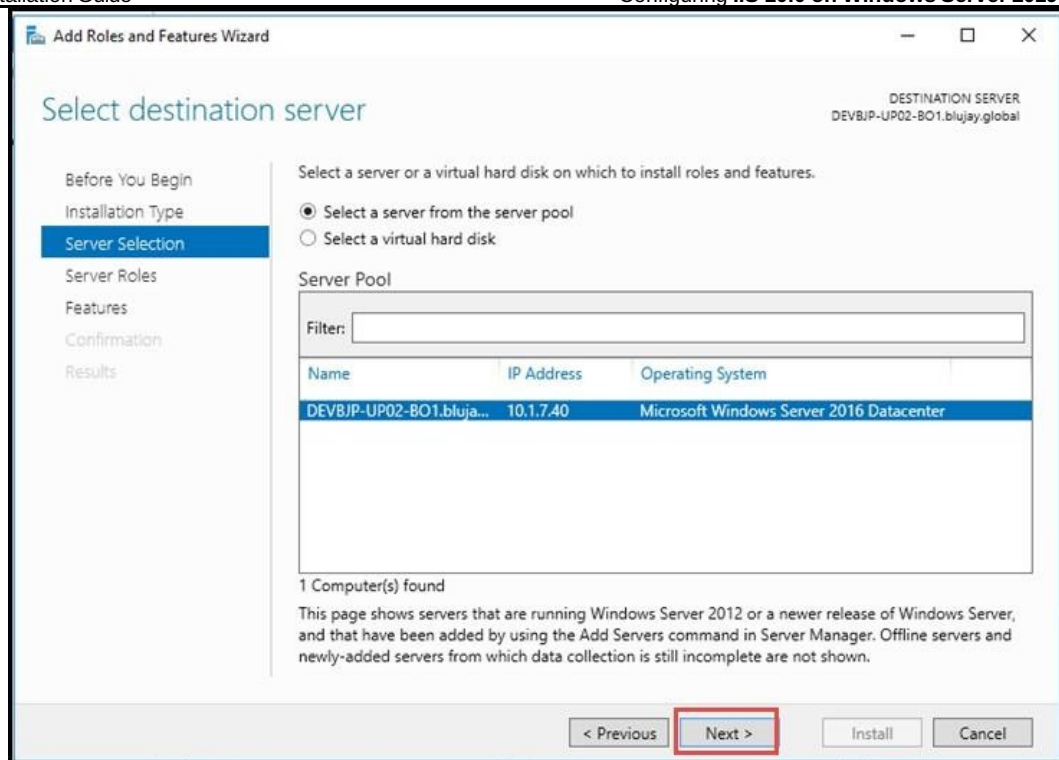
The Select installation type screen displays, as shown in following illustration.

4. In the Select installation type screen, accept the defaults and then click Next, as shown in following illustration.



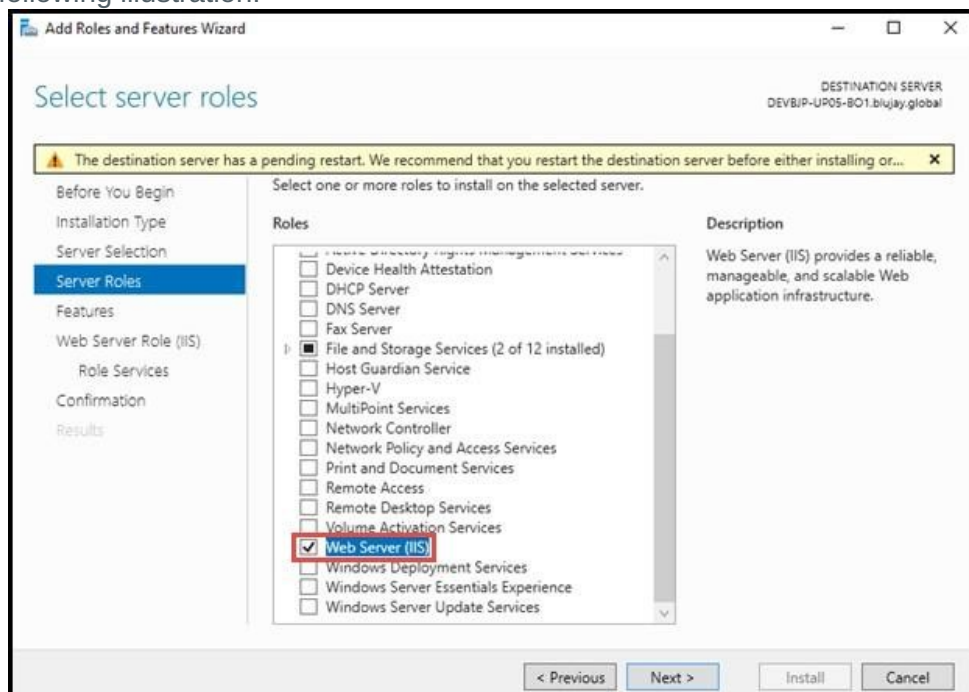
The Select destination server screen displays, as shown in following illustration.

5. In the Select destination server screen, accept the defaults and then click Next, as shown in following illustration.



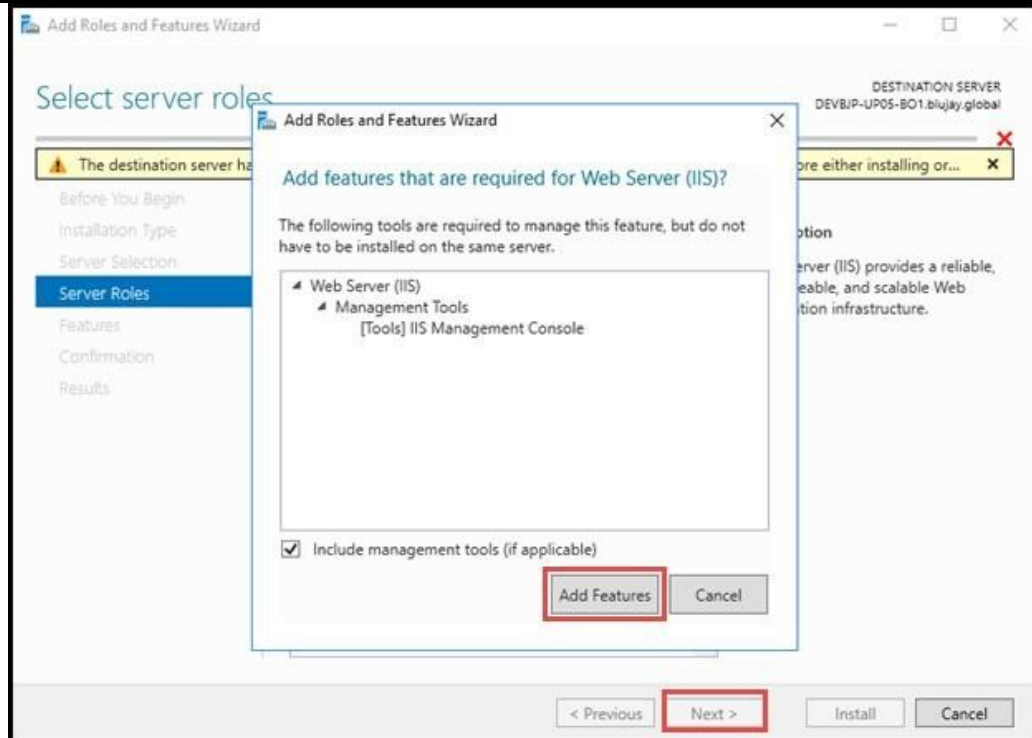
The Select server roles screen displays, as shown in following illustration.

6. In the Select server roles screen, select **Web Server (IIS)** checkbox, as shown in following illustration.



An Add Roles and Features Wizard Pop-up window appears, as shown in following illustration.

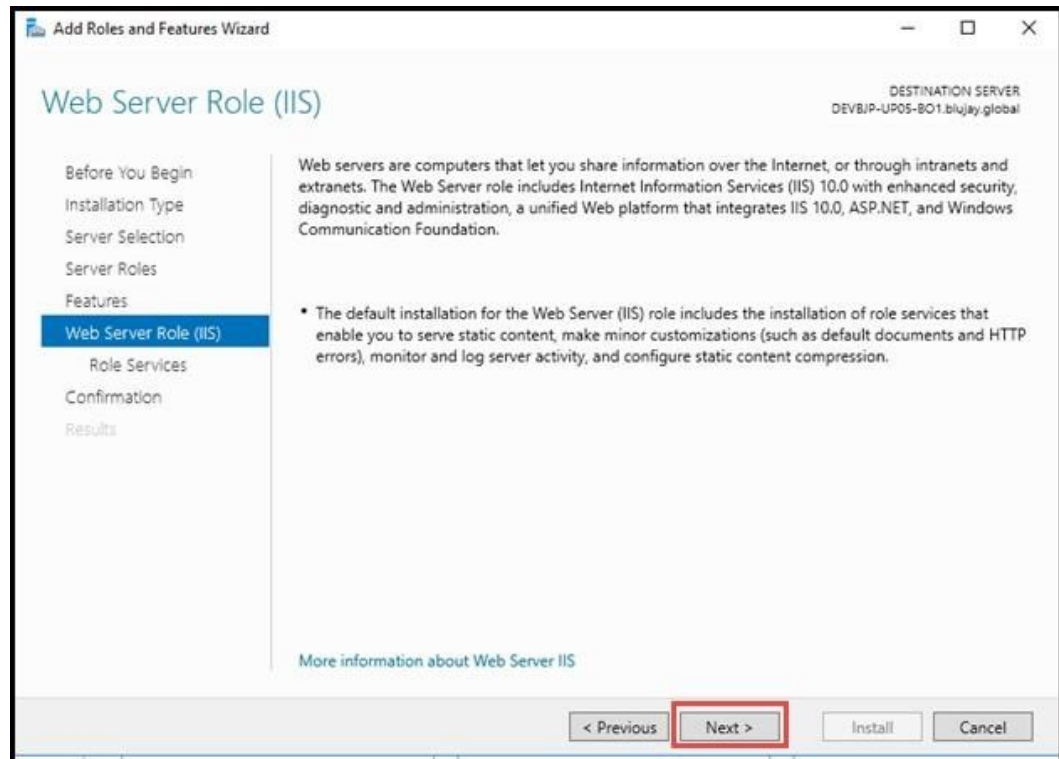
7. In Add Roles and Features Wizard Pop-up window, accept the defaults and click Add Features and then click Next, as shown in following illustration.



Note: Please notice that the Next in Select server roles screen gets enabled, once you click Add Features. The Web Server Role (IIS) screen displays, as shown in following illustration.

