



TM-Parcel Upgrade 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

Overview of Parcel Upgrade Installation.....	6
Third Party Applications Required by Parcel	6
Note on Third Party Applications with Parcel	7
Checking Settings Before and After Upgrading	8
Backing Up Your Existing Data	8
Upgrading Parcel.....	9
Prerequisites for Upgrade Installation	9
Perform Upgrade Installation	10
Upgrading Parcel DB to 24.1.0 on Aurora Server	38
Upgrading Parcel DB to 24.1.0 on Remote Server.....	39
Connecting Remotely to Database.....	41
Converting Parcel from HTTPS to HTTP on Apache Server	48
Post Installation Tasks.....	49
Configuring 64bit DSN.....	49
Update Password to Bcrypt	50
Configuring HTTPS Certificate on Apache Server.....	50
Enabling HTTPS on IIS Server	52
Configuring HTTPS Certificate for UCM.....	55
Accessing the Parcel Application	55
Importing UPS World Wide Validation Data after the Upgrade	55
Add Update Virtual Directory in IIS	57
Moving Apache from one drive to other drive.....	61
Configuring Persistence XML File	61
dbdefines.php Changes.....	63
Reconfigure SSL Settings.....	63
Converting MyISAM to InnoDB	65
Add/Update KOL and CBRM URLs	65
Additional Optional Steps	66
Setting up a Corporate Address Book.....	66
Checking Settings	68

Supporting UCM Integration on HTTPS	69
Converting UCM from HTTPS to HTTP	69
Configuring Stunnel Settings for Encryption of Data in Motion	70
Encryption of Stored Data.....	72
Configure Encrypted Connections to Database	77
Change Log On user for all Kewill _ BluJay Services.....	111
Changing Parcel Artifact Folder Location.....	111
Supporting UMS and E2Proxy Integration	113
Disabling Weak SSL Cipher Suites in IIS.....	115
Disabling Weak SSL Protocol in IIS.....	118
Troubleshooting Upgrade Installation	118
Database Errors with Port Blocking	119
DB Upgrade Problems with configuration.xml File	120
Log File Rollover Problems.....	120
Services Starting Problems	121
Uninstalling Parcel.....	121
Printing Reports	122
Error Message related to powershell	123
Pending tasks during upgrade on an IIS environment.....	123

Overview of Parcel Upgrade Installation

Before upgrading the Parcel to 24.1.0, you must take a backup of your current Parcel system.

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 Server.
PHP	8.2.7	Required to view the Parcel user interface.
Windows Services	N/A	<p>These include services such as:</p> <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.

Checking Settings Before and After Upgrading

If you wish to retain settings from your previous Parcel installation, before upgrading you need to check the settings for your previous installation, and then after the upgrade, check to ensure that they still apply. To check Parcel settings, use SQLyog or another database management tool to display the contents of the didb.settings table in the MySQL database. For more information on checking settings (especially with reference to post-installation tasks), see the following section: Checking Settings

Backing Up Your Existing Data

Before upgrading to Parcel 24.1.0, strongly recommends that you back up your existing data, both your Parcel MySQL databases and any other customized databases that you may have created to interface with Parcel. This step also applies if you plan to upgrade MySQL and Apache. To back up your data, copy the MySQL folder (Program Files\MySQL) to another location, as well as any other data associated with Parcel. You also need to copy the Program Files\Flagship folder to another location.

Note

When upgrading your system, Parcel overwrites all files and database entries. Thus, if you have customized portions of your Parcel system, you may need to reapply your customization. For example, if you have customized the Parcel UI, label templates, or database tables and fields, you need to reapply these customizations when the upgrade has been completed. Perform your settings checks and this backup before upgrading MySQL and Apache.

Note

If you are upgrading TM-Parcel from a base version with database engine type as InnoDB, refer to [Converting MyISAM to InnoDB](#) section.

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.

Upgrading Parcel

This section provides information on upgrading Parcel to 24.1.0.

Note

The Parcel installation program supports upgrades from Parcel 22.1.0, 23.1.0, 23.2.0, 23.3.0 and 23.4.0

Prerequisites for Upgrade Installation

Note

These Prerequisites are applicable only if you are upgrading to TM-Parcel 24.1.0 from a previous version of TM Parcel in which MySQL Secure Connection has been enabled.

1. Backup your **shipnow.ini** and **my.ini** files from the corresponding folders.
2. Turn off the DB communication encryption option in **shipnow.ini** file as **ENCRYPT_DB_COMMUNICATION=ENABLE_ENCRYPTION=n**
3. Navigate to the <Parcel Artifact Folder>/Flagship/java/conf/configuration.properties file and update the SSL option as follows:
 - a. useSSL: **false**
4. In the <Parcel Artifact Folder>\Flagship\ucm\java\META-INF\config.xml file, set line useSSL as 'false'.

- a. `<useSSL>false</useSSL>`
5. Restart the following services:
 - MySQL
 - Kewill DiServer Service
 - Kewill IA Service
 - Kewill Notification Service
 - Kewill Scheduler Service
 - Kewill Tracking Service
 - KewillFlagshipConnectorFileService
 - KewillFlagshipDatabaseFileService
 - KewillFlagshipServerBridgeService
 - KewillReportingService
 - BluJayParcelCensusTool
 - BluJayParcelDataUploadTool
 - (For UCM): BluJayUCMServer Service
 - (For UCM Purge): BluJayUCMPurgeService Service

Note

You must enable the database communication encryption option, update the secure socket layer (SSL) options, and restart the services after successfully completing the upgrade installation process. After successful upgrade, you must reconfigure SSL settings in ODBC. Refer *Configuring SSL Settings in MySQL Connector/ODBC* section under [Configure Encrypted Connections to Database](#) for details.

Perform Upgrade Installation

To perform upgrade parcel installation, follow these steps:

1. Download Parcel from the FTP site and extract the contents from the installation zip file to a local system.
2. Check environment path for below mandatory values:

1. `C:\WINDOWS\system32;`
2. `C:\WINDOWS;`
3. `C:\WINDOWS\System32\Wbem;`
4. `C:\WINDOWS\System32\WindowsPowerShell\v1.0\;`
5. `C:\Program Files\MySQL\MySQL Server 5.7\bin;`

Note: If you are not finding these values, refer to the *Error Message related to powershell* section.

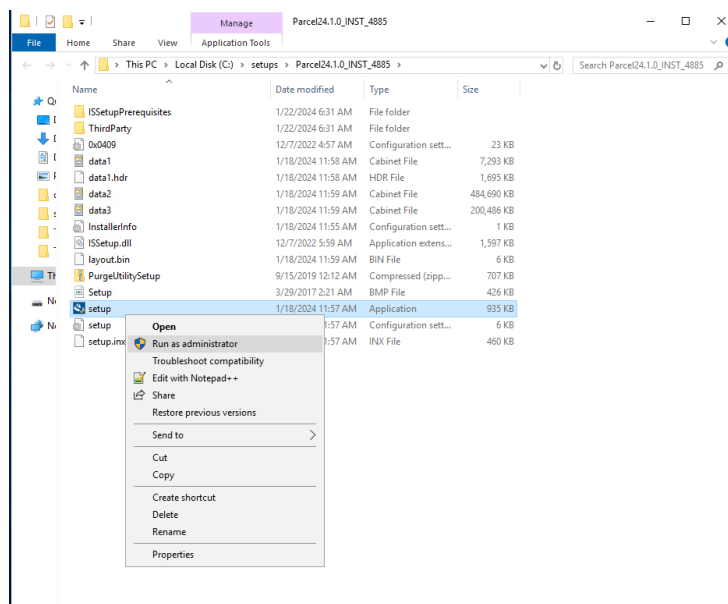
3. If upgrading from 22.x and 23.x to 24.1.0 and using a 'Remote MySQL Server' or a 'Remote Aurora' server, follow steps below. If not, skip to step 4.
 - a. Take a backup of <Parcel Artifact Folder>\Flagship\bin\shipnow.ini
 - b. In Application Server, Navigate to <Parcel Artifact Folder>\Flagship\bin\shipnow.ini
 - c. In shipnow.ini, replace the line starting with MySQLHost with the following:

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

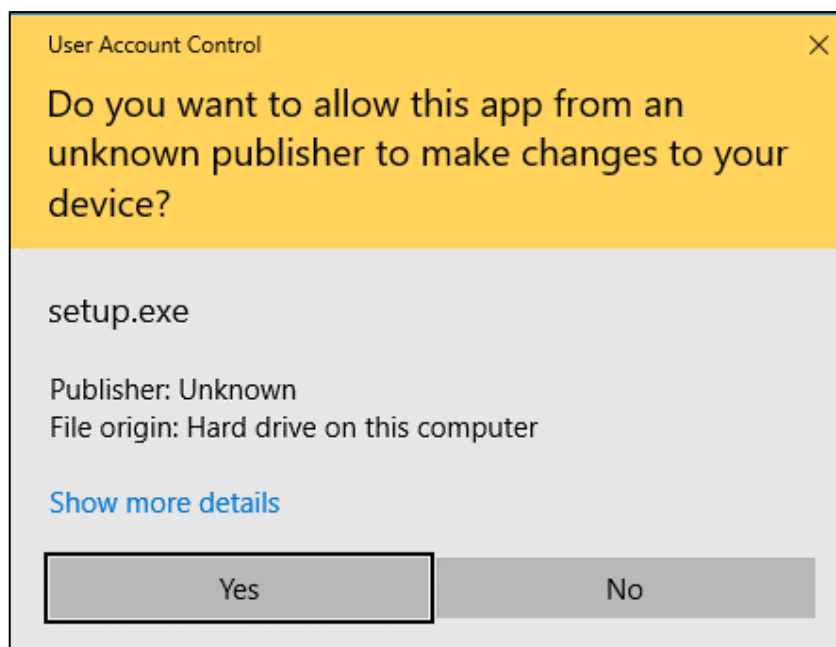
Note

Replace localhost with your remote server IP address or remote hostname and save the file.

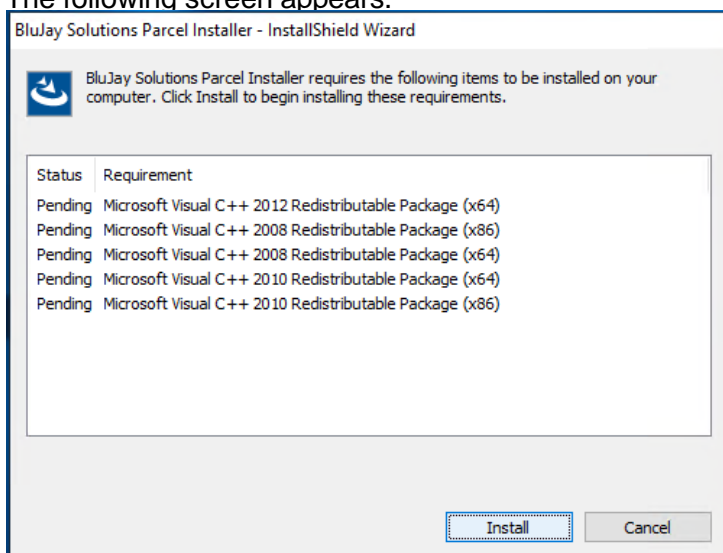
4. Run setup.exe as an 'administrator'.



5. In the setup.exe window, click Yes to the 'Do you want to allow this app from an unknown publisher to make changes to your device?' prompt.



The following screen appears.



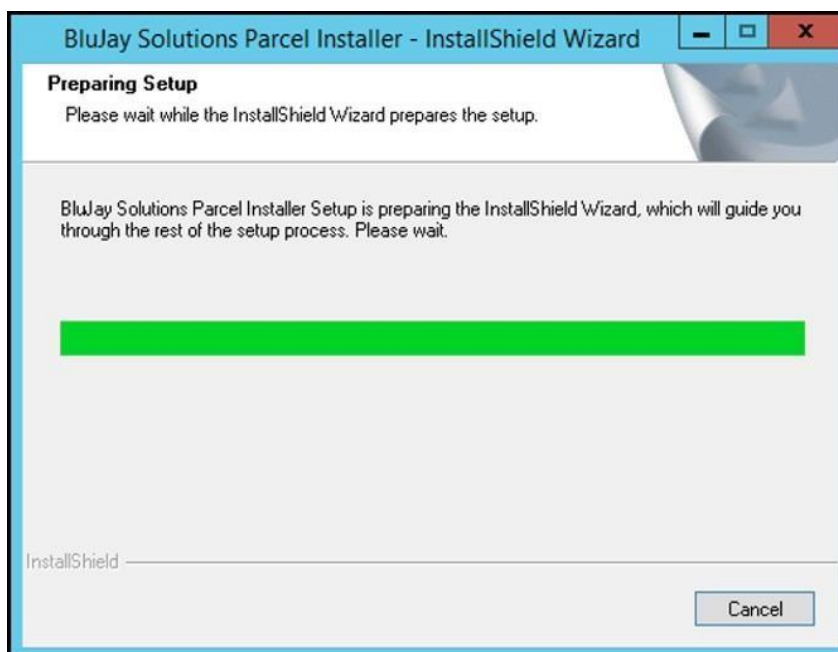
- Click Install.

Note

If you get 'BluJay Solutions Parcel Installer' dialog box with "The installation of BluJay Solutions Parcel Installer requires a reboot" message, click Yes to restart the system. The upgrade installation process continues after system restart.

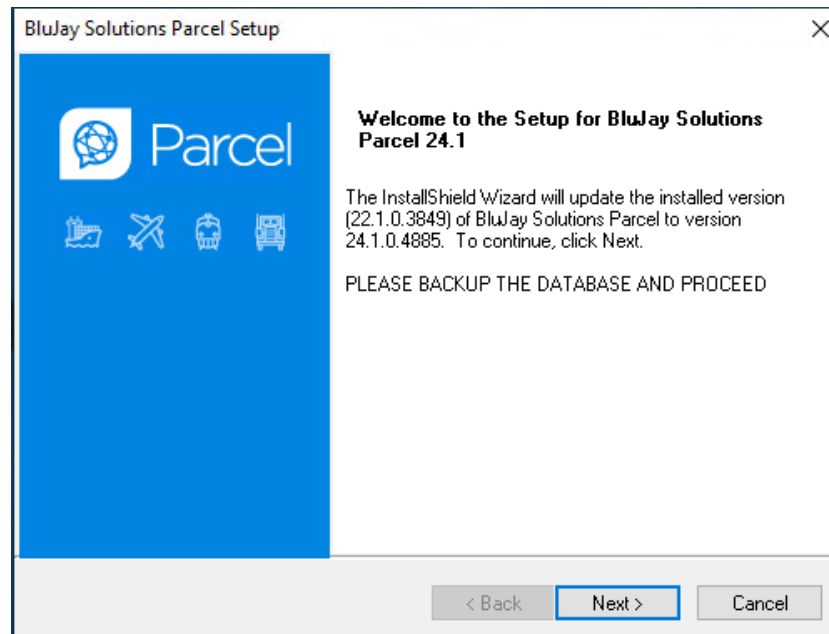


After few seconds, the Preparing Setup screen appears.