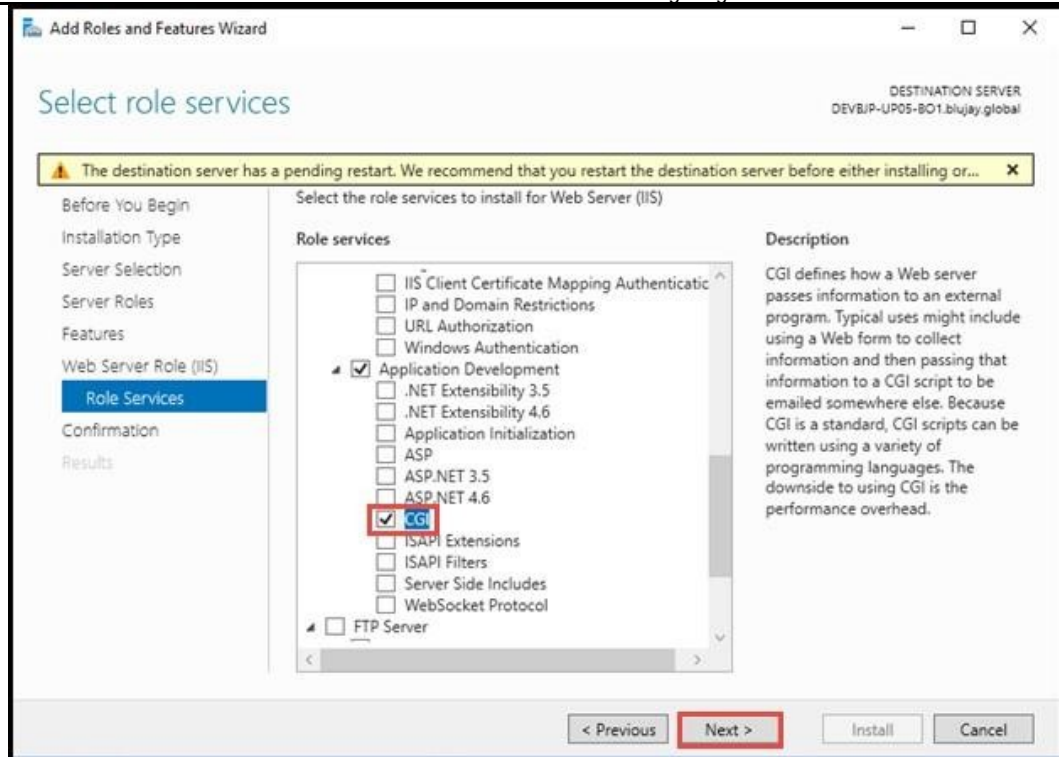
IIS 10.0 on Windows Server 2019

8. In the Web Server Role (IIS) screen, click Next, as shown in following illustration.



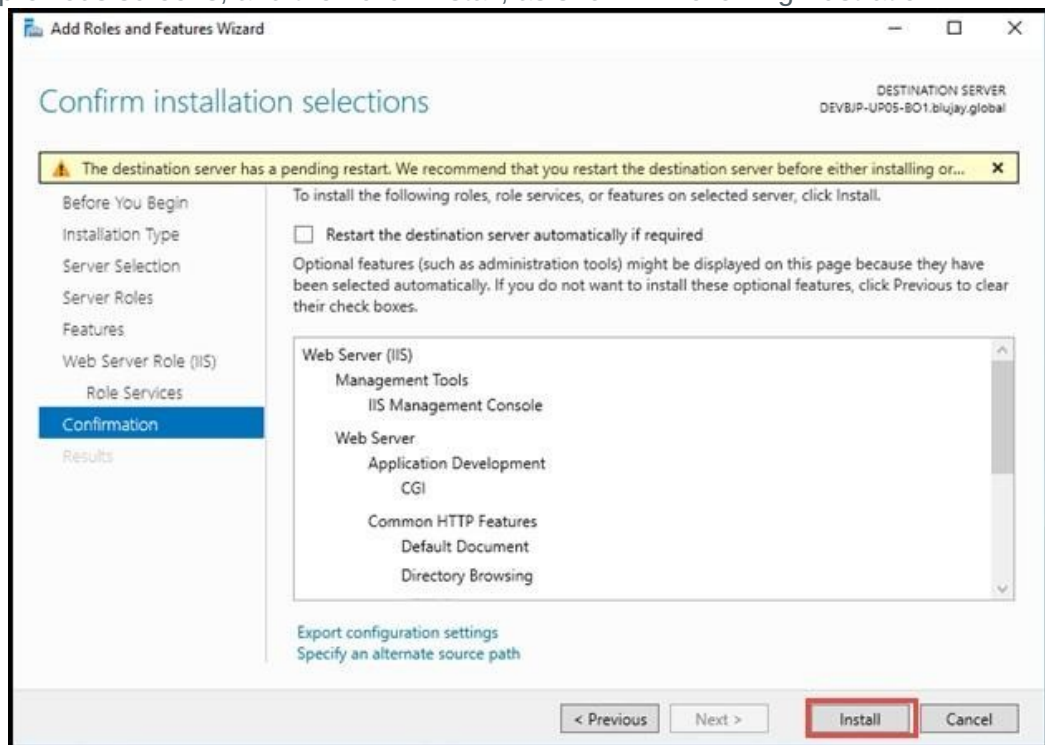
The Select roles services screen displays, as shown in following illustration.

9. In the Select roles services screen, select *CGI* checkbox, accept other defaults and then click Next, as shown in following illustration.

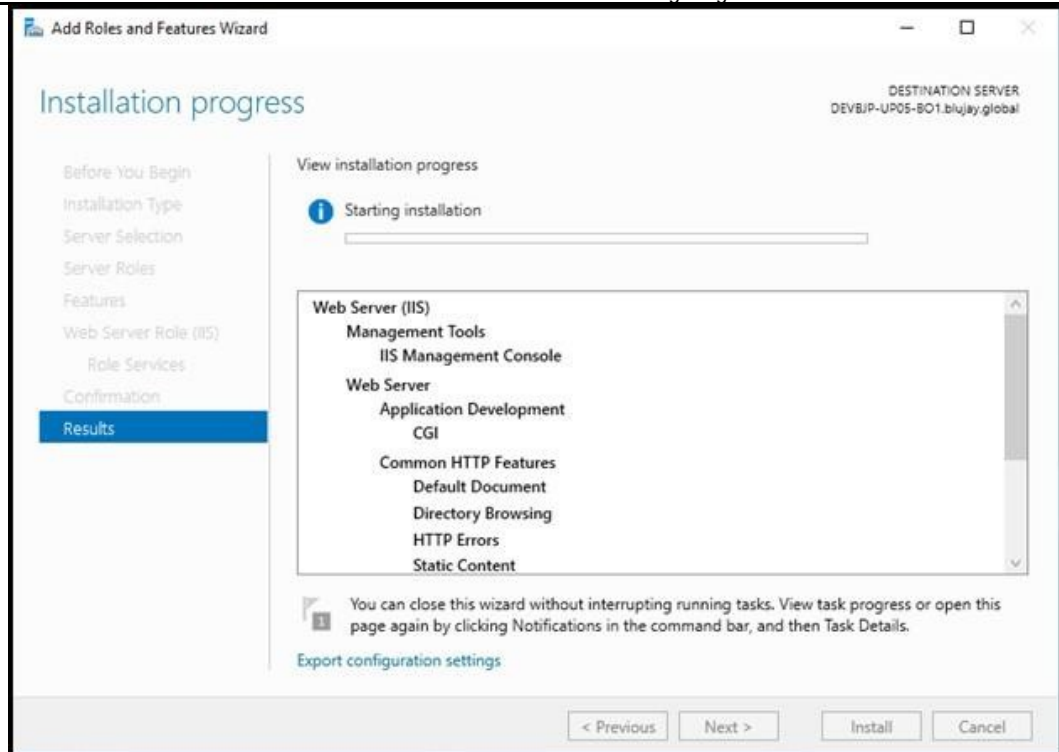


The Confirm installation selections screen displays, as shown in following illustration.

10. In the Confirm installation selections screen, confirm your selections from the previous screens, and then click Install, as shown in following illustration.

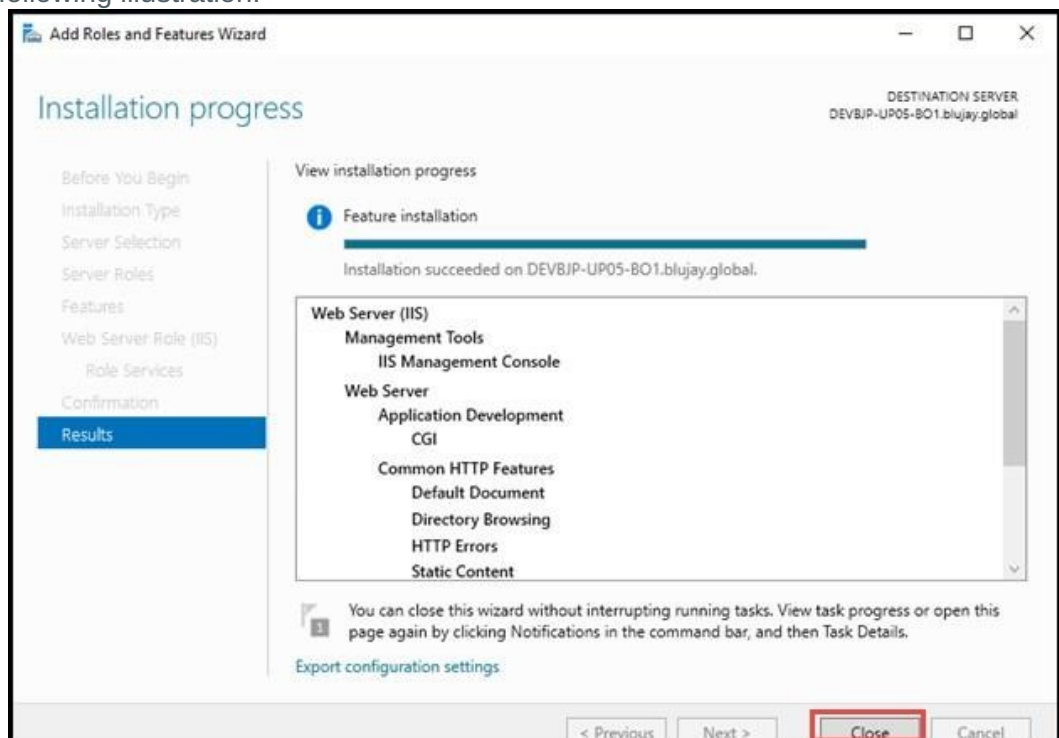


The Installation progress screen displays, as shown in following illustration



After the IIS installation completes the Installation Results screen displays.

11. Verify that the installation was successful, and then click Close, as shown in following illustration.



12. The Web Server Role for IIS is now successfully enabled in Server Manager screen.

Printer Configuration on Windows 2019

Parcel requires a Windows 2019 user with permissions to all necessary local resources and with print access to all peripheral devices (document and label printers); **For Example:** ParcelUser. Before adding printers, create this Windows user. After you create this user, you can add the required printers to Windows Server 2019, and then set up the Parcel Windows services for printing, as described in the following procedures.

To add printers on Windows 2019:

1. Log in to the computer running Windows Server 2019 with the Parcel user you created.
2. As the Parcel user in step 1, add the required document and label printers (network and/or local).

To set up Parcel Windows services for printing:

1. In Windows Administrative Tools, open the Services window.
2. Stop the following Kewill services: Kewill DiServer Service
KewillReportingService
BluJayUCMSERVICE
3. Configure these services for the Parcel user login previously created.
4. Restart the services.

Configuring PHP for IIS 10.0

After installing IIS 10.0, for Parcel to work with IIS 10.0, you need to configure PHP settings as described in the following sections:

- Configuring the PHP.INI File
- Configuring Bindings

Configuring the PHP.INI File

To configure the PHP.INI file:

- Navigate to the following location and open the php.ini file in a text editor:

<Parcel Install Folder>\Flagship\php\php.ini

(Or)

<Parcel Install Folder>\Flagship\ \php.ini

For the below mentioned settings, remove the comments and set them with the following values.

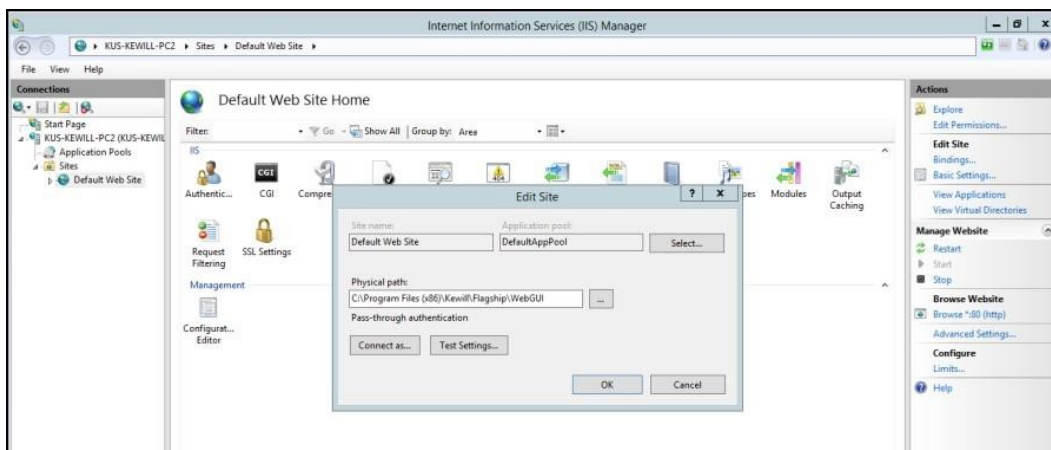
- fastcgi.impersonate = 1
- fastcgi.logging = 0
- cgi.fix_pathinfo = 0
- cgi.force_redirect = 1

For Example:

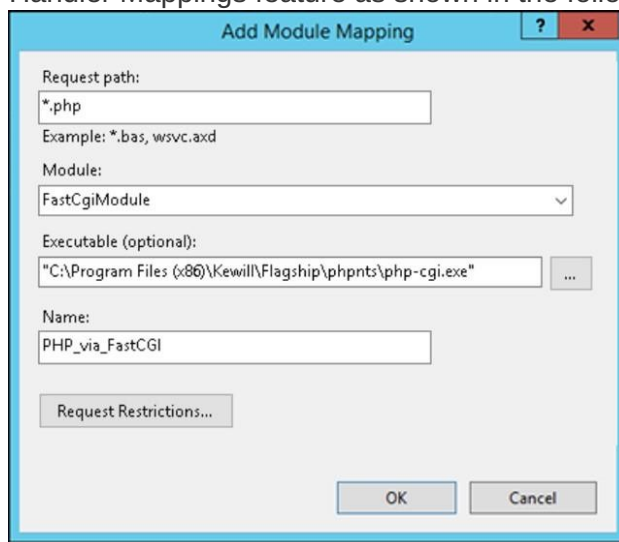
#fastcgi.impersonate needs to be changed as fastcgi.impersonate and ensure that the value should be 1.