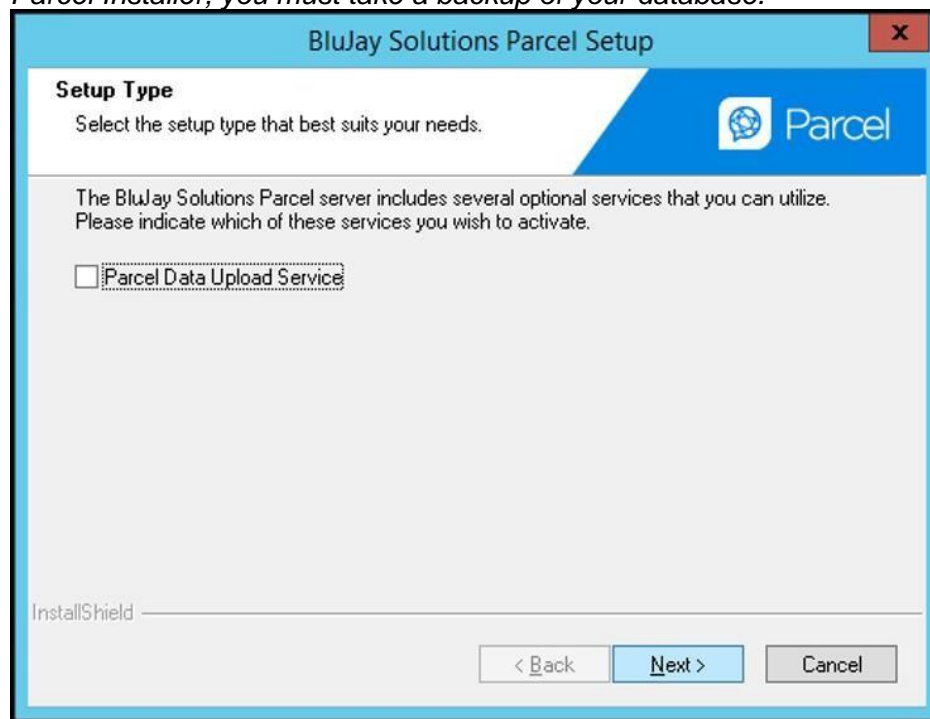


After few seconds, the Welcome screen of the Parcel Setup wizard appears.

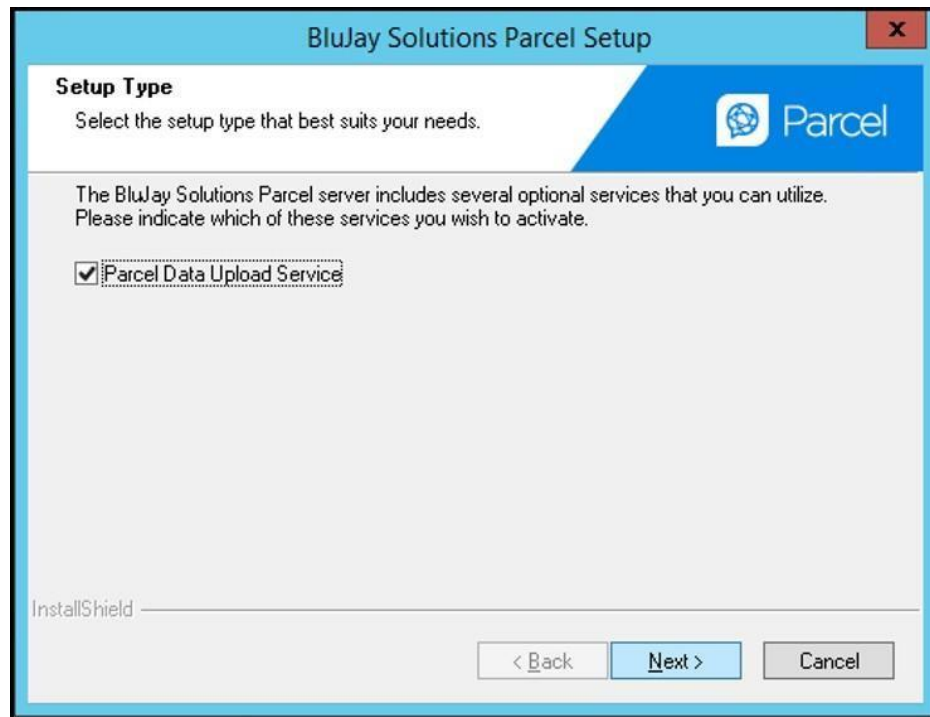
7. Click Next on the 'Welcome to the Setup...' screen of the wizard to continue with the upgrade installation.



Important Note: Before upgrading the MySQL to 8.0.32 and ODBC to 8.0.33 via Parcel Installer, you must take a backup of your database.



8. On BluJay Solutions Parcel Setup screen, select Parcel Data Upload Service checkbox to enable EOD Upload and then click Next and continue with the upgrade installation.

**Note**

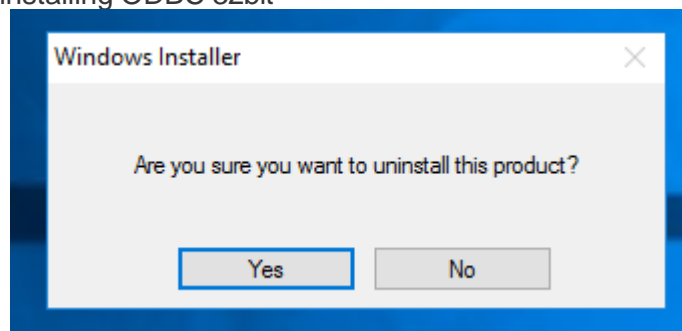
In case 'File Error' dialog box appears, click Retry and continue with the upgrade installation.

9. The system starts to uninstall previous versions of ODBC and MySQL as shown in the below sequence of screens:

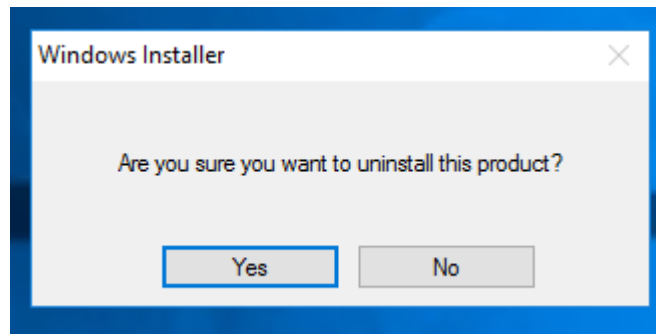
Note

If you are upgrading from 23.2 to 24.1.0, you will not see uninstall message for ODBC 32bit and 64bit.

Uninstalling ODBC 32bit

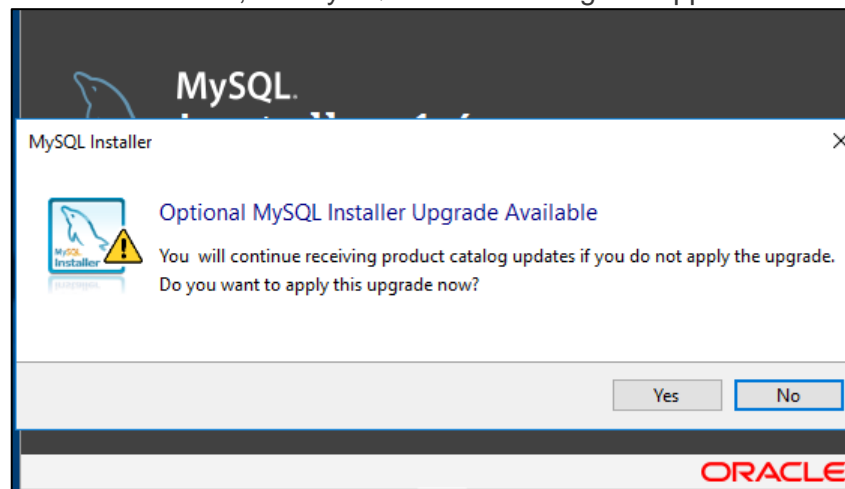


Uninstalling MySQL 5.7



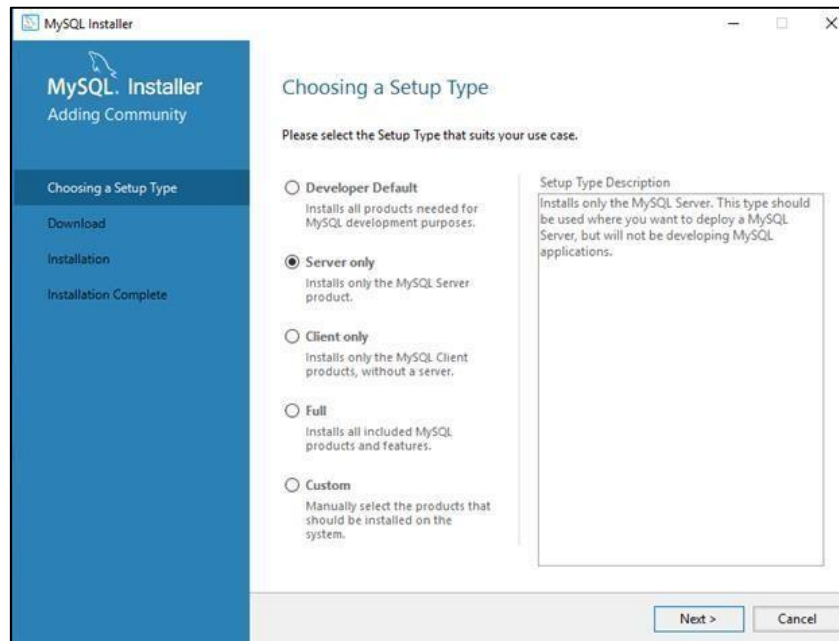
10. Click Yes to continue.

11. After few seconds, the MySQL Installer dialog box appears.

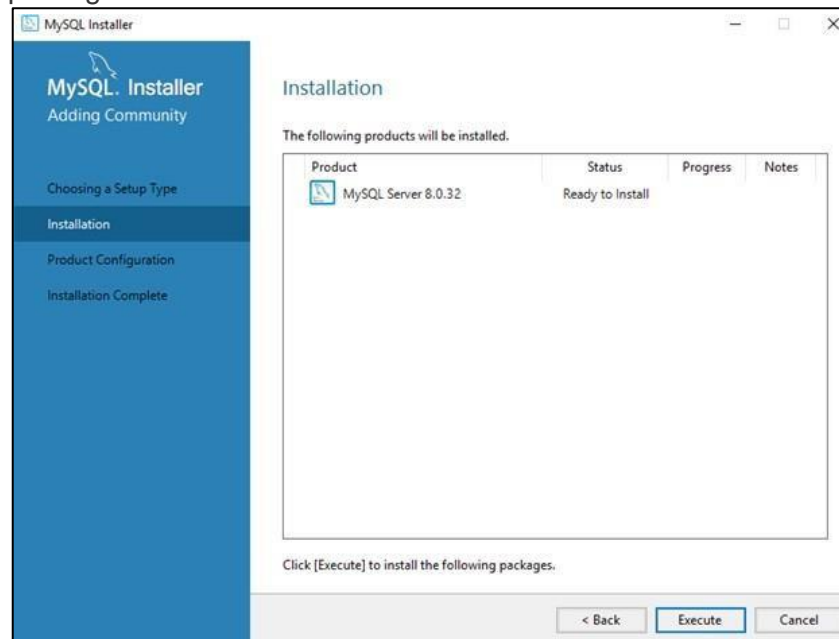


12. Click No to close the dialog box. The Installation Wizard continues with the upgrade installation.

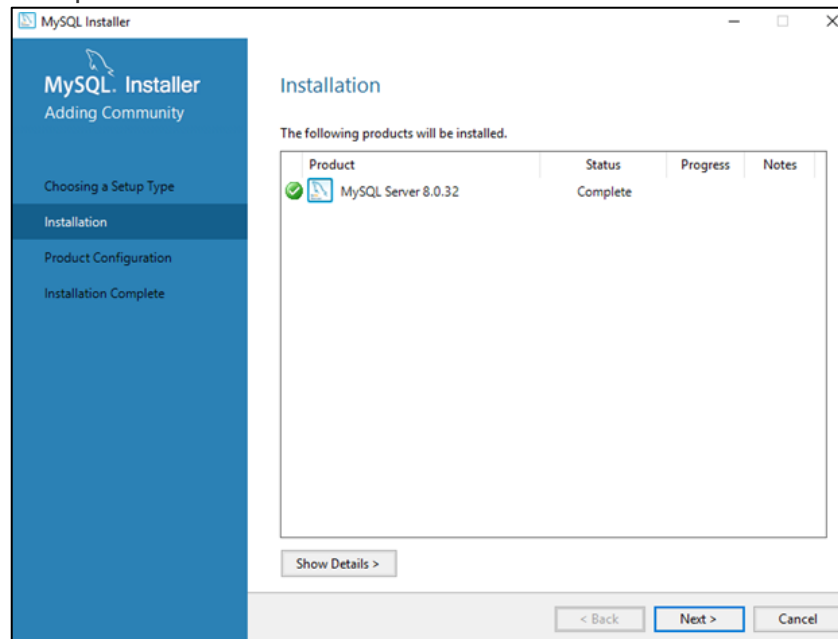
13. On the Setup Type screen, select the **Server only** option and then click Next.