- Edit the Default Web Site with the following basic setting:

Set Physical Path = <Parcel Install Folder>\Flagship\WebGUI The following screen shows this setting:

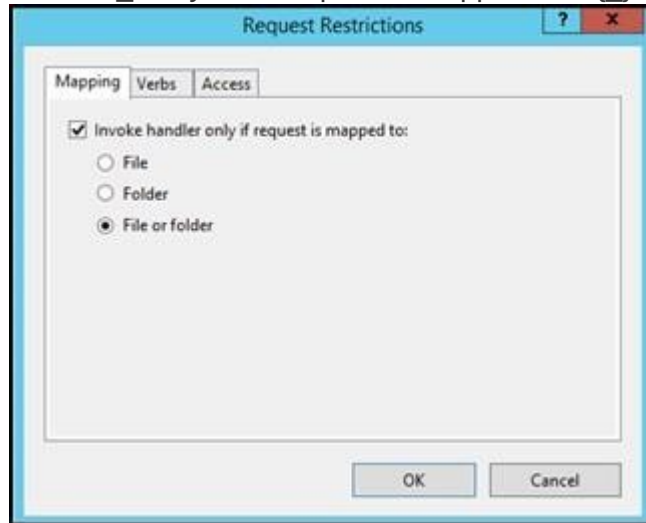


- - a. On the IIS Manager user interface, select the Server Node in the Connections tree view, and then, on the Features View screen open the Handler Mappings feature as shown in the following screen:

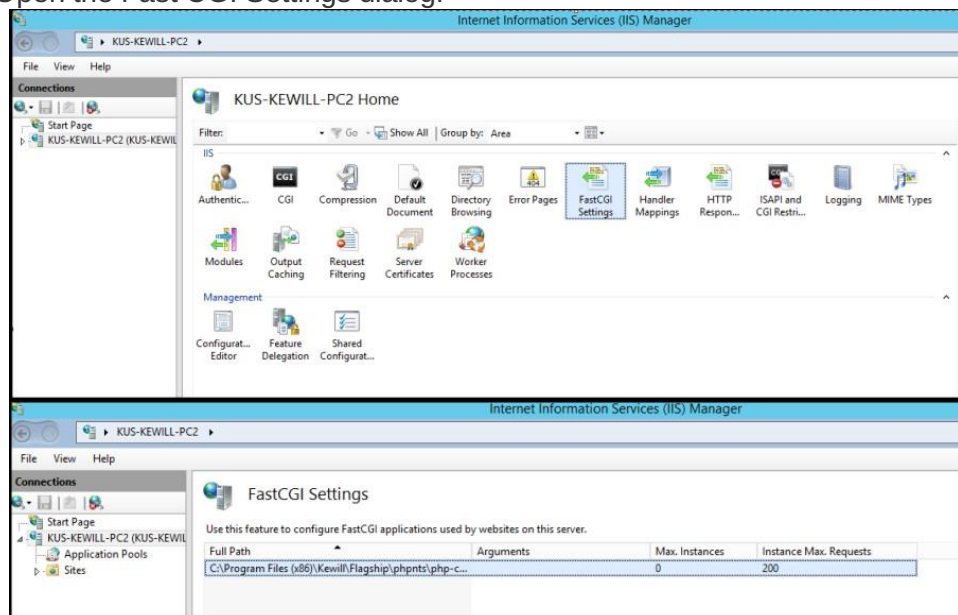


Add the PHP handler mapping configuration as described in the following steps: In the Actions pane click **Add Module Mapping**, and then, on the Add Module Mapping dialog, enter the following values, as shown in the previous screen. Request path: *.php
Module: FastCgiModule
Executable: C:\Path to PHP installation\php-cgi.exe
Name: PHP_via_FastCGI

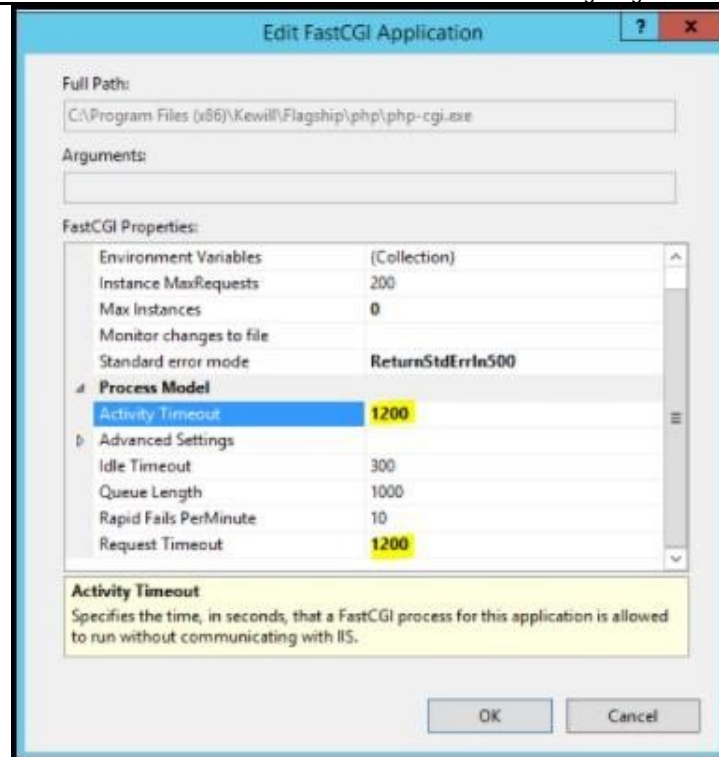
- b. Click Request Restrictions..., and then configure the mapping to invoke Handler _+only if the request is mapped to a '{ }File or a folder'{ }._+



- c. Click OK to save this configuration.
- d. To create a FastCGI application, on the Add Module Mapping Pop-up dialog, click Yes.
- Add the Fast CGI settings, as shown in the following screen.
 - a. Open the Fast CGI Settings dialog:



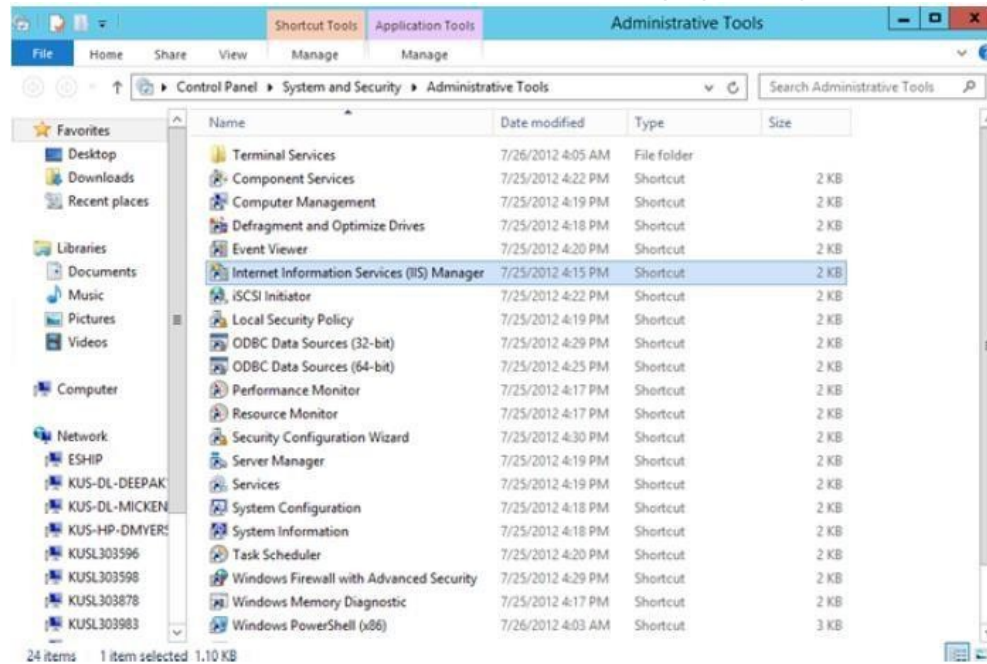
On the Edit FastCGI Application dialog, configure the following settings, and then click OK to save the FastCGI configuration:



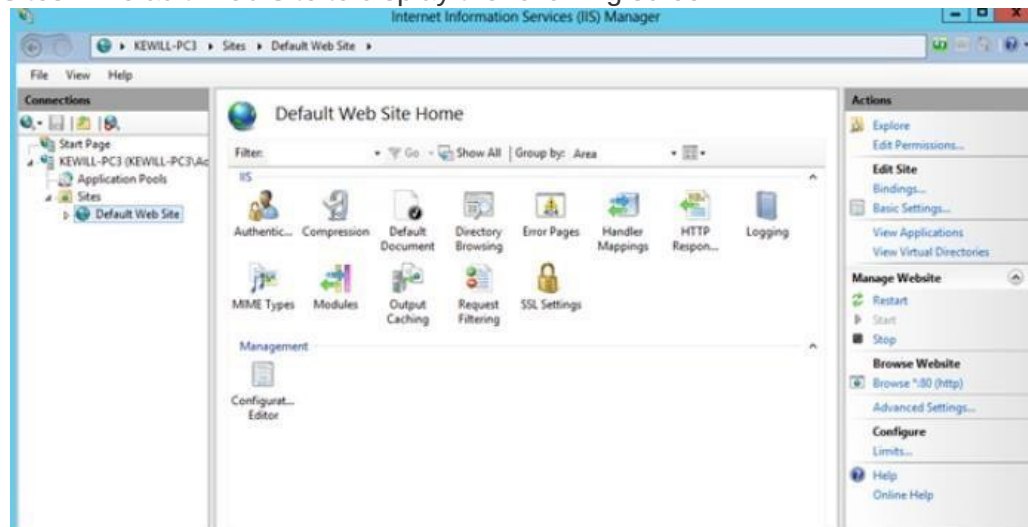
Configuring Bindings

To configure bindings:

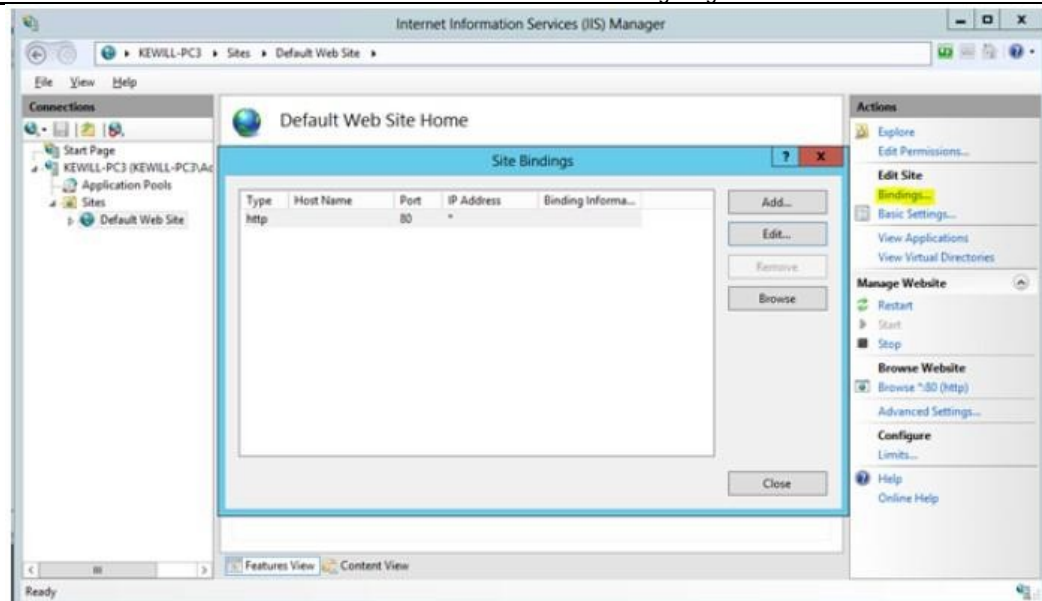
1. From the Start menu, select Control Panel > System and Security > Administrative Tools-Internet Information Services (IIS) Manager:



2. Double-click the IIS Manager listing as shown in the previous screen to display the IIS Manager, and then, on the IIS manager, select <Your_Server_Name> < Sites > Default Web Site to display the following screen:

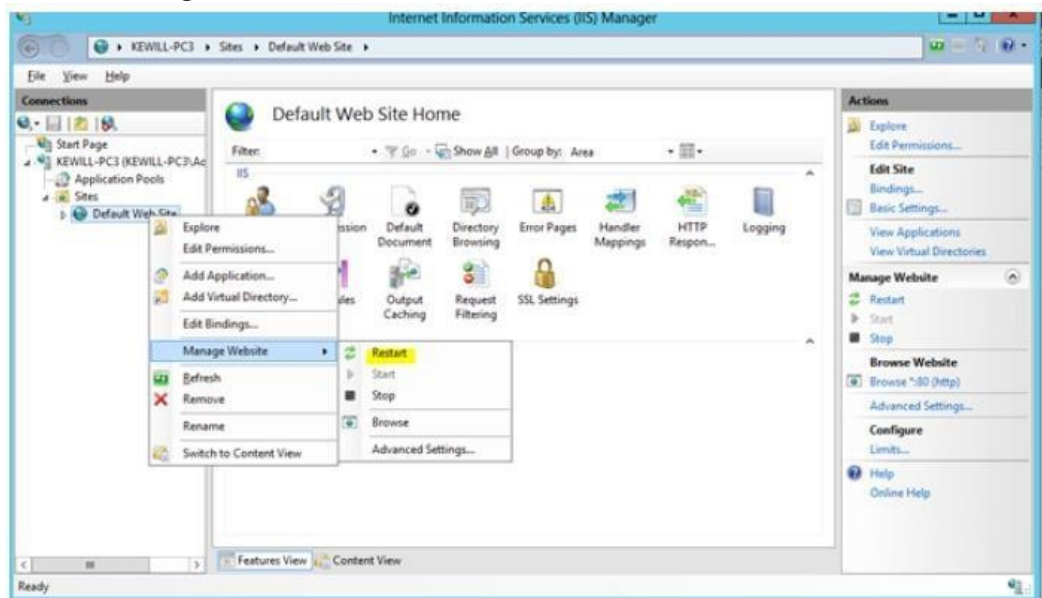


3. In the Actions panel, select Edit Site > Bindings to display the Site Bindings Popup dialog:



Optionally, change the port number if you want to operate the Parcel Web site from a port other than 80; otherwise, click Close.

4. Save the configuration and restart the Web site:



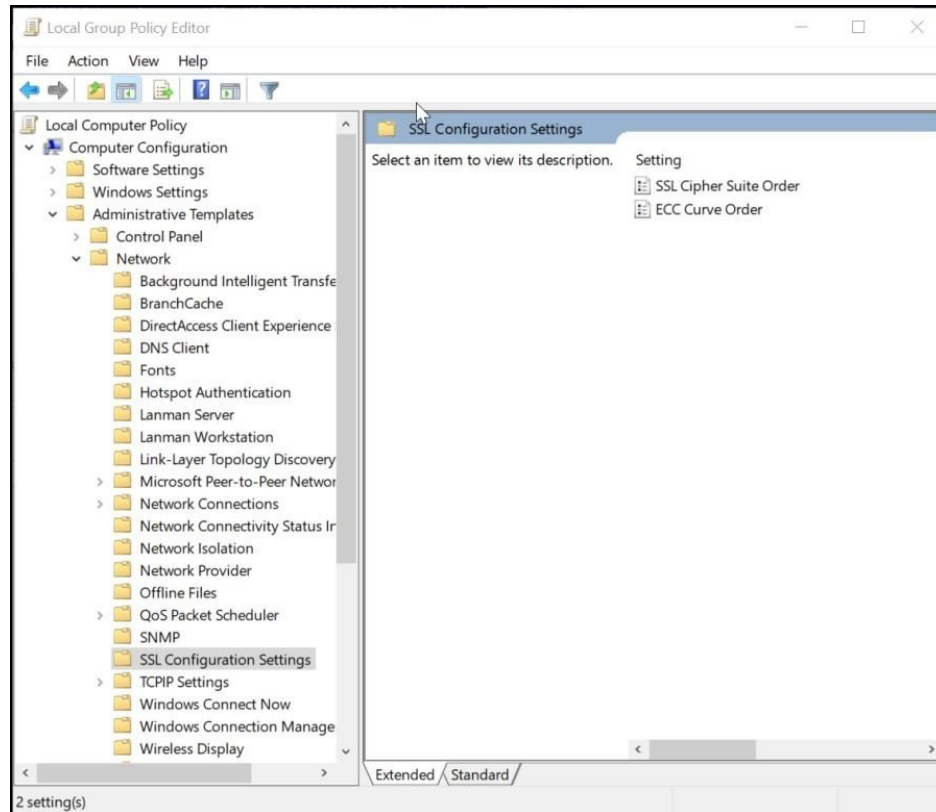
5. Test your Parcel/IIS10/PHP installation and configuration by opening Parcel application using the following URL on the server where Parcel is installed:
<https://localhost/login/login.php>

Note: The above instructions are same for Windows Server 2012 with IIS 8.0

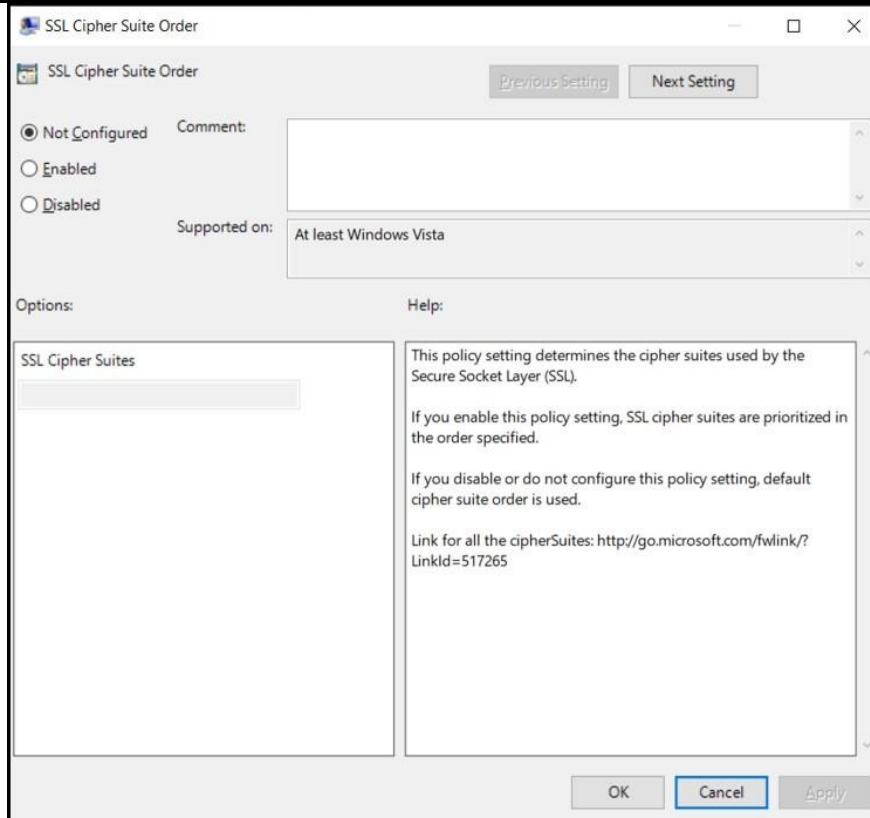
Disabling Weak SSL Cipher Suites in IIS

The user needs to disable weak SSL cipher suites in IIS for security purpose. This section describes about how to disable the weak SSL cipher suites in IIS. To disable Weak SSL Cipher Suites in IIS, follow these steps:

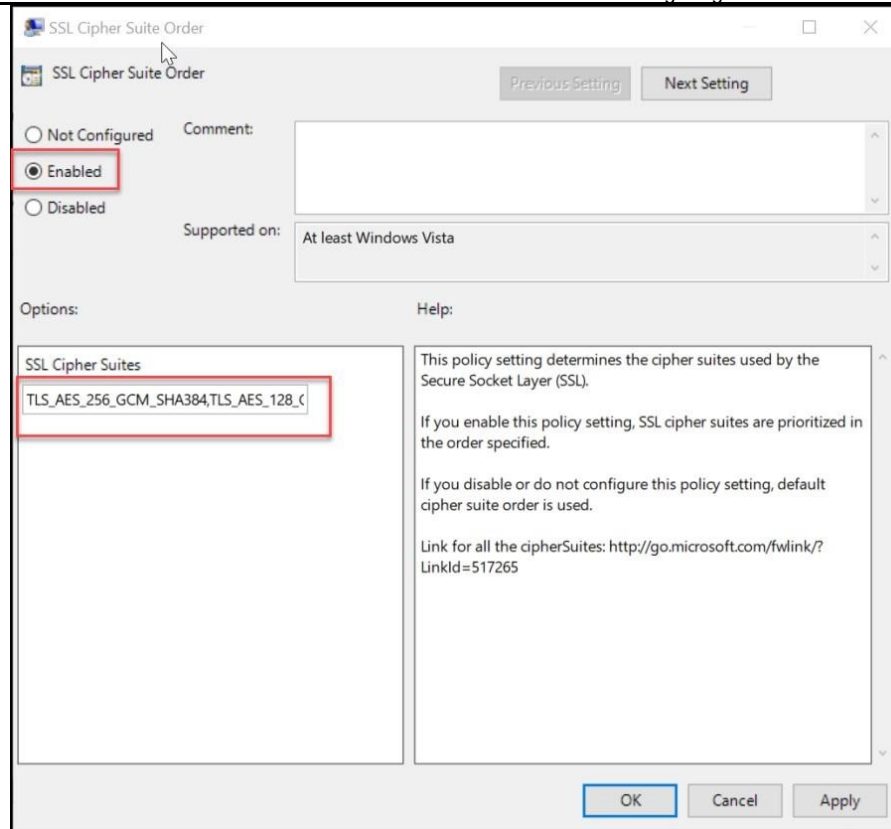
1. Open the Local Group Policy Editor (Start > Run > gpedit.msc).
2. On the left hand side, expand Computer Configuration, Administrative Templates, Network, and then click on SSL Configuration Settings, as shown in following screen.



3. On the right hand side, double click on SSL Cipher Suite Order. The SSL Cipher Suite Order screen displays, as shown in the following screen.



4. By default, the "Not Configured" option is selected. Click "Enabled" option to edit your Server's Cipher Suites.



The 'SSL Cipher Suites' field is filled with text once you click on the "Enabled" option.

5. Replace the existing text with the below text and click OK.


```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_GCM_SHA384,TLS_RSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_WITH_AES_256_CCM_8,TLS_RSA_WITH_AES_256_CCM,TLS_RSA_WITH_AES_128_CCM_8,TLS_RSA_WITH_AES_128_CCM,TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
```
6. Restart the Server Machine.

Disabling Weak SSL Protocol in IIS

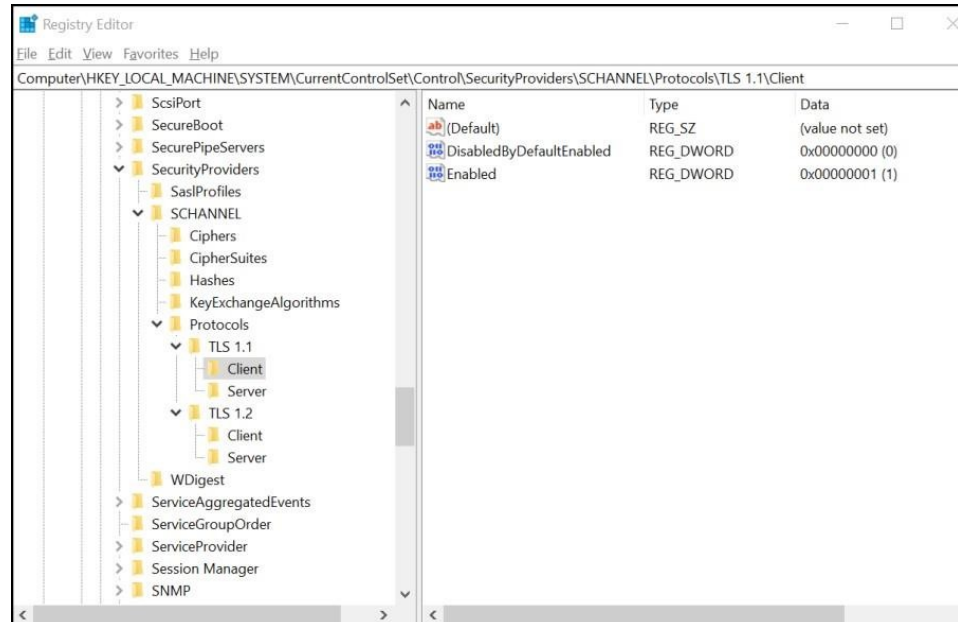
The user needs to disable weak SSL protocol in IIS for security purpose.