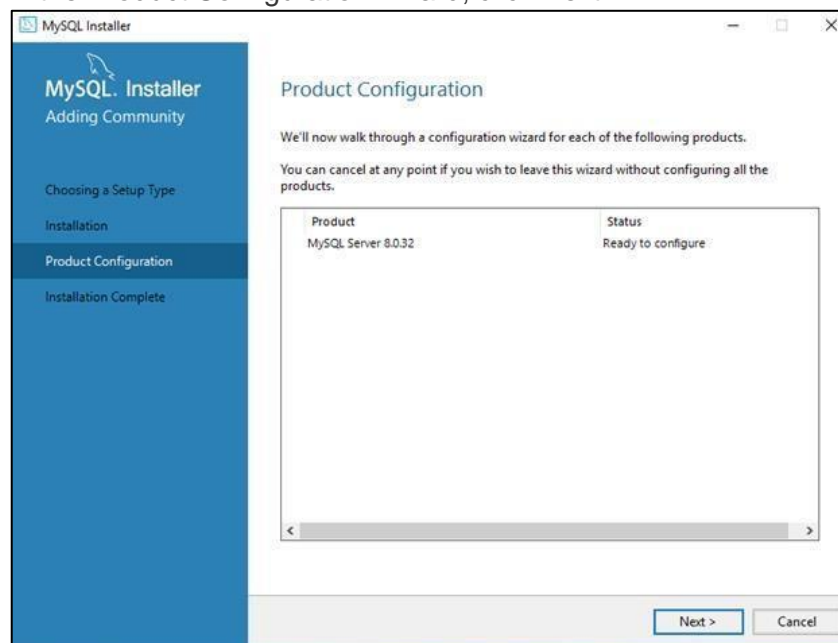
14. In the MySQL Installer screen, click Execute to install MySQL Server 8.0.32 package.



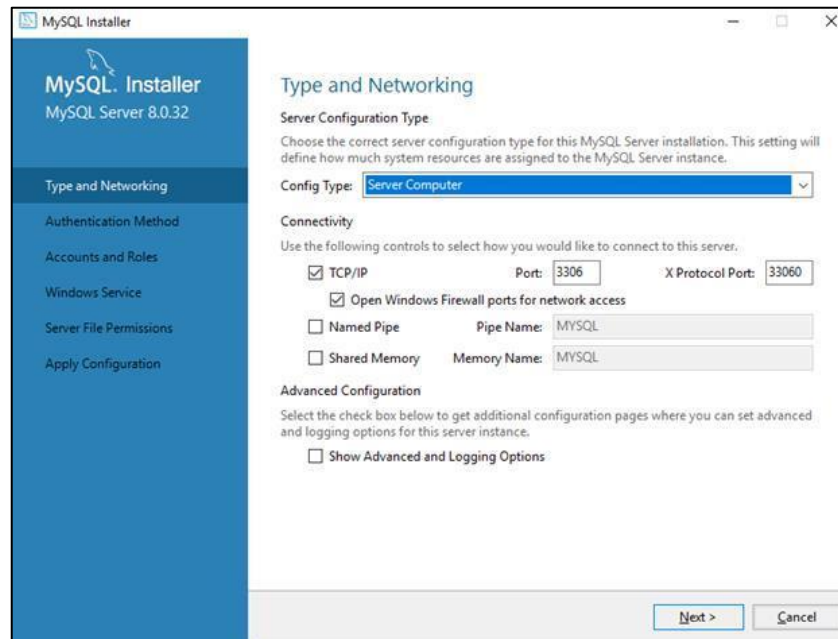
15. The installation completes. Review the MySQL Server 8.0.32 package *Status* as 'Complete' in the Installer screen and then click Next.



16. In the Product Configuration wizard, click Next.



17. On the Type and Networking screen, select Config Type as '**Server Computer**' and then click Next.



18. On the Authentication Method screen, select '**Use Legacy Authentication Method**' and then click Next.

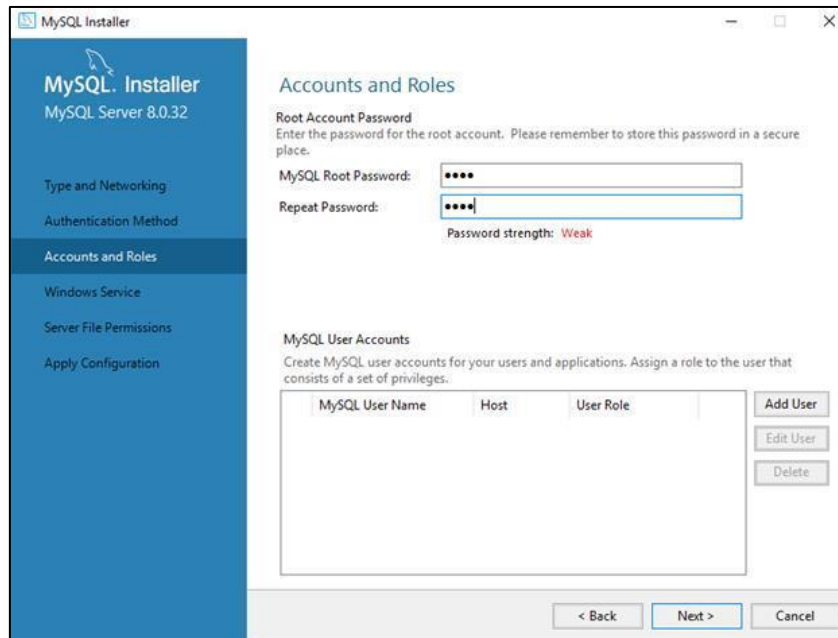


19. On the Accounts and Roles screen, type "root" (all lowercase letters without quotation marks) in the "MySQL Root Password" and "Repeat Password" fields, and then click Next.

Warning

You must type this specific password, since Parcel uses this as the root account password as required by the Parcel Configuration (Web Admin) Tool.

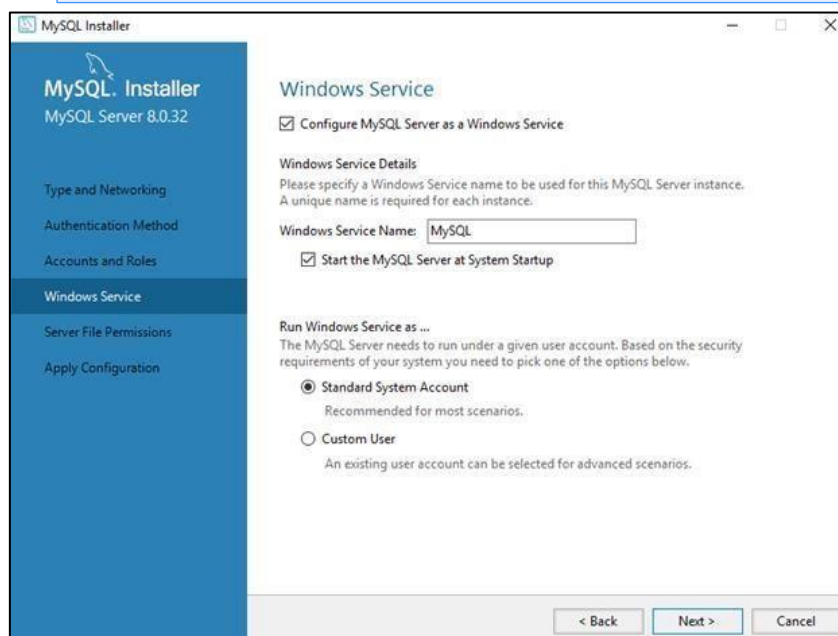
The root account has all privileges in the MySQL database. It is important to create a root account password. Any user logged in from a valid hostname can access MySQL and make alterations to the database using this root account.



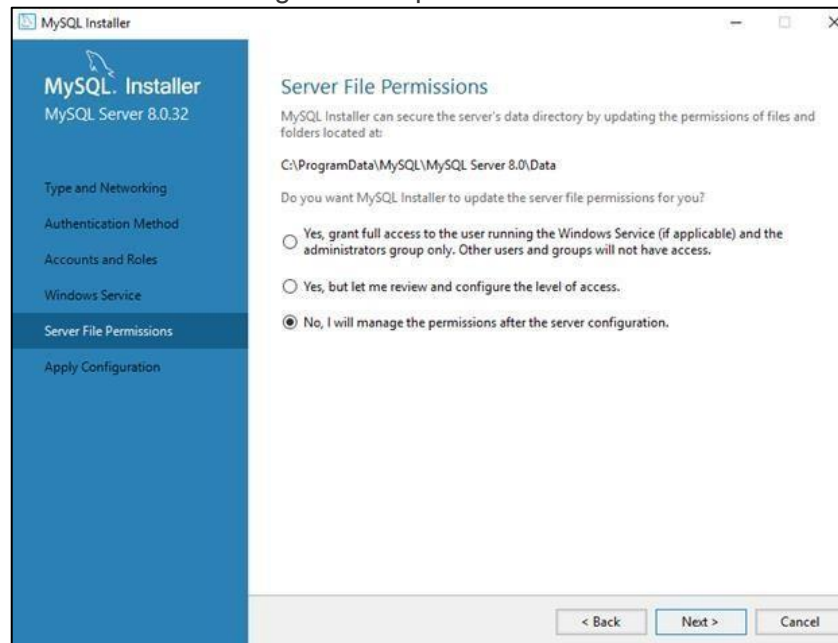
20. On the Windows Service screen change the window service name to MySQL in "Windows Service Name" field and leave the default settings as it is in the screen and then click Next.

Note

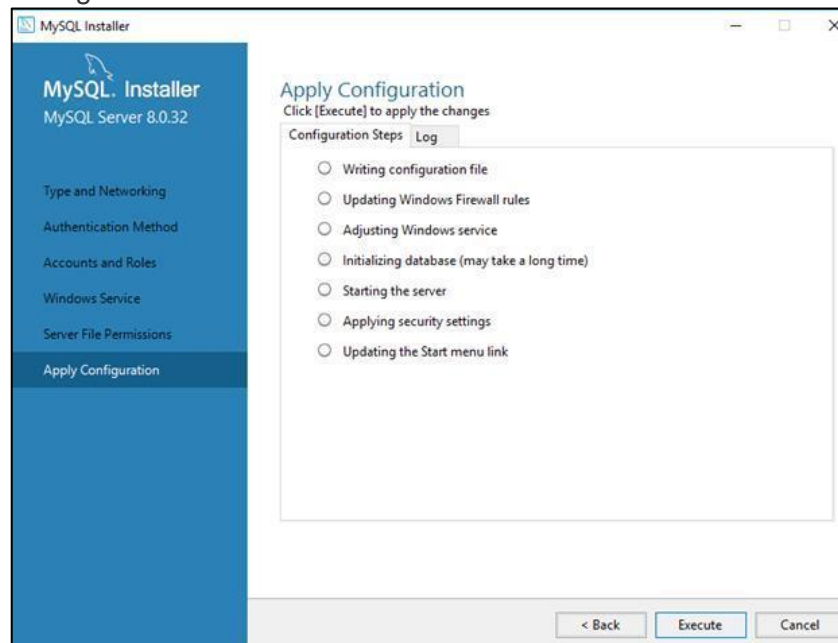
Ensure that the Windows Service Name field is MYSQL.



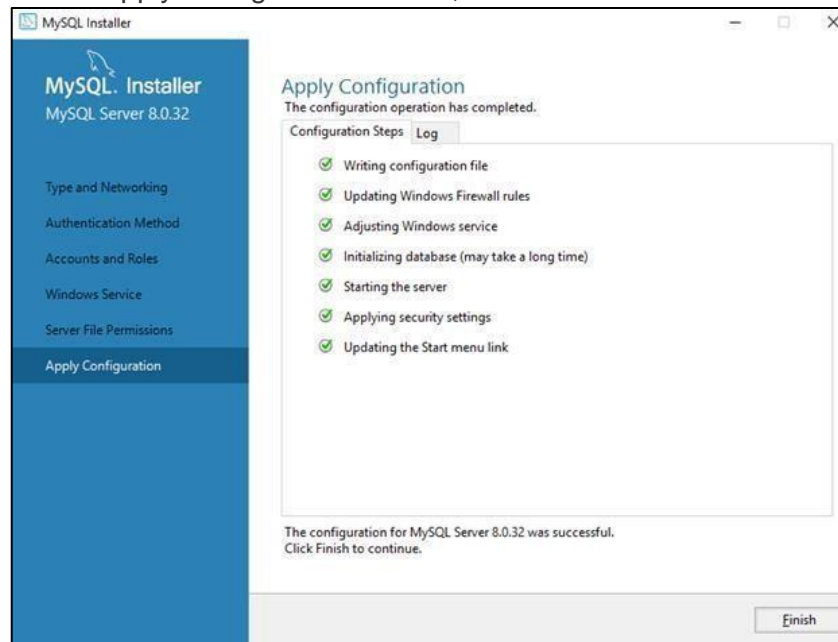
21. On the Server File Permissions screen, select "No, I will manage the permissions after the server configuration" option and click Next.



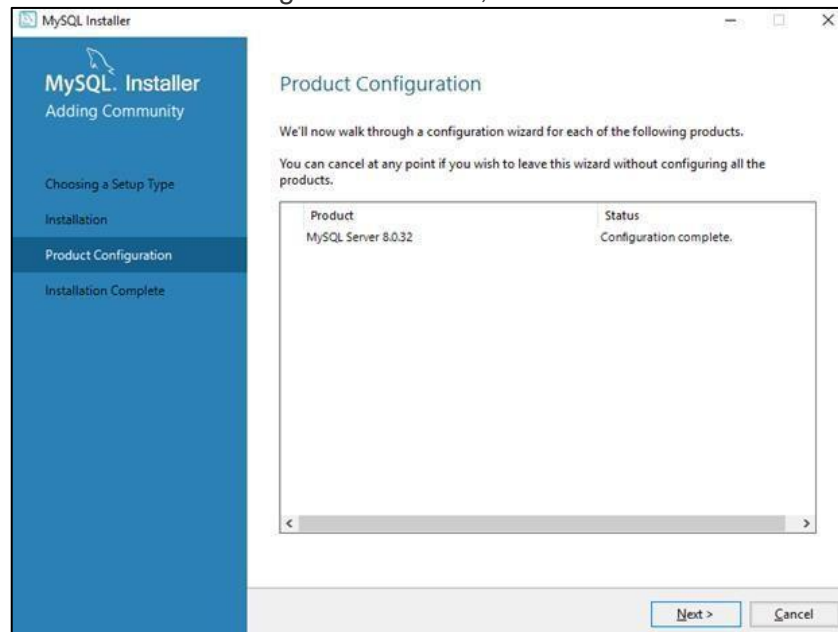
22. On the Apply Configuration screen, click Execute to enable your configuration settings.



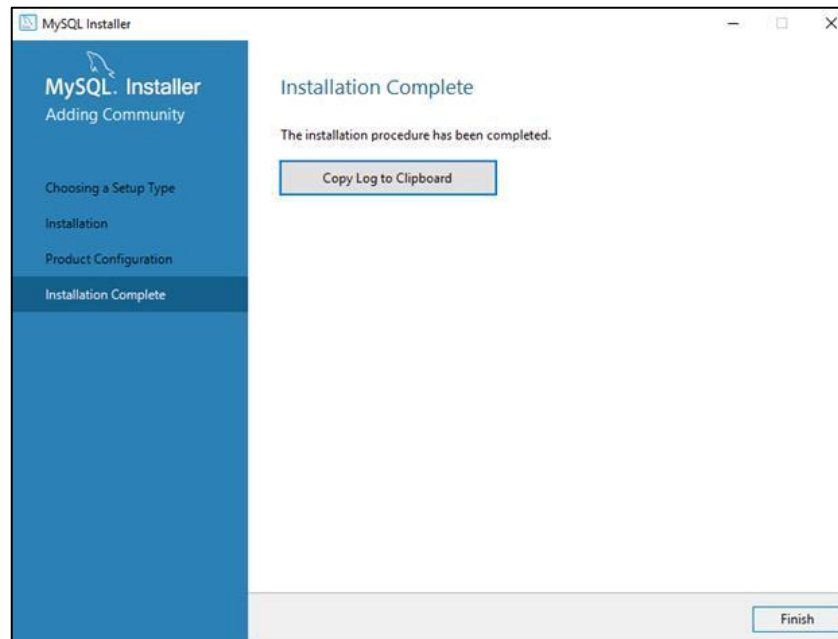
23. On the Apply Configuration screen, click Finish.



24. On the Product Configuration screen, click Next.



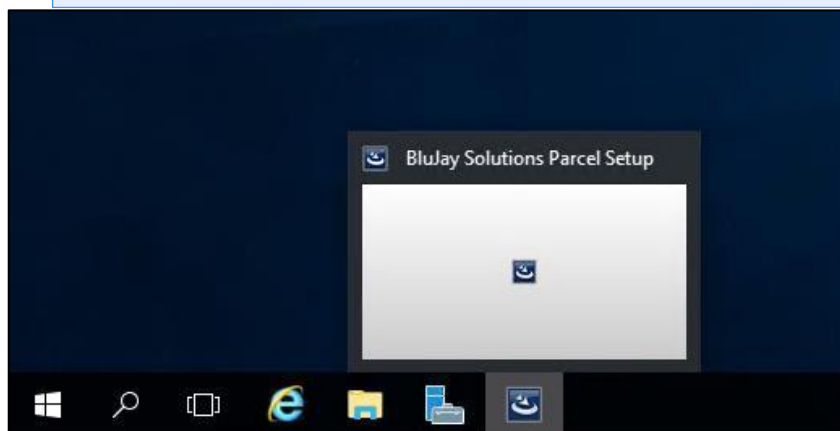
25. On the Installation Complete screen, click Finish to complete the MySQL installation.



26. After you click the Finish button, the upgrade process takes some time to display the next screen.

Note

You can view the process icon on your task bar.



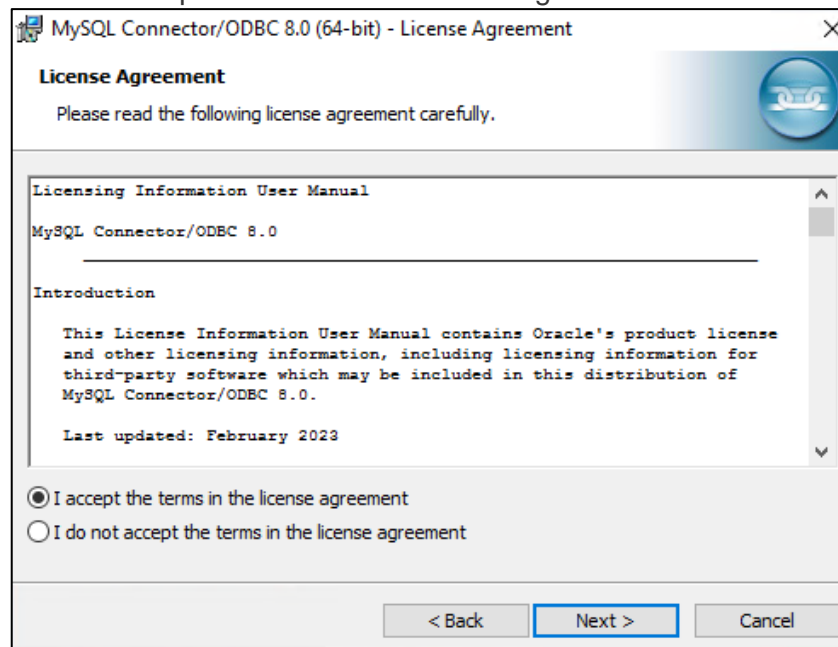
The Setup Wizard for MySQL Connector/ODBC 8.0 (64 bit) appears.



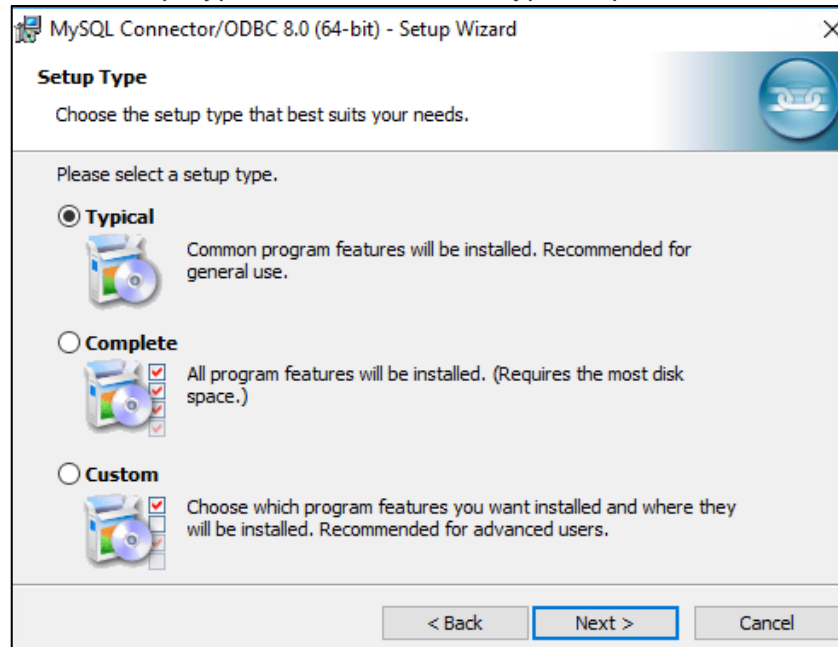
27. Click Next in the Setup Wizard.

The MySQL ODBC License Agreement screen appears.

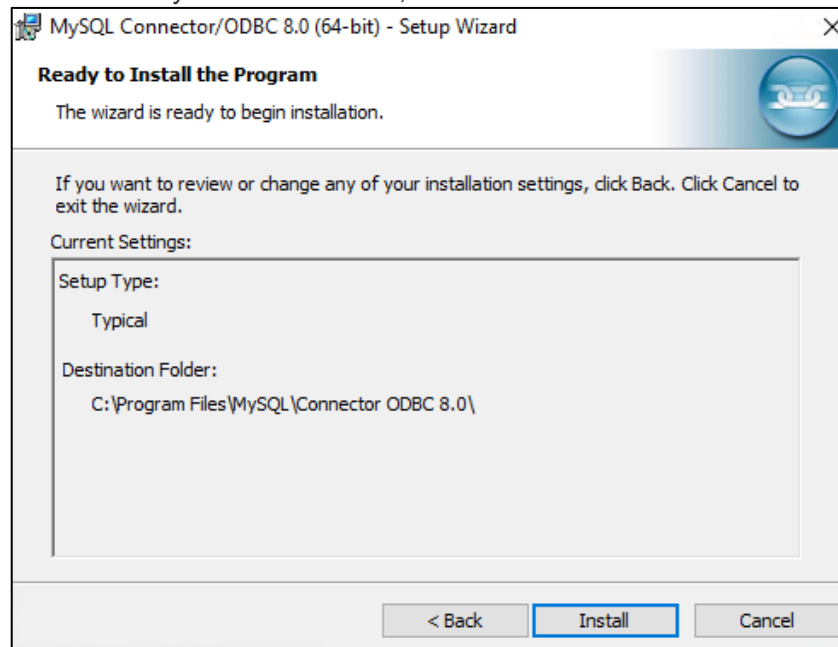
28. Select 'I accept the terms in the license agreement' and then click Next.



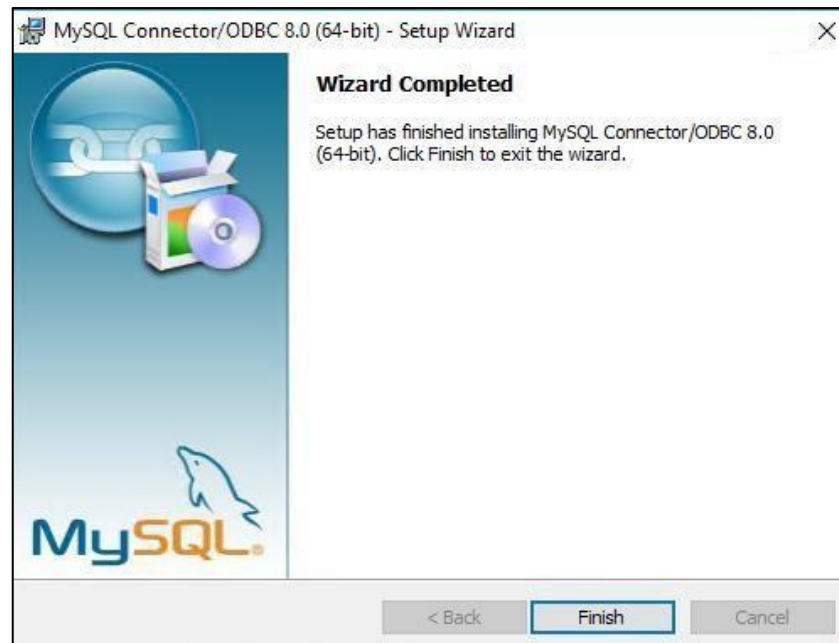
29. On the Setup Type screen, select the Typical option and then click Next.



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



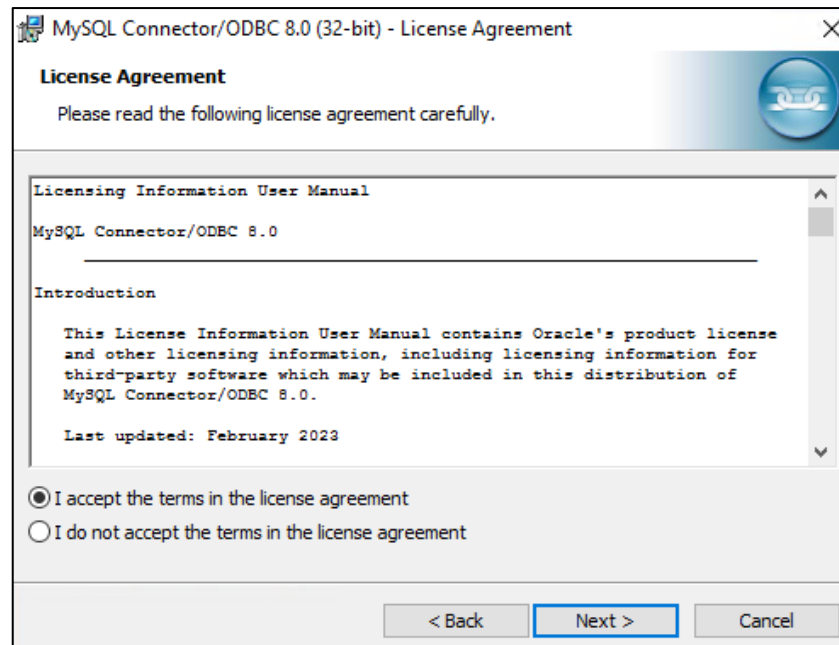
31. Click Finish in MySQL Connector/ODBC 8.0 (64-bit)-Setup Wizard to complete the installation.



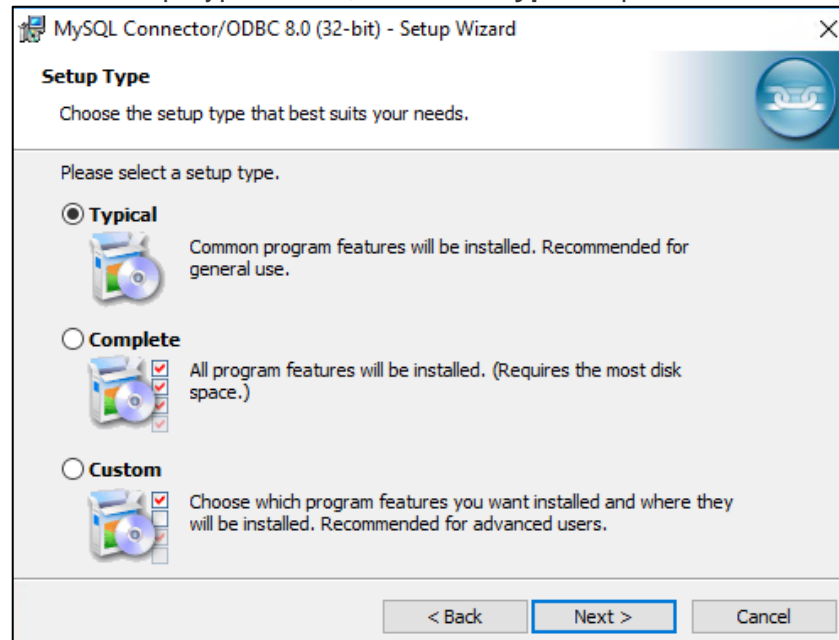
The MySQL Connector/ODBC 32bit Setup Wizard appears.