This section describes about how to disable the weak SSL protocol in IIS. To disable Weak SSL Protocol in IIS, follow these steps:

1. Open the Registry Editor (Start > Run > regedit).
2. Create the new keys called "TLS 1.1" (Protocols > New > Key TLS 1.1) and "TLS 1.2" (Protocols > New > Key TLS 1.2)
3. Right-click the "TLS 1.1" and "TLS 1.2" Keys and create subkeys:
 - the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProvider

s\SCHANNEL\Protocols directory:"Client"
"Server"

- Right-click the "Client" and "Server" subkey and create a new DWORD (32-bit) Value called 'DisabledByDefaultEnabled'. (New > DWORD (32bit) Value > DisabledByDefaultEnabled).
- Leave the default value as '0'.
- Right-click the "Client" and "Server" subkey and create a new DWORD (32-bit) Value called 'Enabled'. (New > DWORD (32-bit) Value > Enabled).
- Leave the default value as '1'.



- Close the Registry Editor.
- Restart the Server Machine.

Additional Setup Tasks

Configuring a Connector/ODBC DSN for 32-bit Windows

Before you can connect to a MySQL database on a separate server from the Parcel DIServer using the MySQL Connector/ODBC driver, you must configure an ODBC Data Source Name (DSN). The DSN applies a name to the various configuration parameters required to communicate with a database. Then you can use the DSN to communicate with the database without having to specify individual parameters.

For Parcel, you need to add a System DSN. A System DSN is a global DSN that is available to any user and application on the system. To create a System DSN, you need Administrative privileges.

To add a System DSN using the MySQL ODBC 5.1.6 driver, follow these steps:

1. Open the ODBC Data Source Administrator, and then click the Start menu and select Administrative Tools > Data Sources (ODBC).
2. Select the **System DSN** tab, and then select the Data Source Name from the System Data Sources list.
3. Click Configure.. to display the Connector/ODBC Data Source Configuration dialog.
4. In the Connector/ODBC dialog box, complete the fields as follows, test the connection to each database (see step 5), and then click OK.

In this field...	Do this...
Data Source Name	The System Data Source name that you selected in step 3 is automatically displayed in this field.
Description	Type MySQL ODBC 5.1 Driver DSN
TCP/IP Server	Type the Host Server name or static IP address
Port	Type the port number used in configuring MySQL. Note: Port sets the TCP/IP port number to use when communicating with MySQL. Communication with MySQL uses port 3306 by default. If you configured MySQL server to use a different TCP/IP port, (Step 8 in the Installing the MySQL Server topic) you must type that port number in the Port field.
User	Type sn_usr
Password	Type shipnowdb
Database	To test connections (step 5), select the appropriate database from the drop-down list: <ul style="list-style-type: none"> • didb • sordb • idatadb]

Note: As long as all three databases belong to the same (MySQL) data source, you only need to complete this configuration once.

5. In the Connector/ODBC dialog, after you select each database, click Test to test the connectivity to that database.

Editing the php.ini File

Depending on your configuration, you need to edit the php.ini file in the WINDOWS folder as follows:

- For all installations, the setting to allow include/require to open URLs (like https:// or ftp://) as files – See the following procedure.
- For Microsoft SQL server – See the following subsection: **Editing the php.ini file**

Note: You can also edit the php.ini file to set the timeout period in Parcel. See the section "Resetting the Login Timeout." **To edit the php.file to treat URLs as files**

1. In the WINDOWS folder, open the php.ini file, and then find the section headed Fopen Wrappers.
2. Ensure that the following setting is in effect: allow_url_include = on

```
.....  
; Fopen wrappers ;  
.....  
  
; Whether to allow the treatment of URLs (like http:// or ftp://) as files.  
allow_url_fopen = On  
  
; Whether to allow include/require to open URLs (like http:// or ftp://) as files.  
allow_url_include = on
```

3. Save and close the php.ini file.

Resetting the Login Timeout

If you are experiencing frequent Parcel timeouts due to user inactivity that require the user to log in again, you can reset the timeout period in the php.ini file to make it longer.

To reset the timeout period:

1. Open the php.ini file in a text editing program such as Notepad.
2. Select the Find function and enter the following text string to find the parameter setting: session.gc_maxlifetime.
3. The value of this parameter is set to 1440 by default. This setting produces a timeout period of 1440 seconds or 24 minutes. Set this parameter to a new, higher value as desired for the number of seconds until a timeout is generated.
4. Save and close the php.ini file.

Configuring Parcel with UTF-8 Support

Parcel supports the UTF-8 character set. UTF-8 is a variable-width encoding that can represent every character in the Unicode character set. To facilitate localization, Parcel includes UTF-8 by default. This requires modifications to the following files and database tables: Settings table in the didb database for a Microsoft SQL Server sordb and idatadb

Notes:

- Even though UTF-8 support is installed with Parcel by default, you need to configure Parcel for UTF-8 using the Web Admin tool (recommended) or modifying settings in the didb.settings table directly. See the following section: "Modifying database settings." Modifications for Microsoft SQL Server are required whether or not you plan to use UTF-8. If you want to use UTF-8 with Parcel, you also need to configure an additional database setting.
- For Oracle SOR and IDATA databases, configuration for UTF-8 is automatic.

Modifying SOR and IDATA database settings for UTF-8

You must modify the settings for the Microsoft Sequel Server SOR and IDATA databases for UTF-8 in the MySQL didb.settings table using one of the following methods:

- With a database administration tool such as SQLyog, edit the didb.settings table directly with the required sordb and idatadb url key_name values.
- Using the Parcel Web Admin tool, navigate to the Global Settings > Settings screen (essentially a view on the didb.settings table) and make the required changes. For information on editing this table in Parcel, see the following topic in the Parcel Online Help: Parcel Configuration (Web Admin) Tool > Global Settings > Settings.

Note: The following procedures are independent of the particular method you use to modify the SOR and IDATA databases. **Bold text** indicated the string that you need to append to the existing key value.

Microsoft SQL Server SOR and IDATA settings for UTF-8

To configure the Microsoft SQL Server SOR and IDATA database setting for UTF-8

1. In the SOR database entry below for the url key name, enter the following string for Key Value: `jdbc:sqlserver://Machine_Name;databaseName=sordb`

Database Column	Database Record
Machine Name	ALL
Domain	dbcs-connection
Sub Domain	sordb
Key Name	url
Key Value	<code>jdbc:sqlserver://localhost:1433;databaseName=sordb</code>
Display Name	Connection URL used to connect to sordb via Database Service

2. In the IDATA database entry below for the url key name, enter the following string for Key Value:

`jdbc:sqlserver://Machine_Name;databaseName=idatadb`

Database Column	Database Record
Machine Name	ALL
Domain	dbcs-connection
Sub Domain	idatadb
Key Name	url

Key Value	jdbc:sqlserver://localhost:1433;databaseName=idatadb
Database Column	Database Record
Display Name	Connection URL used to connect to sordb via Database Service

Troubleshooting

Overview - Troubleshooting

If any errors occur during the installation, they appear in a Pop-up and also in the log file. The log file is located in the root of the folder where you installed Parcel (usually <Parcel Install Folder>\Flagship) and has the following form:

BJ232Install_<yyyymmddhh_mm_ss>.log;

For Example: BJ232Install_20243052408_35_58.log

"Problems that need to be resolved" Screen

If the "Problems that need to be resolved" screen appears, it means that the installation could not be completed. Read the detailed information in the screen.

If you decide that you need to re-install Parcel, you must first uninstall Parcel. See the section **Uninstalling Parcel** for instructions.

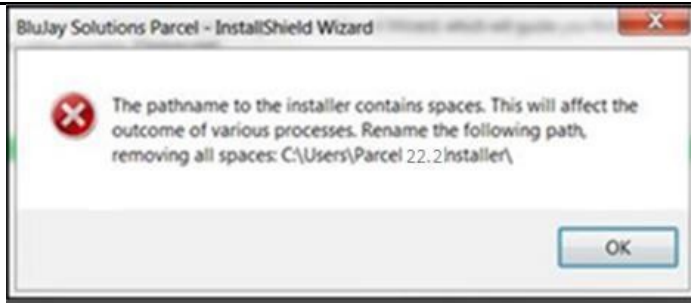
Common Problems, Causes, and Solutions

The following table lists some common problems that you may encounter during installation:

Common Problem	Cause/Suggestion for Resolution
On opening the Parcel Installation Wizard, a message is displayed indicating that the pathname of the installer contains spaces (see illustration below).	You should not receive this message if you install directly from the Parcel CD. However, if you first copy the installation folder to a local drive on the machine where you are installing Parcel, you need to ensure that the pathname to this folder does not contain spaces.
Any error occurs during installation.	Errors are displayed in Pop-up windows and also in the log file. (See above for information on this file.) Consult these sources for additional information on the source of the error.
The "Problems that need to be resolved" screen is displayed at the conclusion of the installation process.	The installation could not be completed. Read the detailed information on the screen. The following rows describe some of the more common errors.
The "Problems that need to be resolved" screen displays the following message: "The MySQL MyODBC Connector was installed and will need configuration."	You need to configure the ODBC Connector for MySQL on the server. Follow the instructions in the following section: Configuring a Connector/ODBC DSN for 32-bit Windows

Error message re spaces in the installation path

The following error message is displayed at the start of the installation process if there are spaces in the path to the setup.exe program:



See the previous table for how to resolve this error.

Database connection error with port blocking

When using Parcel, if you have port blocking activated you may receive the following MySQL error (or a similar database connection error) in the log file:

```
RateEngine.cpp;CRateEngine::CRateEngine;INFO;Error connecting to  
database::DB Connection was timed out. Will be tried once again when user  
calls CONNECT
```

For information on correcting this error by using an alternative to port blocking, see the following section: [**Database Errors with Port Blocking**](#)

Database Errors with Port Blocking

The Problem with Port Blocking

Several network security providers include port blocking functionality as a defense against malware and other destructive programs. This functionality accomplishes this by blocking ports that malicious programs can open to listen for or poll for commands in order to use the machine as a bot or vector for spam. This port blocking technique usually works by allocating ports in the Windows registry in a way that prevents the use of certain ports for external traffic to and from the machine.

This type of port blocking can adversely affect the operation of Parcel and MySQL for the following reason. Each of these applications employs a strategy of listening for connections on a common port, and then shunting each connection to a different, randomly-selected port in order to listen for the next connection. (This same strategy is employed by virtually every multithreaded program that handles multiple TCP/IP connections.) With port blocking enabled, Parcel or MySQL may randomly allocate a port within the blocked range, and then move a connection to the blocked port. However, the blocked port prevents any traffic in either direction.

If this scenario involves an interaction between an API client and Parcel, it deceptively appears that Parcel has the connection open but is ignoring data flow through this connection. In the `di_debug` log, this circumstance typically shows as a successful initial connection with no additional traffic.

If this scenario involves an interaction between Parcel and MySQL, MySQL returns the following error message in the `di_debug` log:

```
RateEngine.cpp;CRateEngine::CRateEngine;INFO;Error connecting to  
database::DB Connection was timed out. Will be tried once again when user calls  
CONNECT
```

Note: Since the connection itself does not actually fail, this message is only a warning in Parcel rather than a fatal error, although subsequent database queries may result in "no data found" errors. This error is intermittent, since not every port allocated by MySQL will be in the blocked range; most transactions should still go through. Additionally, since the

above error message can also occur when MySQL encounters other types of connection problems, it may not necessarily result from port blocking.

Workaround

You should disable port blocking permanently on any machine operating in conjunction with the Parcel system, including after-market port blocking (which allows the ports to be opened and then blocks traffic without notifying the application).