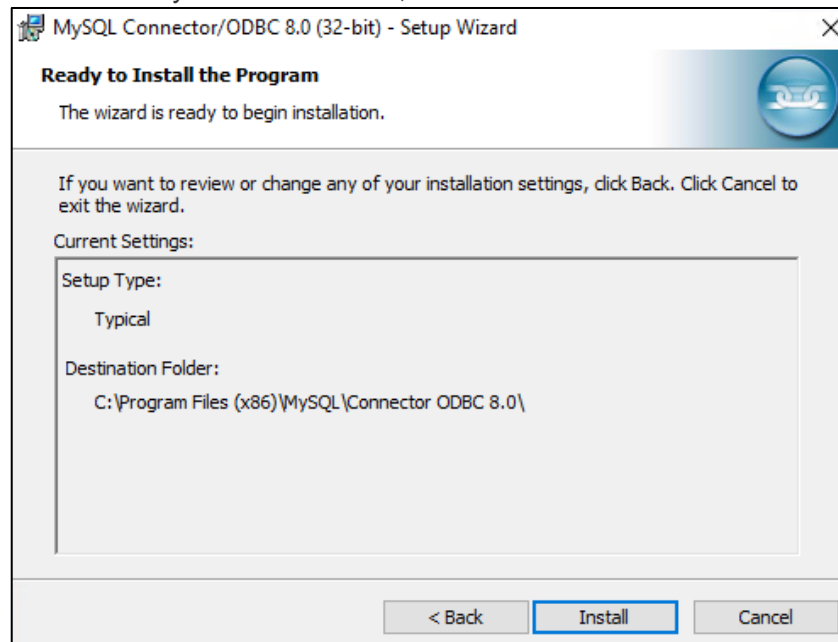
32. On the Welcome screen of the MySQL Connector/ODBC Setup Wizard, click Next.
33. Select 'I accept the terms in the license agreement' and then click Next.



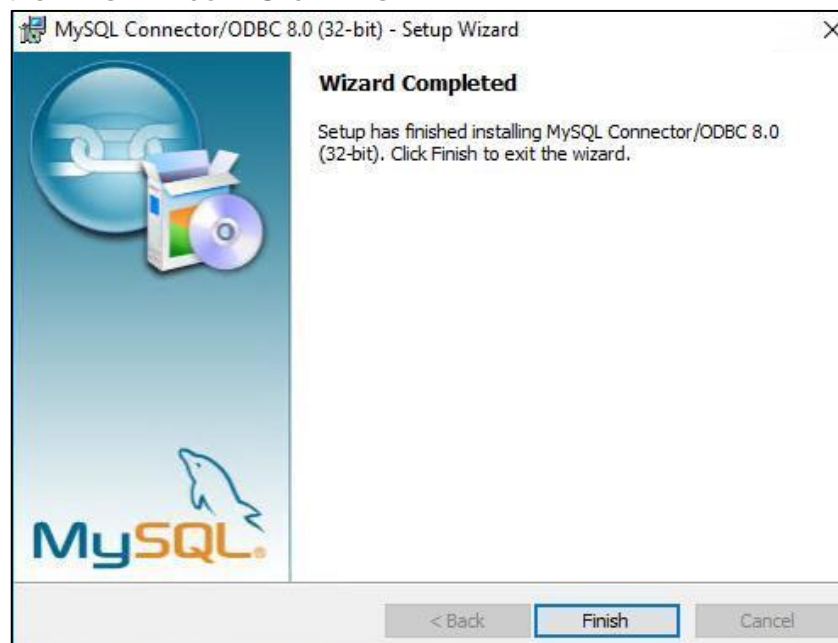
34. On the Setup Type screen, select the **Typical** option and then click Next.



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



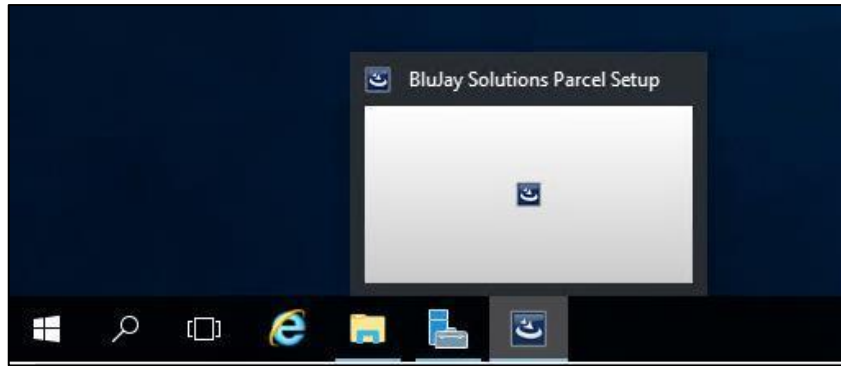
36. A progress bar enables you to view the progress of the installation. Installation completes when the MySQL Connector/ODBC 8.0 (32-bit) Setup Wizard displays the Finish window. Click Finish.



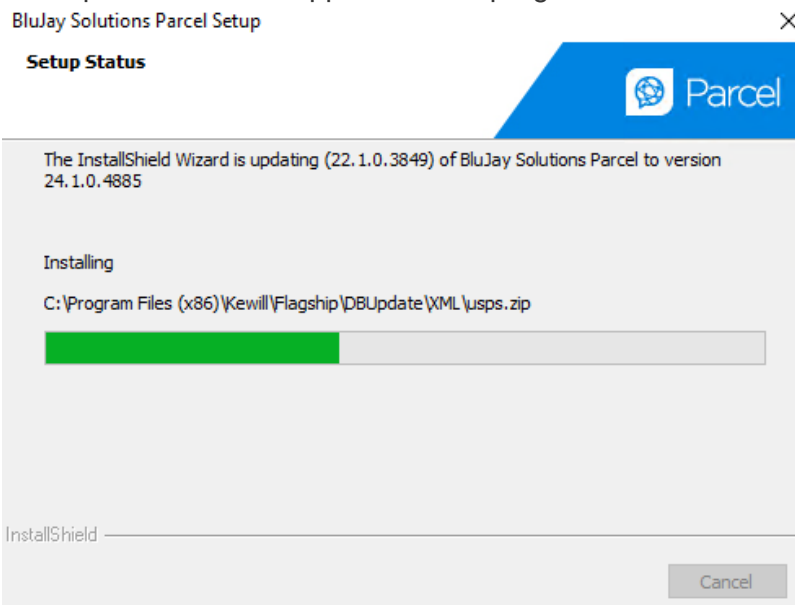
37. After you click the Finish button, the upgrade process takes some time to display the next screen.

Note

You can view the process icon on your task bar.

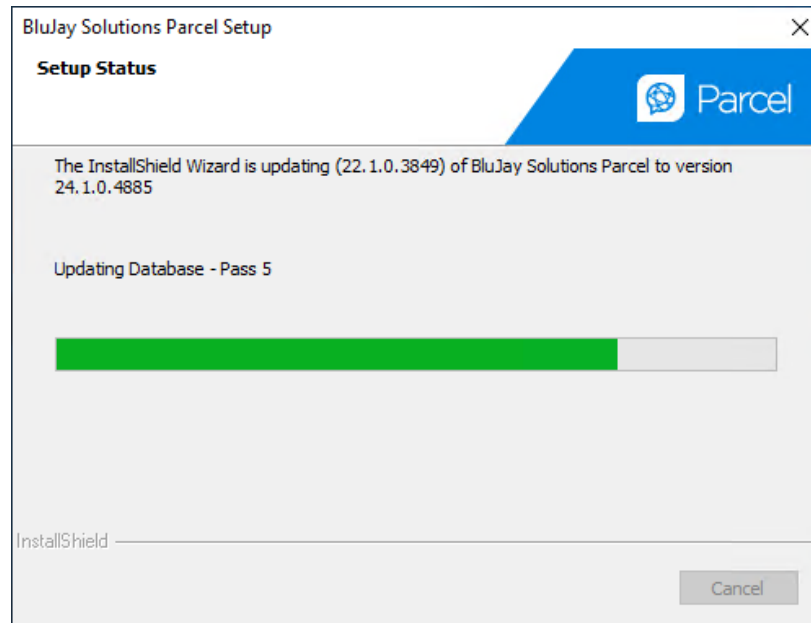


38. The Setup Status screen appears with a progress bar.

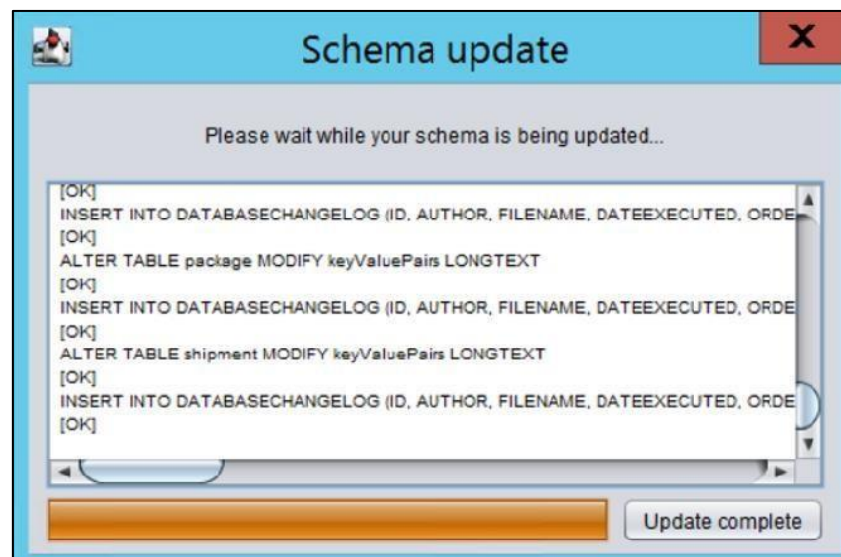


After the installation wizard completes installing the MySQL components that you selected to install, there a few more steps to complete the Parcel upgrade installation.

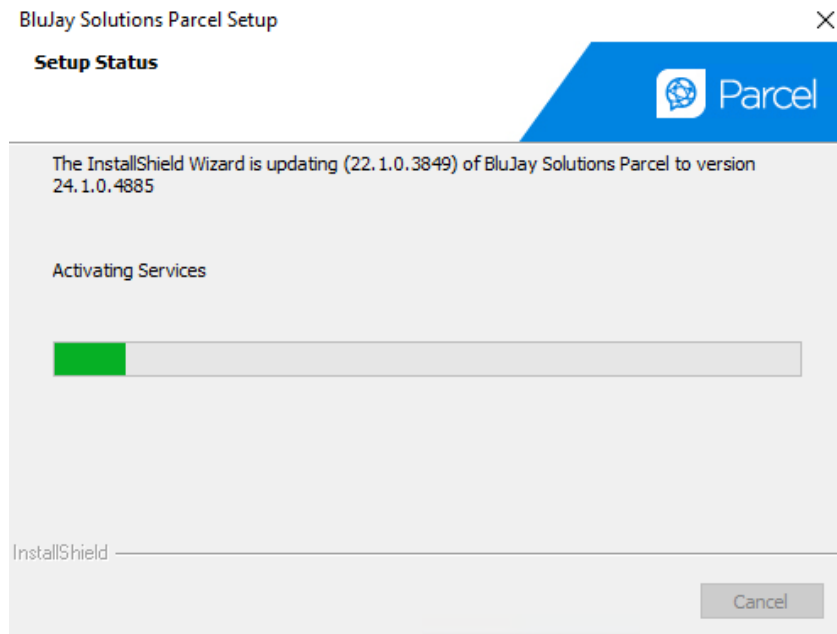
39. Click Next. The Setup Status screen displays Post Installation Activities progress bar.



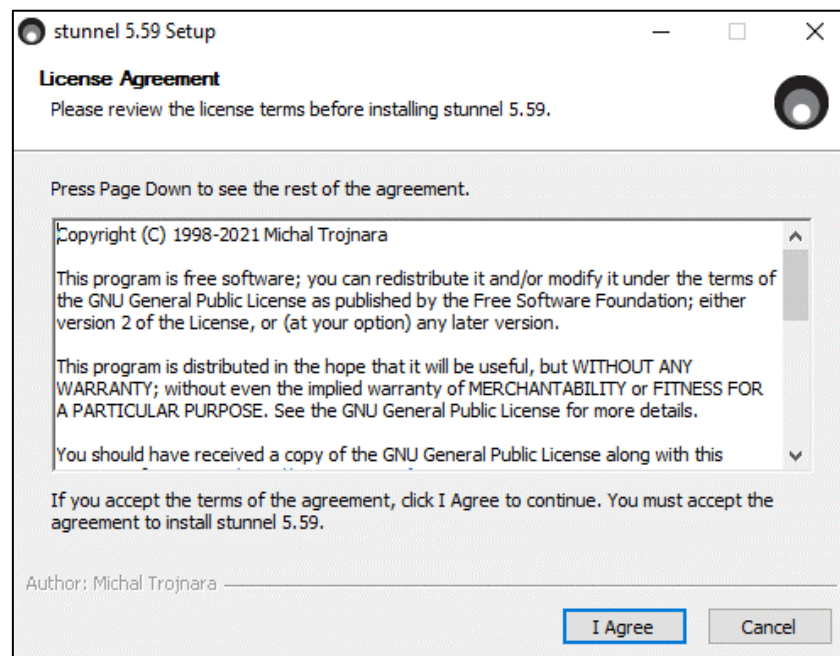
After updating Parcel Database, the Schema update screen appears for updating the Schema.



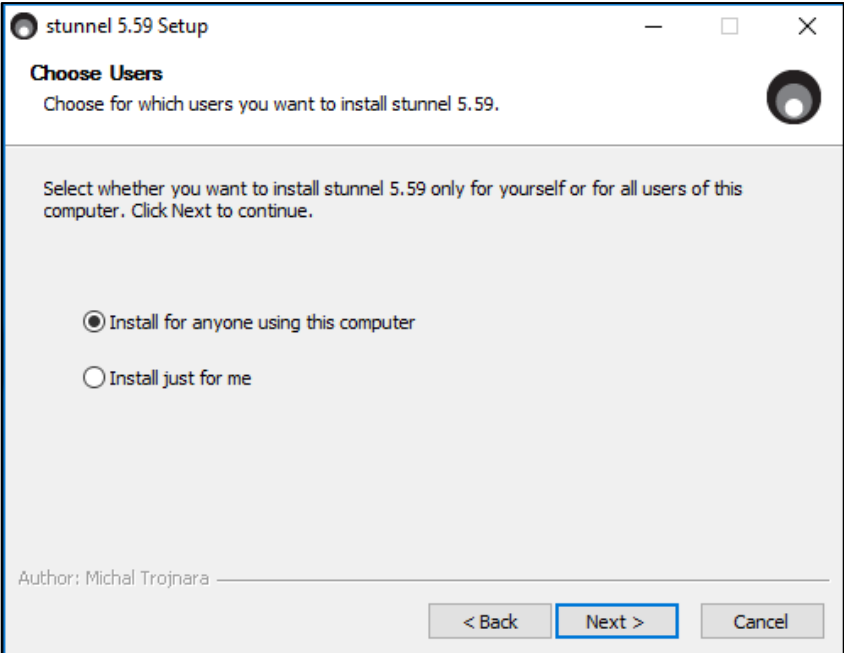
40. After completing the Schema update, click Update complete to finish the installation.
After Schema update is complete, Setup Status screen displays activating the services, as shown in following screen.



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

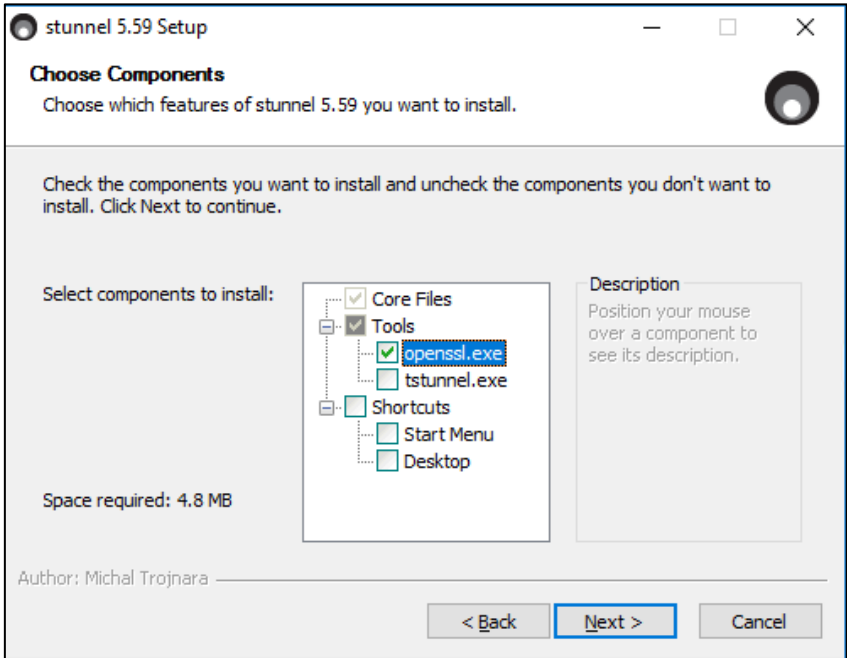


42. On the stunnel 5.59 Setup: Choose Users screen, select **Install for anyone using this computer** option, and then click Next.



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.

43. On the stunnel 5.59 Setup: Choose Components to install stunnel with selecting **openssl.exe** check box.

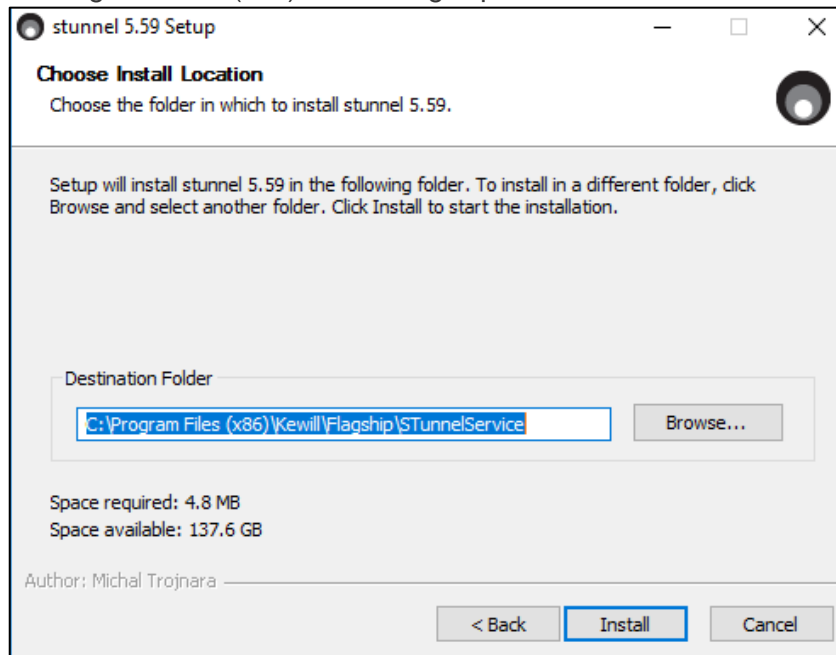


44. On the stunnel 5.59 Setup: Choose Install Location screen, click Browse... and specify the following Destination Folder and then click Install to proceed with the stunnel installation.

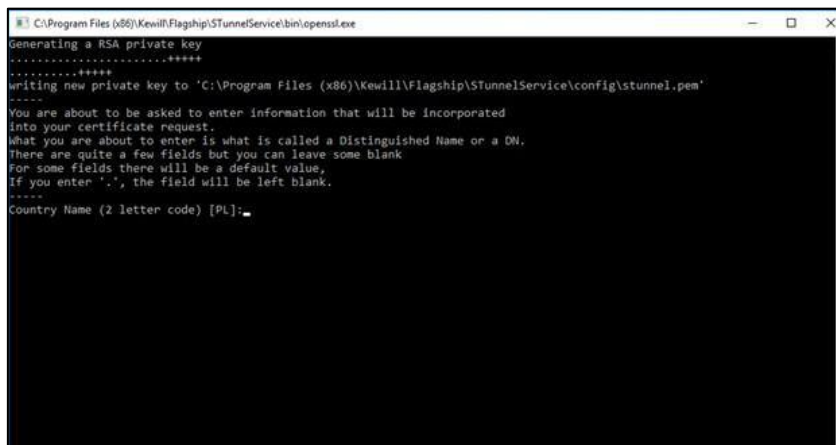
<Drive>: \<Parcel Install Folder>\Flagship\STunnelService\

For Example:

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



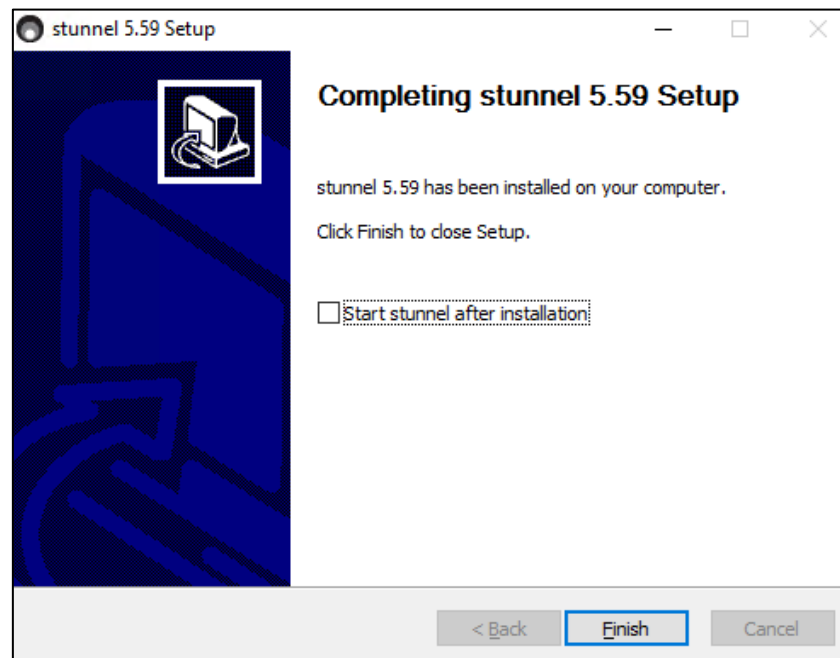
45. Enter your address details for the certificate in the openssl.exe file, as shown in the following table.



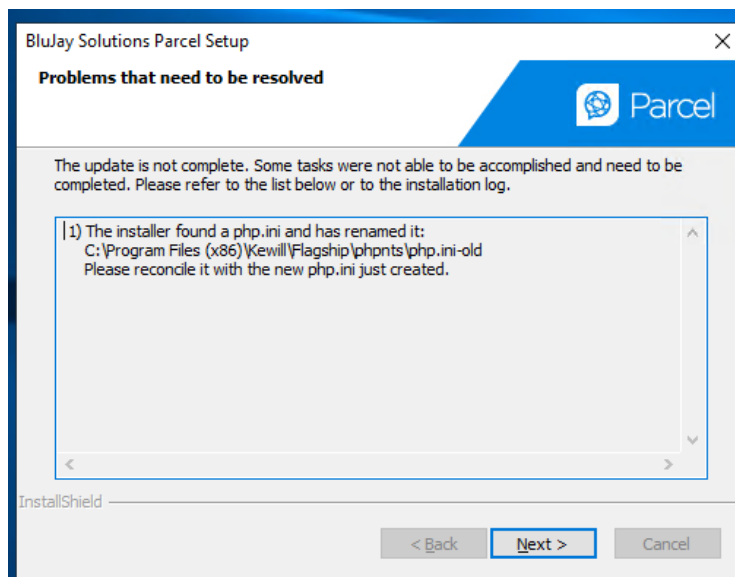
Field	Task
Country Name	Enter the country name in 2 letter code. For Example: US
State or Province Name	Enter the state or province name. For Example: Massachusetts
Locality Name	Enter the city name. For Example: Chelmsford

Field	Task
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.

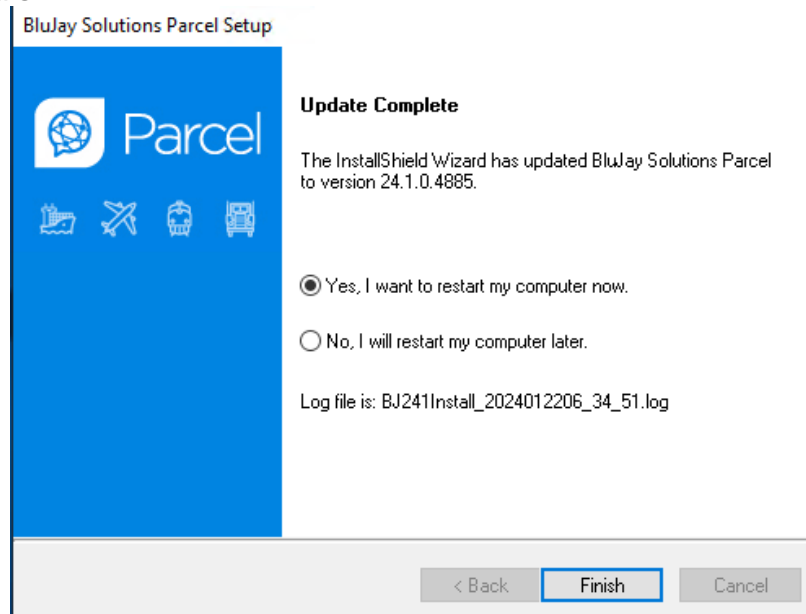
46. On the stunnel 5.59 Setup: Completing stunnel 5.59 Setup screen, click Finish to complete the stunnel installation.



Once activating service is completed, if there are any errors, the Setup wizard displays these errors, as well as the location of the installation log file.



47. If there are errors review the installation log files. Refer sections under **Troubleshooting** for information on resolving these. Otherwise, click Next to complete the upgrade installation.
48. If there are no errors during the installation, the Update Complete screen appears.



To run Parcel, you need to restart the computer where it is upgraded. The screen gives you the following options:

- a. Yes, I want to restart my computer now (default selection)

- b. No, I will restart my computer later.
49. Make the desired selection, and then click **Finish** to complete the upgrade. After Parcel upgradation is successfully completed, follow the Post Installation Tasks.

Upgrading Parcel DB to 24.1.0 on Aurora Server

This section provides the information on upgrading Parcel DB 22.x and 23.x to 24.1.0 on Aurora Server.

Note: The below steps are same for upgrading Parcel DB older versions on Aurora Server. But the Prerequisites of Parcel versions on Application Server and Aurora Server are differ based on the respective Parcel versions.

Prerequisites:

- Application Server should have Parcel 22.x or 23.x and ensure that MySQL installed on Application Server.
- Aurora Server should have Parcel DB 22.x or 23.x.