As an alternative security measure to port blocking, BluJay Solutions recommends the use of Windows IPsec functionality. For more information on IPsec, see the following Microsoft Web page: <http://support.microsoft.com/kb/813878>

DB Upgrade Problems with configuration.xml File

When performing an upgrade on an existing Parcel system, the process may freeze during the database upgrade stage if you have edited or deleted and recreated the following Java configuration file:

<Parcel Artifact Folder>\Flagship\java\conf\configuration.xml

If, for some reason, this file becomes corrupted or, for any reason, you need to edit or delete and recreate this file, please carry out the following steps:

1. Open the Windows Component Services window: Start > Administrative Tools > Component Services > Services (Local).
2. Stop the following services: Kewill DiServer Service
KewillFlagshipDatabaseFileService
3. Before editing or deleting the configuration.xml file, make a copy of the existing file and forward it to BluJay Solutions Customer Support. (If possible, wait for analysis and advice from Customer Support before taking further steps.)
4. After editing the configuration.xml file or creating a new one and adding it to the *..\\Program Files\\Kewill\\Flagship\\java* folder, restart the following service: KewillFlagshipDatabaseFileService
5. This required step re-initializes the configuration.xml file with the correct paths.
6. Copy the flagshipProperties.xml file from the <Parcel Artifact Folder>\Flagship\DBUpdate\XML folder to the ..\\Program Files\\Kewill\\Flagship\\Java\\tmp\\dbin folder and wait for it to be deleted automatically by the service after it has been processed.
7. Restart the following service: Kewill DiServer Service

Log File Rollover Problems

Changes were introduced in the Parcel logging process to ensure that the di_debug.log file is correctly backed up after rolling over when the maximum file size is reached, and a backup copy of the old log file is made when the new log file is created. With the new logging changes, interprocess locking was introduced to ensure correct log rotation. However, if for some reason log rotation is not working, then you need to carry out the following steps:

1. Manually stop all Flagship services.
2. Delete all files in the Flagship/loglocks directory, or else delete the directory itself.

3. Manually restart all Flagship services.

The log rollover process should now function correctly.

Services Starting Problems

After Parcel installation is completed and machine is restarted, Windows may take some time to reconnect to different network drives. So, when either network/mapped drive is set as Parcel Artifact folder and if windows try to start Kewill services before network drive is up, it might fail.

In few cases, if network drive is too slow and failed to start any of Kewill Services, then users have to Manually restart all Kewill/BluJay/Apache services.

Uninstalling Parcel

If you receive an error at the end of the installation program and you want to try reinstalling Parcel using the installation program, you must first uninstall Parcel. You can uninstall Parcel and any of the third-party programs installed by the installation program (Apache Web Server, MySQL). **To uninstall Parcel, follow these steps:**

1. Open the Control Panel > Administrative Tools > Services window. You can access the Control Panel by clicking the Start in the lower-left corner of your screen.
2. In the Services window, the Flagship services are named beginning with the word "Kewill". If you have trouble locating the services listed below, contact BluJay Solutions Technical Support.
To stop services, double-click the service and click the Stop in the dialog box that appears. These are the services you will need to stop: Apache 2.4MySQL - you must stop this service even if you are not uninstalling MySQL. All Kewill ServicesStunnel SSL Wrapper
3. Navigate to the Add/Remove Programs screen from the Control Panel.
4. In the Add/Remove Programs list, select *BluJay Solutions Parcel{*}, and then click Remove. Windows uninstalls Parcel. However, the third-party programs installed by the installation program (such as Web Server and MySQL) are not uninstalled. Optionally, to uninstall these programs, select them in the following order in the Add/Remove Programs list, and then click Remove:
a. MySQL Connector/ODBC
MySQL Server
5. If you uninstalled MySQL, delete the MySQL directory where it was installed. By default, this is C:\Program Files\MySQL.
6. To remove Apache, delete the Apache Group directory. By default, this is C:\Program Files\Apache Group.
7. If you uninstalled MySQL, search the C:\WINDOWS\System and C:\WINDOWS\System32 directories for .dll and .exe files related to MyODBC and MySQL. Delete them.
8. Rename the C:\Program Files\Kewill\Flagship directory if you want to save existing log files.

9. Open the Windows Registry Editor<ac:structured-macro ac:name="anchor" ac:schema-version="1" ac:macro-id="47c8d416-6b2d-47a9-8a80-80e38ab8beae"><ac:parameter ac:name="">_Hlk33801290</ac:parameter></ac:structured-macro> (Navigate to Start > Run, type regedit in the Open field, and then click OK).

Warning: Be very careful editing the Registry. Before you edit the Registry, you should create a backup of it. If you have Windows XP, you can do this by creating a restore point using System Restore (Start > All Programs > Accessories > System Tools > System Restore). For other Windows operating systems, your system administrator will need to create an image of the system.

1. In the left pane of the Windows Registry Editor, expand HKEY_LOCAL_MACHINE > System > CurrentControlSet > Services.
2. Delete the following keys:DI_Server_svcJTrackKewill TSN Communication ServiceMySQL (delete only if you uninstalled MySQL!)Notification ServiceSchedulerSvcStunnel SSL Wrapper
3. Look for the keys listed in Step 11 in any ControlSet00n folders (where *n* is a digit). The ControlSet00n folders would appear on the same level as the CurrentControlSet folder. If the keys are found in any ControlSet00n folder, delete them just as you did in Step 11.
4. Close the Registry Editor.
5. Restart your computer.

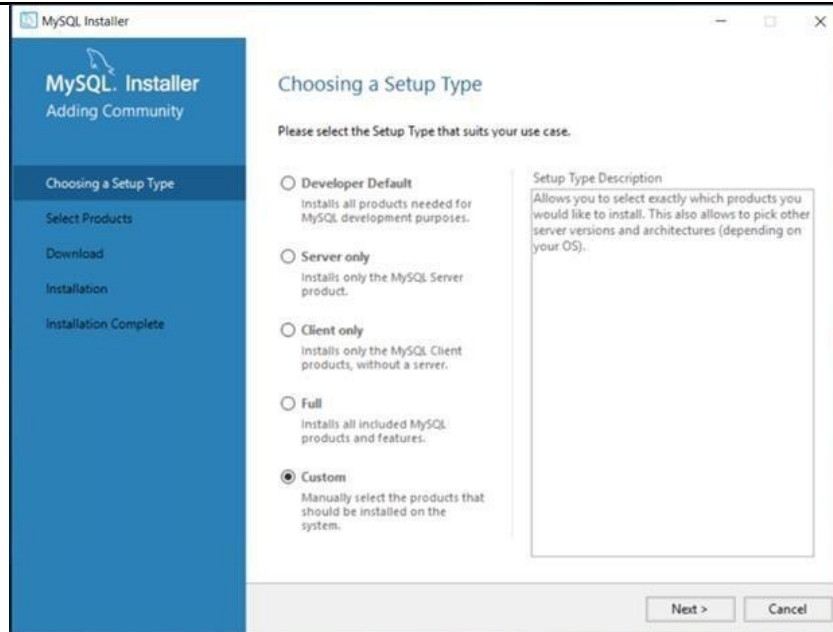
Printing Reports

Note: On the Reports page, when you select a postage statement and click Print, if Parcel returns the error *Report Server could not be started*, you need to start the Kewill Reporting Service manually. To do this, navigate to the Windows Control Panel > Administrative Tools > Services list (click the Start in the lower-left corner of your desktop to find the Control Panel). Locate the Kewill Reporting Service in the Services list. Right-click on it and select Start.

Installing MySQL on different drive

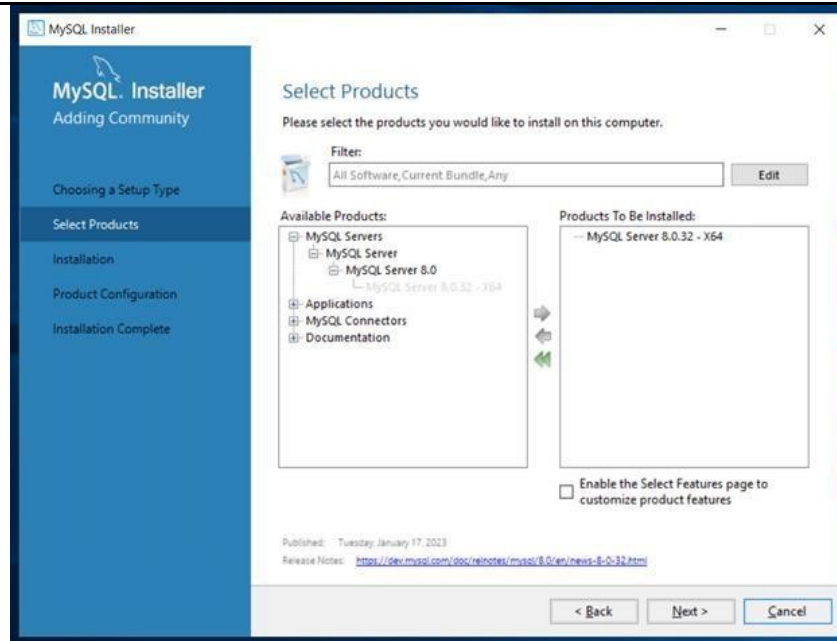
To install MySQL on different drive, please follow these steps: **Note:** The newer version of MySQL Server is 8.0.32.

1. In the Setup Type screen, select the **Custom** option and then click Next.



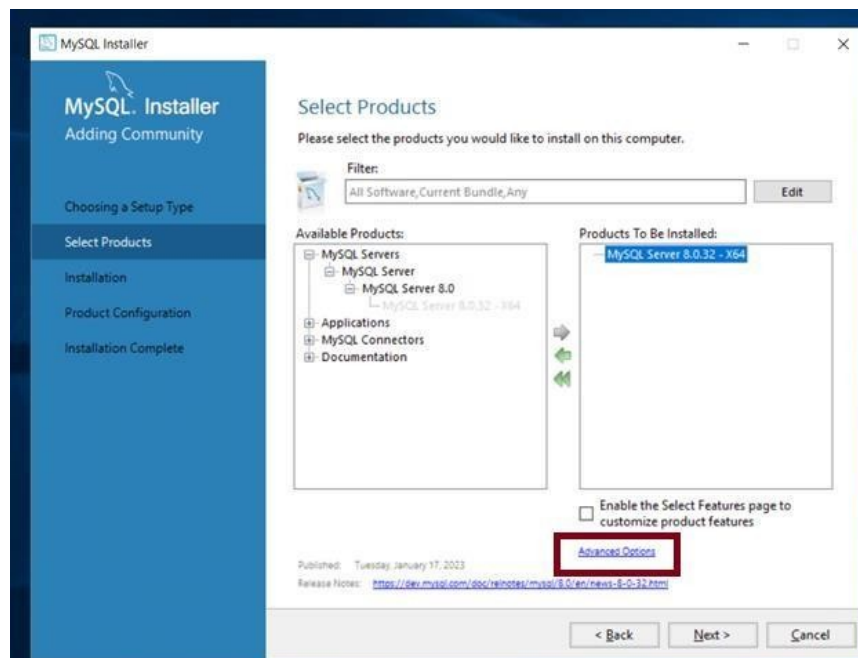
Setup Type	Description
Developer Default	Select this option to install all products needed for MySQL application development.
Server only	Select this option to install only the MySQL Server product.
Client only	Select this option to install the MySQL Client products, without a server.
Full	Select this option to install all including MySQL products and features.
Custom	Select this option to manually select the products that you want to install in different drive or system.

- On the MySQL Installer screen, under move MySQL Server 8.0.32-x64 from Available Products to Products to be Installed.



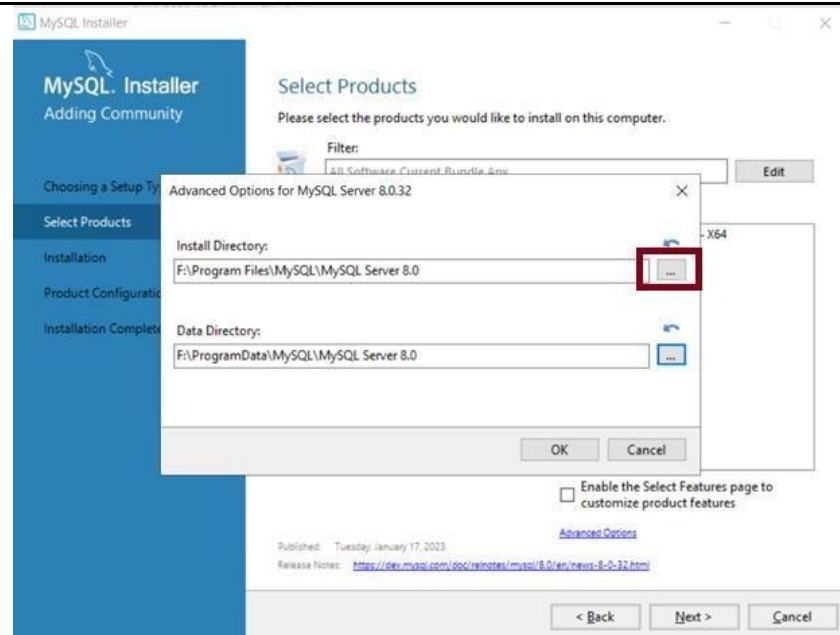
Note that **MySQL Server 8.0.32** now moves to the right side of the section.