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

1. From Upgrading Parcel section, follow the instructions from steps 1-5.
2. Follow the below steps to upgrade Parcel DB from to 24.1.0 in the Application Server.
3. Navigate to <Parcel Artifact Folder>\Flagship\DBUpdate\XML\flagshipProperties.xml to change the value for 'flagshipHost' element from 'localhost' to Hostname/IP of the Aurora Server.
4. Navigate to <Parcel Install Folder>\Flagship\DBUpdate\XML\SetupProperties.bat
5. 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"
6. 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%
7. 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. mysql -h <hostname> -u<username> -p<pwd> -f < %create_fs_user%
8. Save the file.
9. Navigate to <Parcel Install Folder>\Flagship\DBUpdate\UpdateDB_All_50.bat
10. Replace the line "mysql -f <set_permissions.sql" 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 < set_permissions.sql
```

11. Save the file.
12. Open a command prompt using Administrative privileges and change directory to folder: <Parcel Install Folder>\Flagship\DBUpdate and Execute the command.
13. Execute the following command and wait for it to complete.UpdateDB_All_50.bat
1 > update.log 2>&1
Now, the Parcel DB on Aurora Server is upgraded to 24.1.0.

After the successful upgrade to Parcel DB 24.1.0, connect Application Server with Aurora DB. See [Connecting Remotely to Database](#) section for details.

Upgrading Parcel DB to 24.1.0 on Remote Server

This section provides the information on upgrading Parcel DB 24.1.0 on Remote Server. **Note:** The below steps are same for upgrading older versions on Remote Server. But the Prerequisites of Parcel versions on Application Server and Remote MySQL Server might differ based on the respective Parcel versions.

Prerequisites:

- Application Server should have Parcel 22.x or 23.x and ensure that MySQL along with data folder exists.
- Remote MySQL Server should have Parcel DB 22.x or 23.x

To upgrade Parcel DB to 24.1.0 on Remote Server, follow these

steps: 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. Uninstall MySQL 5.7.x and restart the Server.
2. Extract the contents of the Parcel distribution zip file to a folder with no spaces on the remote server.
3. Navigate to ThirdParty folder and install MySQL 8.0.32. Follow steps 1-12 from *Installing the MySQL Server* section as described in the **TM-Parcel Fresh Installation Guide**. Now, the MySQL on Remote Server is successfully installed.

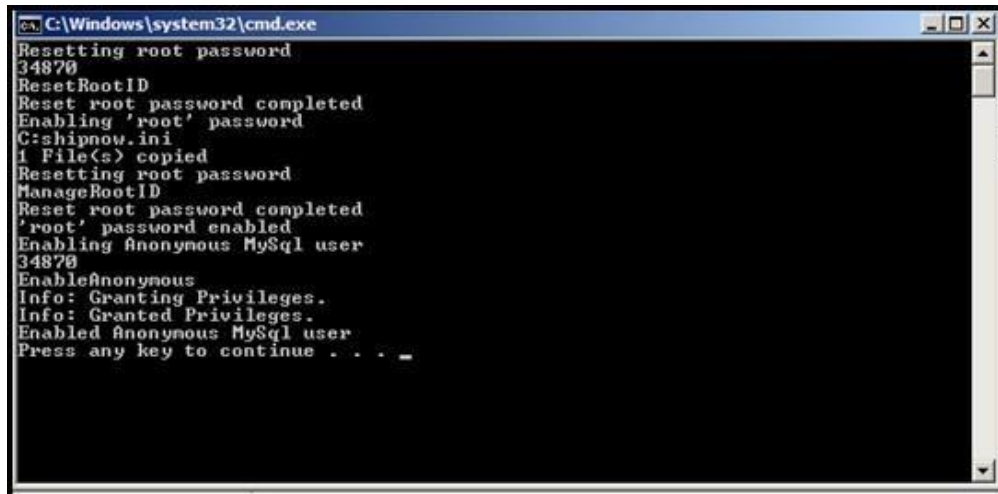
Note

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.

4. Copy the my.ini file from Application Server MySQL 8.0 folder and replace the file my.ini file on MySQL 8.0 Server folder of the Remote Server.
5. Restart MySQL Service.

On Application Server

1. Copy the 'RemoteMySQL' folder from Parcel 24.1.0 installation package to a local 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_upgrade.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
5. Navigate to <Parcel Install Folder>\Flagship\DBUpdate\XML\SetupProperties.bat
6. 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"
7. 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%
8. 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%
9. Save the file.

10. Navigate to <Parcel Install Folder>\DBUpdate\UpdateDB_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
11. Open a command prompt using Administrative privileges and change directory to folder: <Parcel Install Folder>\Flagship\DBUpdate and Execute the command.
12. Execute the following command and wait for it to complete.
UpdateDB_All_50.bat 1 > update.log 2>&1

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

Now, the Parcel DB on Remote Server is upgraded to 24.1.0 To disable anonymous user navigate to 'RemoteMySQL' folder and double click on 'DisableAnonymous_RemoteServer.bat' file.

Note

After the successful upgrade to Parcel DB 24.1.0, connect Application Server with Aurora DB. See [Connecting Remotely to Database](#) section for details.

After Remote Parcel DB upgrade is successfully completed, follow the **Post Installation Tasks**.

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, 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.

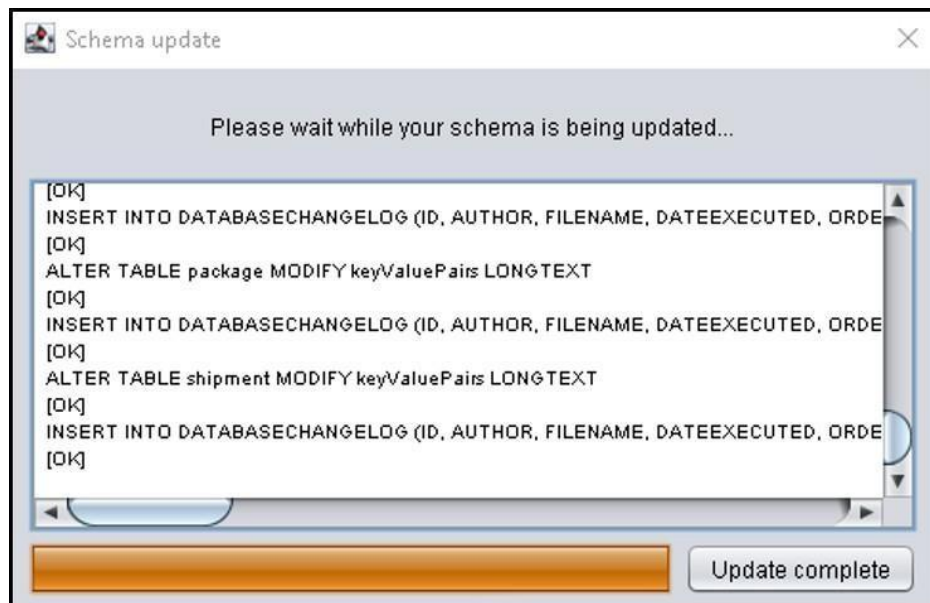
```

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 ?>

```

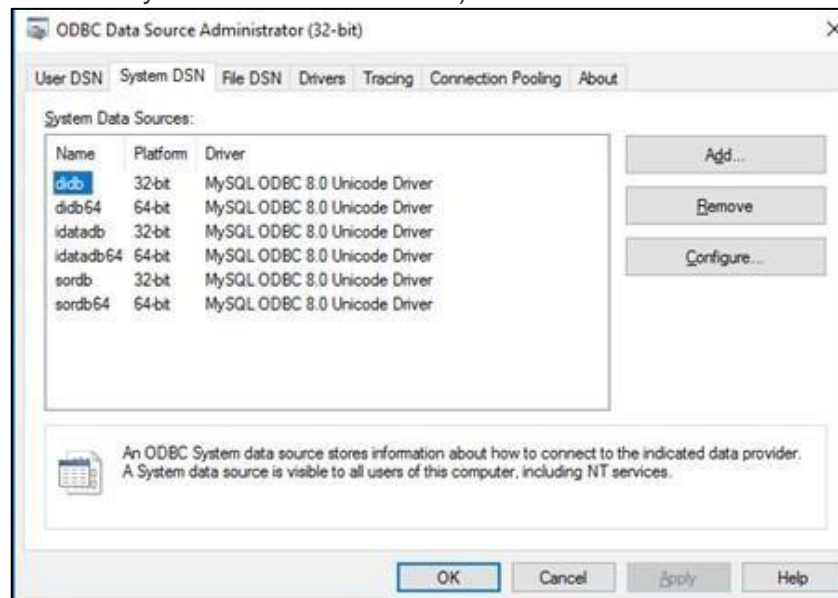
5. For UCM - configure the details in 'Config.xml' file: **ucm/java/META-INF** and Persistence.xml file: **ucm/java/META-INF** (replace localhost and provide Remote MySQL Server IP address and update username and password.)
6. Navigate to <Parcel Install Folder>\Flagship\ucm\java folder, open 'UCM-Server-Service-Install.bat' 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-Server-Service-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 update.

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

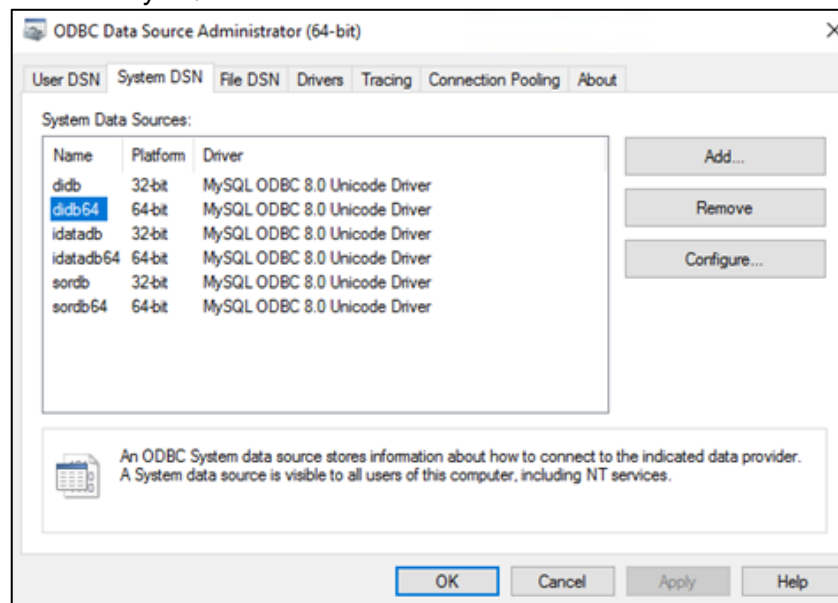


9. Select **didb** and click Configure.

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

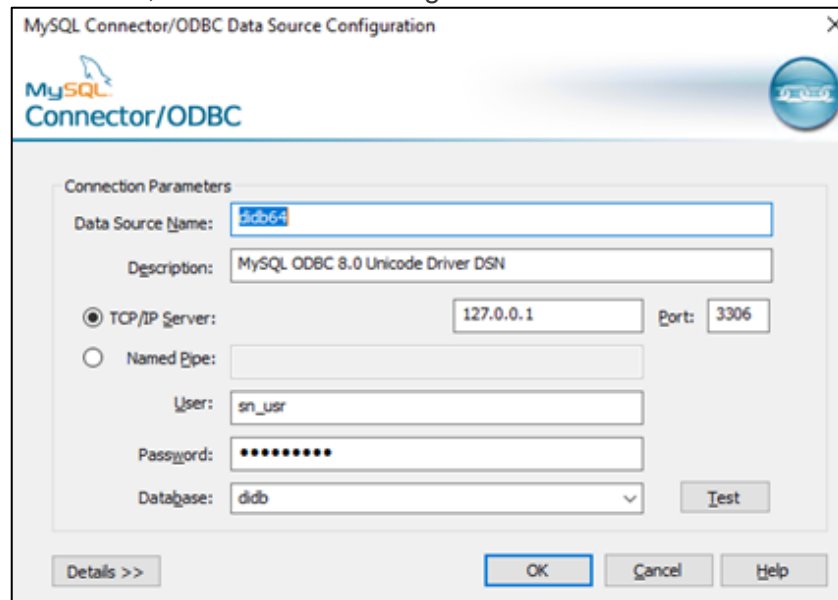


11. Similarly do for **idatadb** and **sordb**.
12. Do the below modifications as shown in ODBC 64 bit (replace localhost with the Remote MySQL Server IP address).



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 **idatadb64** and **sordb64**.

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:

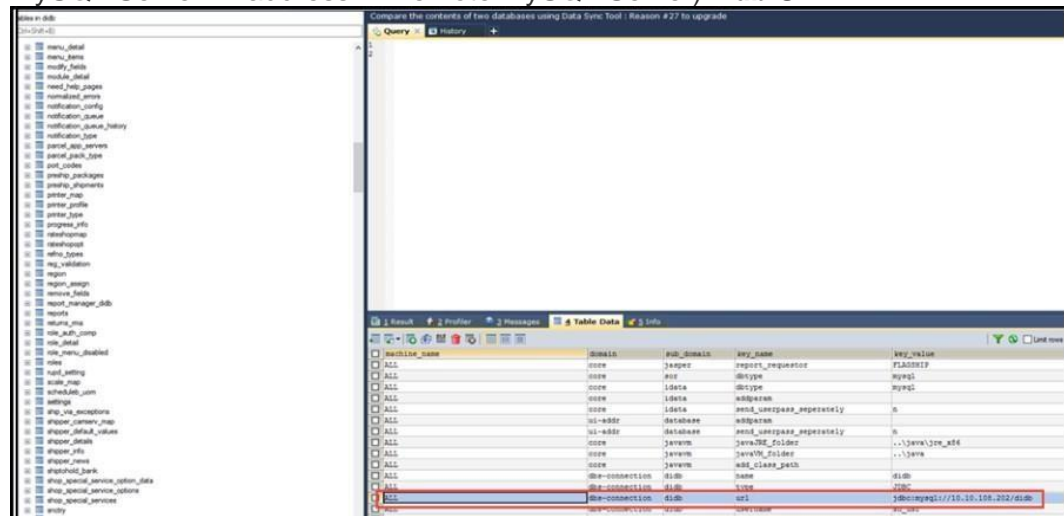
checkver.ini

purge.ini

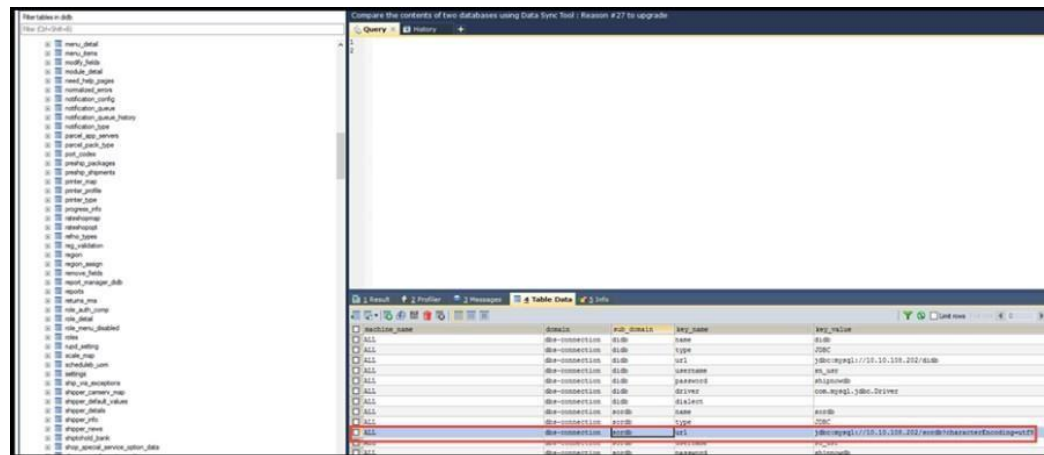
tracking.ini

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

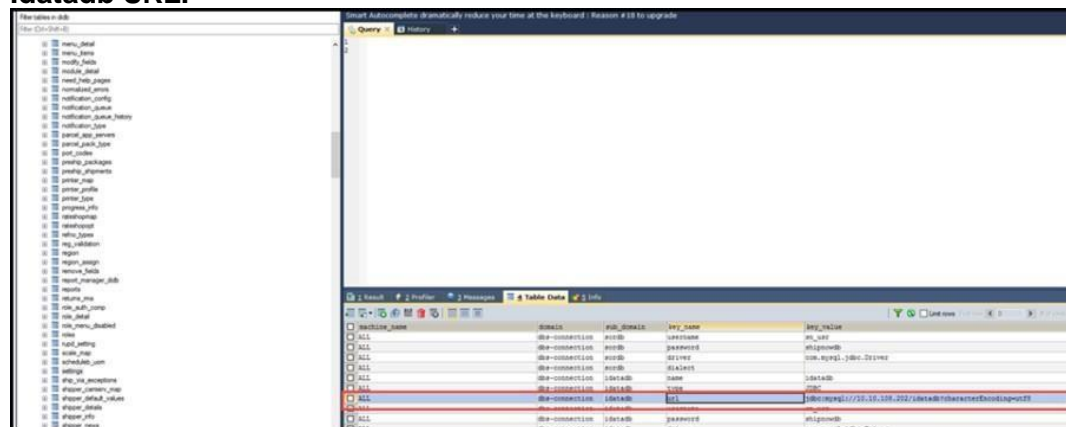
17. Do the below changes in **didb.settings** (replace localhost and provide Remote MySQL Server IP address in Remote MySQL Server)**Didb URL:**



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)

e2open Global Parcel Location: [US Smoke Test Loc](#) Ship Date: [01/31/2024](#) administrator

Ship Track My Profile System Workstation UCM Help

System / Parcel App Servers

Page 1 of 4

Location ID Location Name SEARCH

Global Settings

- Add Location
- Delete Location
- Corporate DSN
- CloseConfig
- Custom Data Mapping
- E2NET Watermill Integration
- Tracking Module Export Carriers
- Control Tower Integration
- Dangerous Goods Data
- Dangerous Goods Packing Types
- Configurable Business Rules Modul
- 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

Parcel Server	Parcel Web Host	Output Directory
localhost	http://localhost	C:\Program Files (x86)\Kewill\Flagship\WebGUI\outpu

Displaying rows 1 to 1 of 1

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

dev8025.dev.e2open.com dev8015.dev.e2open.com dev8010 dev8012.dev.e2open.com

File Edit View Query Database Server Tools Scripting Help

Navigator SQL File 1

SCHEMAS

notification_queue
notification_queue_j
notification_type
parcel_app_servers
parcel_data_import
parcel_pack_type
payer_type
port_codes
preship_packages
preship_shipments
printer_map
printer_profile
printer_type
progress_info
rateshopmap
rateshopopt
refno_type
reg_validation
region

1 * SELECT * FROM didb.parcel_app_servers;

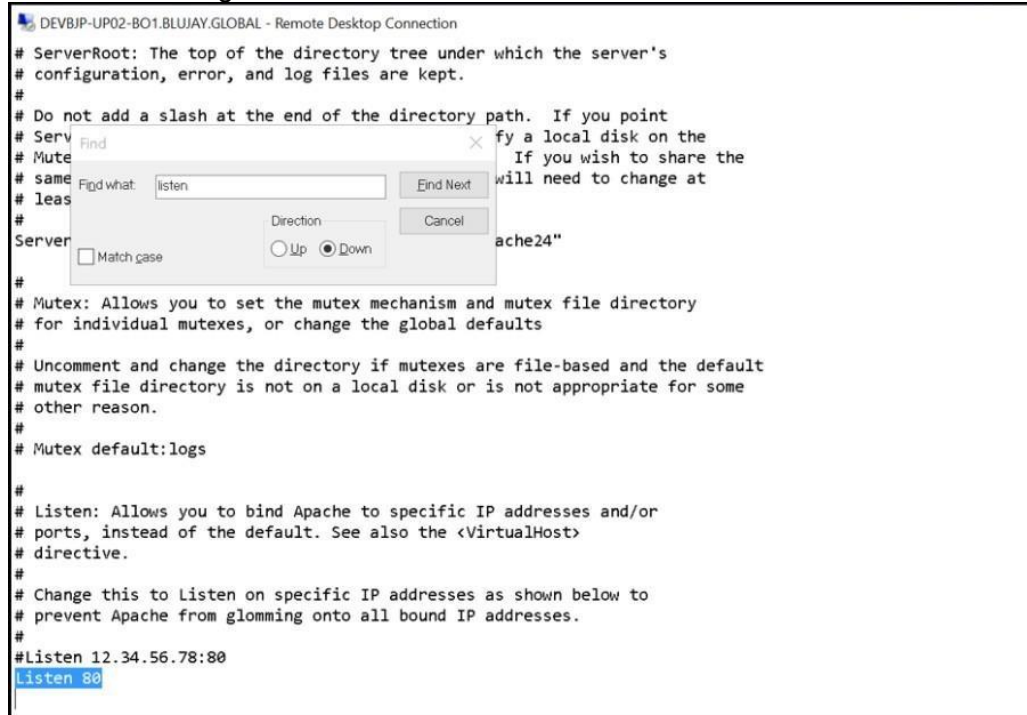
Result Grid Filter Rows

parcel_server	parcel_web_host	output_dir	url	url_service_path	registered_serial_no	registered_system_type
localhost	http://localhost	C:\Program Files (x86)\Kewill\Flagship\WebGUI\outpu	http://dev8012.dev.e2open.com:8103/LACD_anc	http://dev8012.dev.e2open.com:8103/LACD_anc	FA1C24PDP7CIPDD7	Test

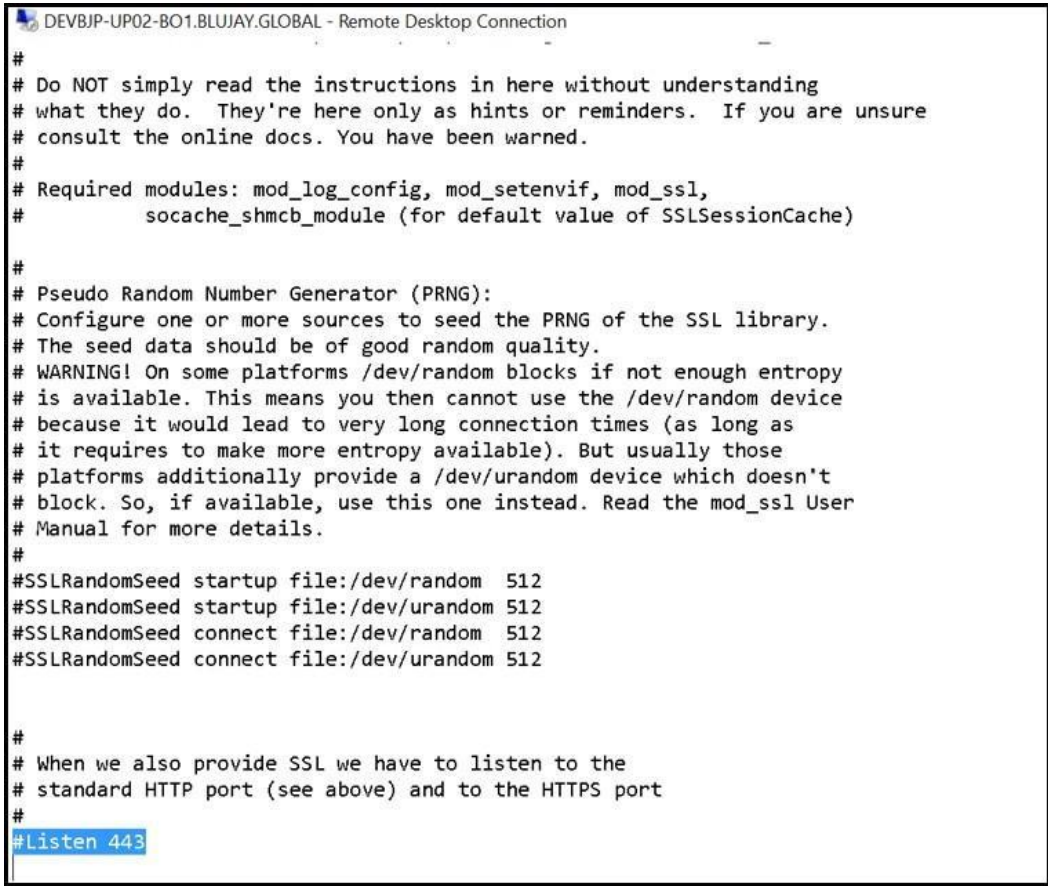
After making all the changes Restart MySQL Server in Application Server.

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



DEVBJP-UP02-BO1.BLUJAY.GLOBAL - Remote Desktop Connection