3. Click Next.
4. On the MySQL Installer, click Advanced Options.

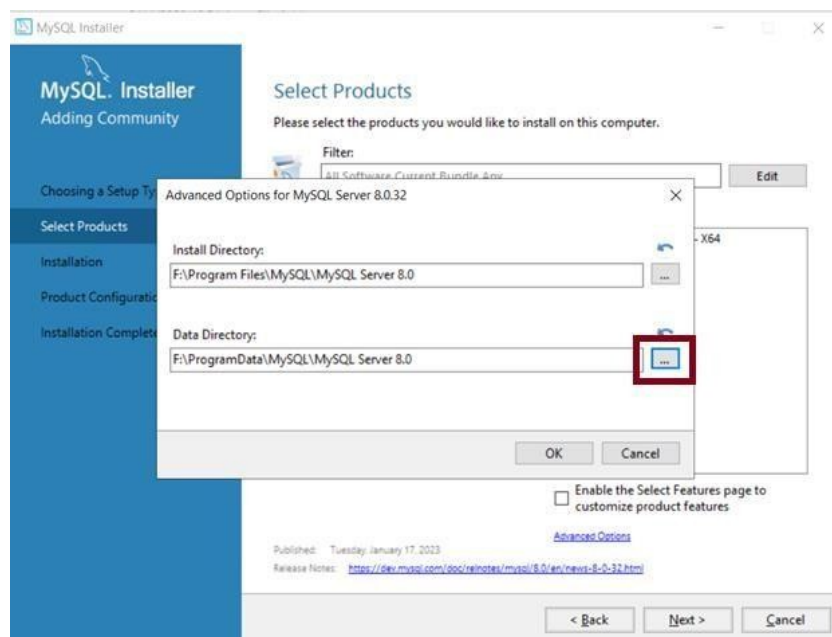


The Advanced Options for MySQL Server 8.0.32 window box appears.

5. In the Advanced Options for MySQL Server 8.0.32 window, click ... and browse to the respective folder, where you want to install MySQL and then click OK.

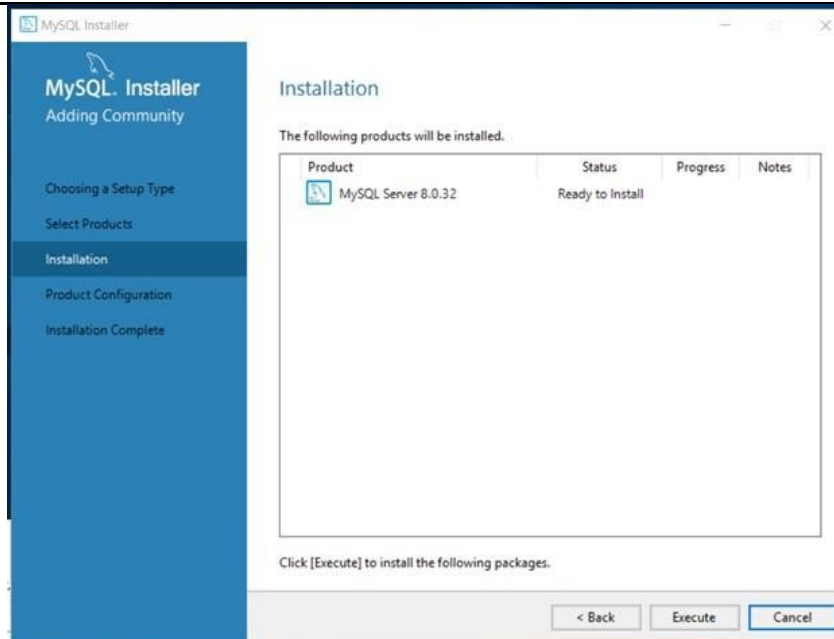


6. In the Advanced Options for MySQL Server 8.0.32 window, click ... and browse to the respective folder, where you want to install data folder and then click OK.



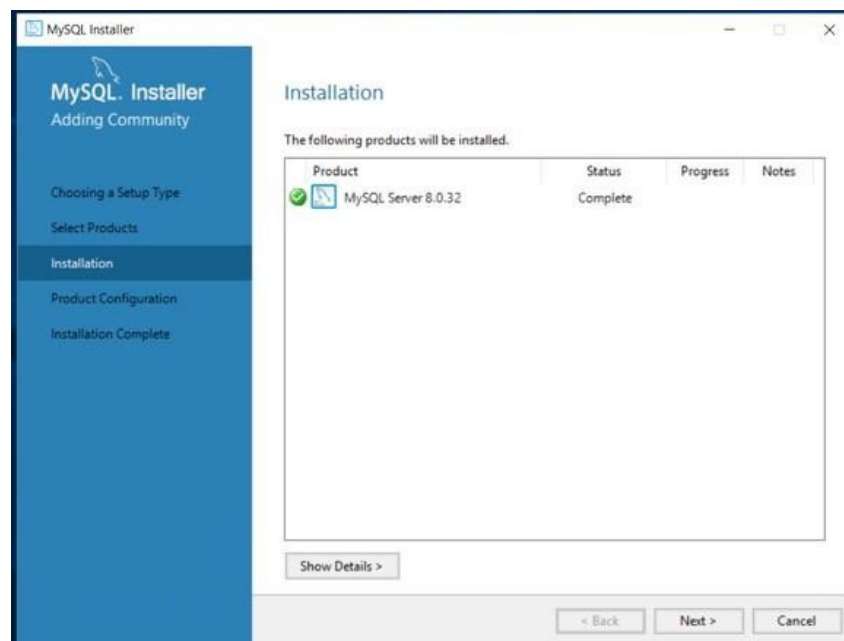
The Installation screen appears with the Ready to install status for MySQL Sever 8.0.32.

7. In the Installation screen click Execute.

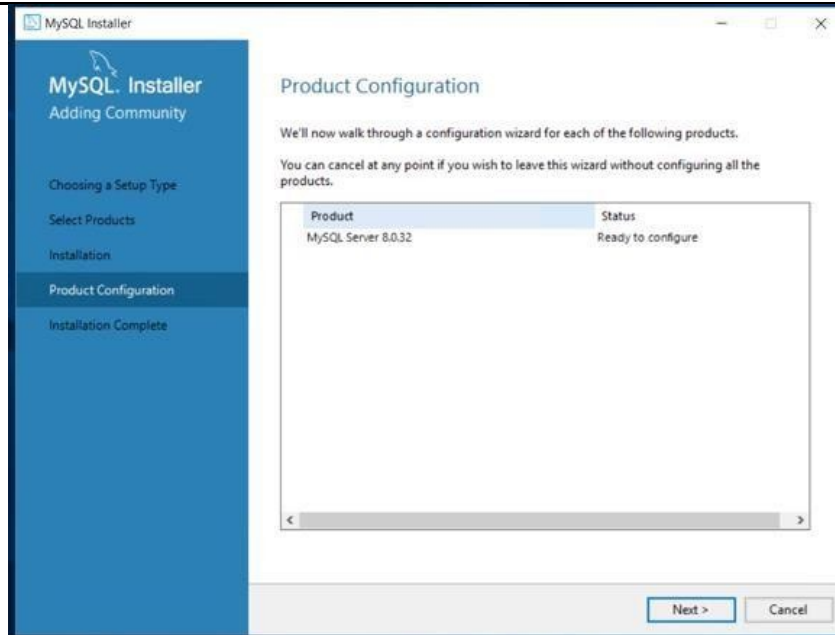


After few seconds, the MySQL Installation gets completed.

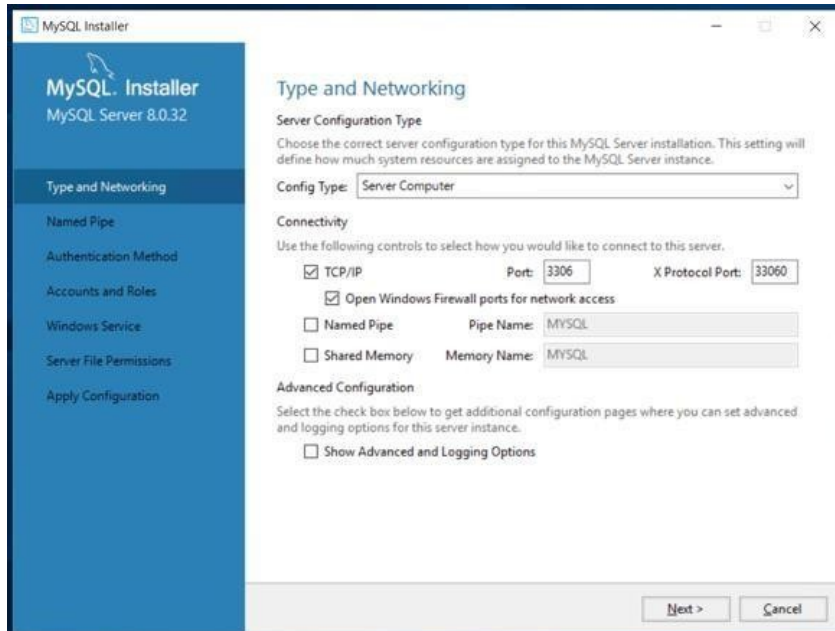
8. In the Installation screen, click Next to continue with the Product configuration.



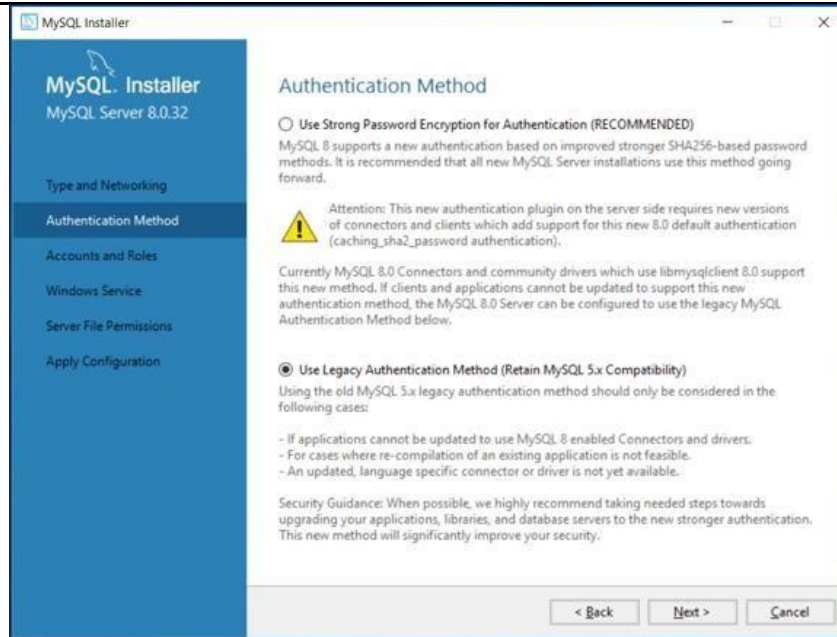
9. On the Product Configuration screen, click Next.



10. On the High Availability screen accept the default selection of the "Standalone MySQL Server / Classic MySQL Replication" and then click Next.
11. On the Type and Networking screen, select "Server Computer" from the "Config Type" drop-down and leave the default settings in "Connectivity" and "Advanced Configuration" section and then click Next.



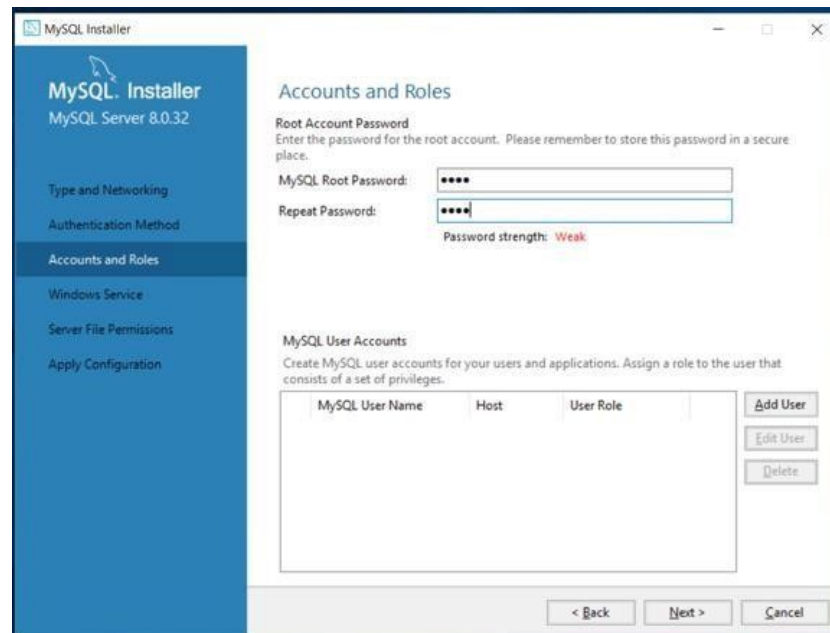
12. On the Authentication Method screen, select Use Legacy Authentication Method and click Next.



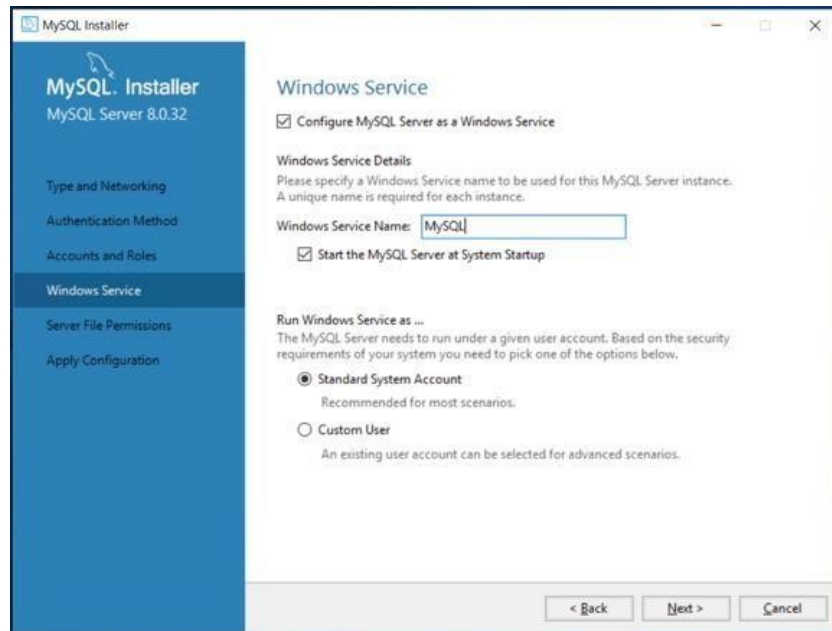
13. On the Accounts and Roles screen type "root" (all lowercase letters without quotation marks) in the "MySQL Root Password" and "Repeat Password" fields, and then click Next, as shown in following illustration:

You must type this specific password, since Parcel uses this as the root account password as required by the Parcel Configuration (Web Admin) Tool. The root account has all privileges in the MySQL database.

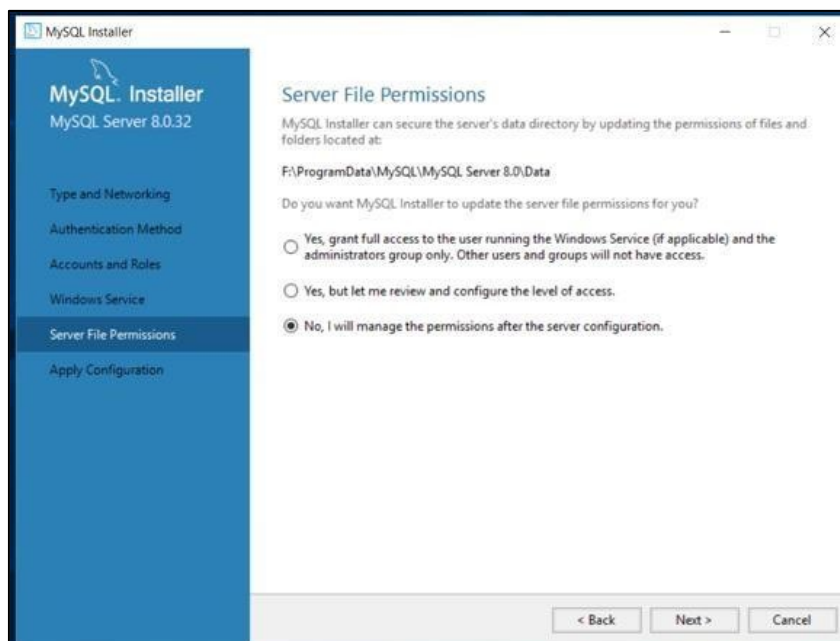
Note: It is important to create a root account password. Any user logged in from a valid hostname can access MySQL and make alterations to the database using the root account.



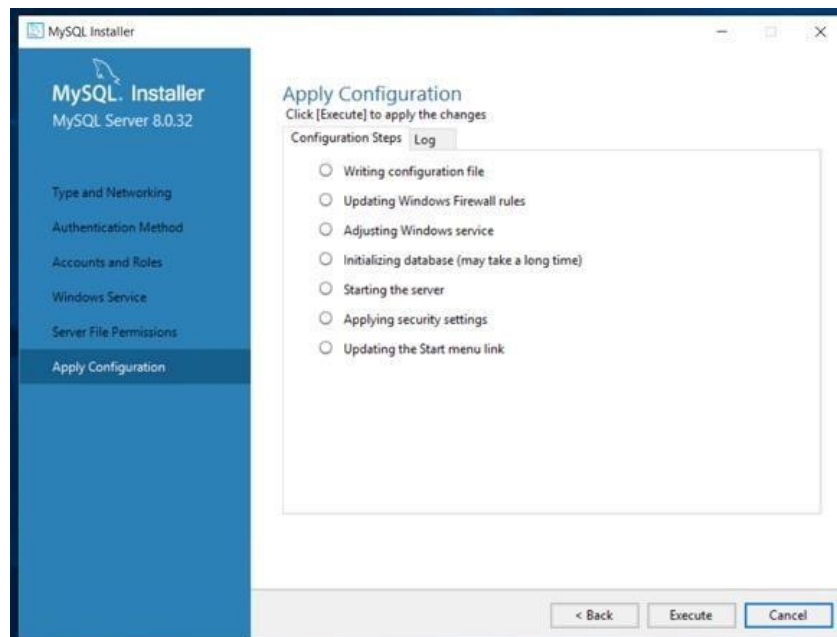
14. On the Windows Service screen change the window service to **MySQL** in Windows Service Name field and leave the default settings as it is in the screen and then click Next.



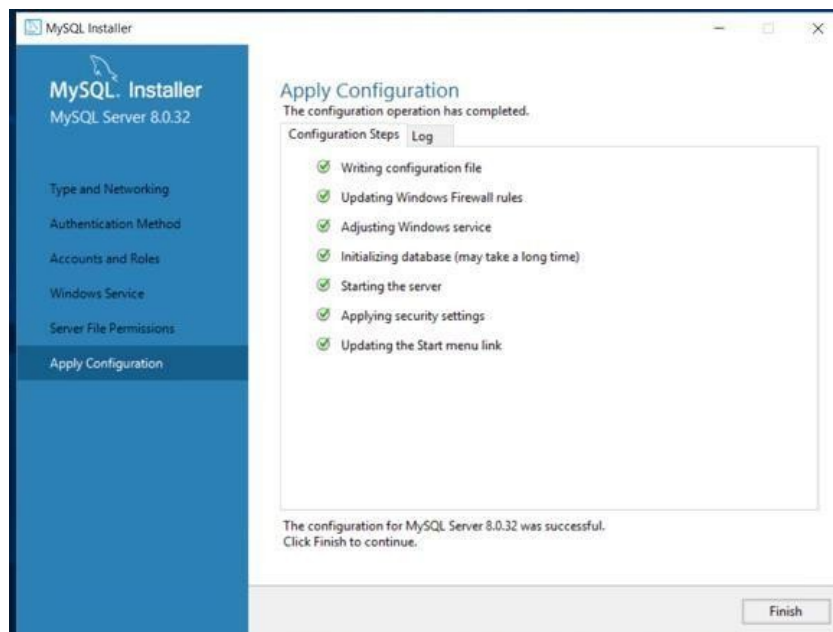
15. On the Server File Permissions screen, select **No, I will manage the permissions after the server configuration** option and click Next.



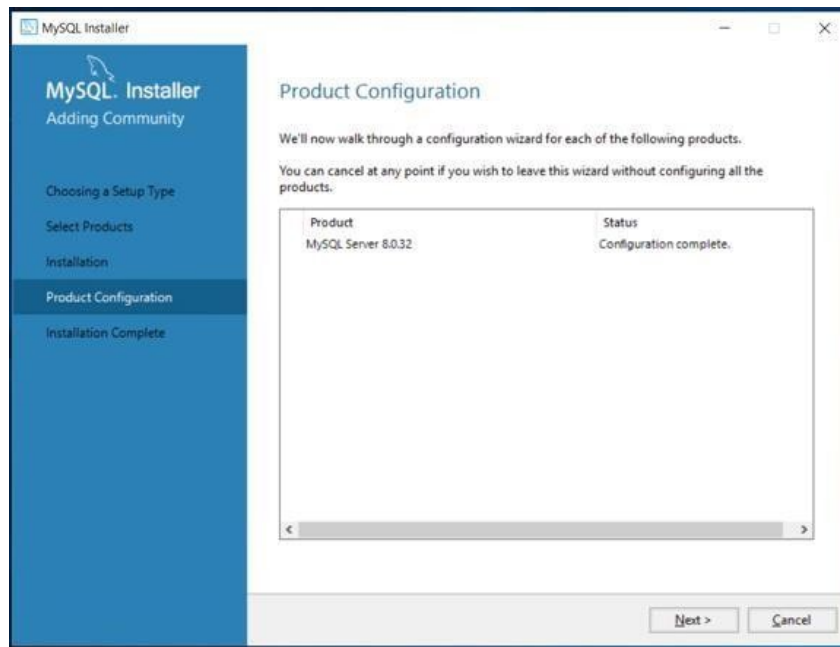
16. On the Apply Configuration screen, select the desired configuration settings and click Execute to enable your configuration settings.



17. On the Apply Configuration screen, click Finish.

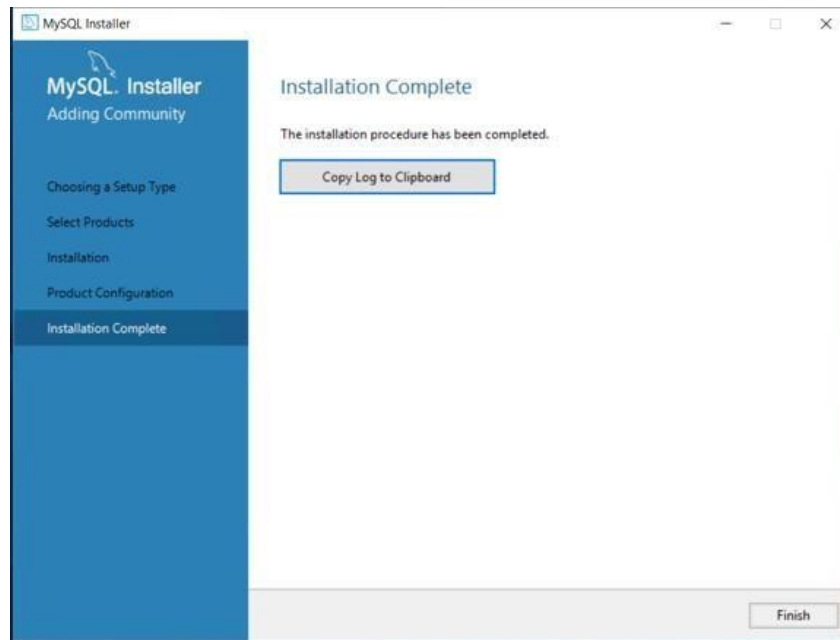


18. On the Product Configuration screen, click Next.



19.

On the Installation Complete screen, click Finish to complete with the MySQL installation.



The system now continues with installing MySQL Connector/ODBC. Refer [Installing the MySQL Connector/ODBC](#) for details.

Glossary

Term	Definition
Stunnel	Stunnel is an open-source multi-platform application used to provide a universal TLS/SSL tunneling service.
Web Server	It is used to host and provide Internet-based services that delivers web content through internet. Parcel supports both Apache and IIS.
Windows Services	Windows Services are a core component of the Microsoft Windows operating system and enable the creation and management of long-running processes.
OpenSSL	An OpenSSL (Open Secure Sockets Layer) is open-source version of the SSL and TLS security protocols, which provide encryption and server authentication over the Internet.
Oracle Wallet	An Oracle Wallet is a password-protected container used to store authentication and signing credentials including private keys, certificates and trusted credentials needed by SSL.
ORAPKI command line	The ORAPKI tool is available with Oracle database, so this tool can be used only by those users have a license for Oracle database.