```
#
# 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.

Post Installation Tasks

Configuring 64bit DSN

Steps to add 64bit DSN:

- Open command prompt as administrator.
- Navigate to the installer path. Navigate to.....\ThirdParty\MySQL folder (Example: C:\Parcel24.1.0_INST_4769\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 . . .
```

Update Password to Bcrypt

1. For TM-Parcel version 23.3.0 and above, the encryption algorithm of the stored password has changed from md5 to Bcrypt to enhance the security of the password during transmission as well as storage. Therefore, all the existing passwords must be updated.
2. To update the password of all existing users except for built-in users, please use "Update_Password_To_Bcrypt.zip" package. If you don't update the passwords of all the existing users, they won't be able to log-in the application.

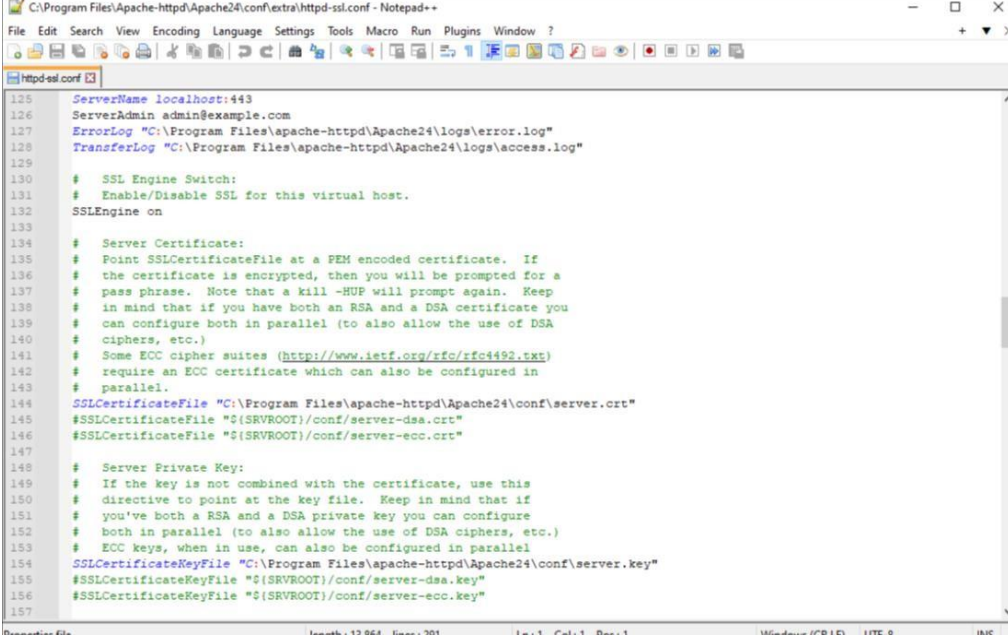
Note:- Built-in user's (administrator, enterprise, application, holdship and system_api_user) passwords will be automatically encrypted and updated during the upgrade process.

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:

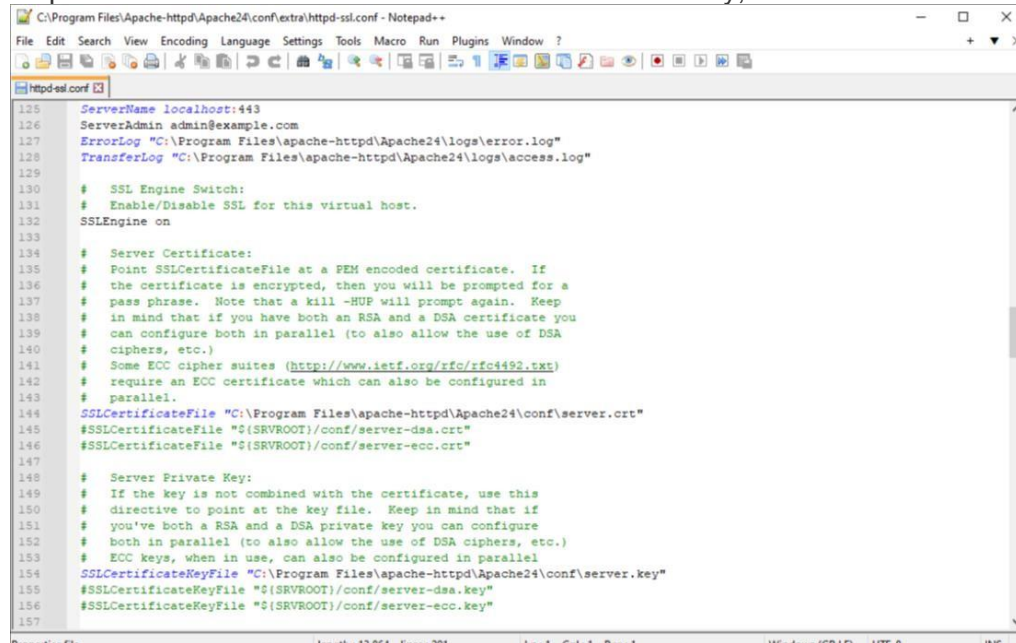


```

125 ServerName localhost:443
126 ServerAdmin admin@example.com
127 ErrorLog "C:\Program Files\apache-httpd\Apache24\logs\error.log"
128 TransferLog "C:\Program Files\apache-httpd\Apache24\logs\access.log"
129
130 # SSL Engine Switch:
131 # Enable/Disable SSL for this virtual host.
132 SSLEngine on
133
134 # Server Certificate:
135 # Point SSLCertificateFile at a PEM encoded certificate. If
136 # the certificate is encrypted, then you will be prompted for a
137 # pass phrase. Note that a kill -HUP will prompt again. Keep
138 # in mind that if you have both an RSA and a DSA certificate you
139 # can configure both in parallel (to also allow the use of DSA
140 # ciphers, etc.)
141 # Some ECC cipher suites (http://www.ietf.org/rfc/rfc4492.txt)
142 # require an ECC certificate which can also be configured in
143 # parallel.
144 SSLCertificateFile "C:\Program Files\apache-httpd\Apache24\conf\server.crt"
145 #SSLCertificateFile "${SRVROOT}/conf/server-dsa.crt"
146 #SSLCertificateFile "${SRVROOT}/conf/server-ecc.crt"
147
148 # Server Private Key:
149 # If the key is not combined with the certificate, use this
150 # directive to point at the key file. Keep in mind that if
151 # you've both a RSA and a DSA private key you can configure
152 # both in parallel (to also allow the use of DSA ciphers, etc.)
153 # ECC keys, when in use, can also be configured in parallel
154 SSLCertificateKeyFile "C:\Program Files\apache-httpd\Apache24\conf\server.key"
155 #SSLCertificateKeyFile "${SRVROOT}/conf/server-dsa.key"
156 #SSLCertificateKeyFile "${SRVROOT}/conf/server-ecc.key"
157
  
```

4. Repeat Step 2.

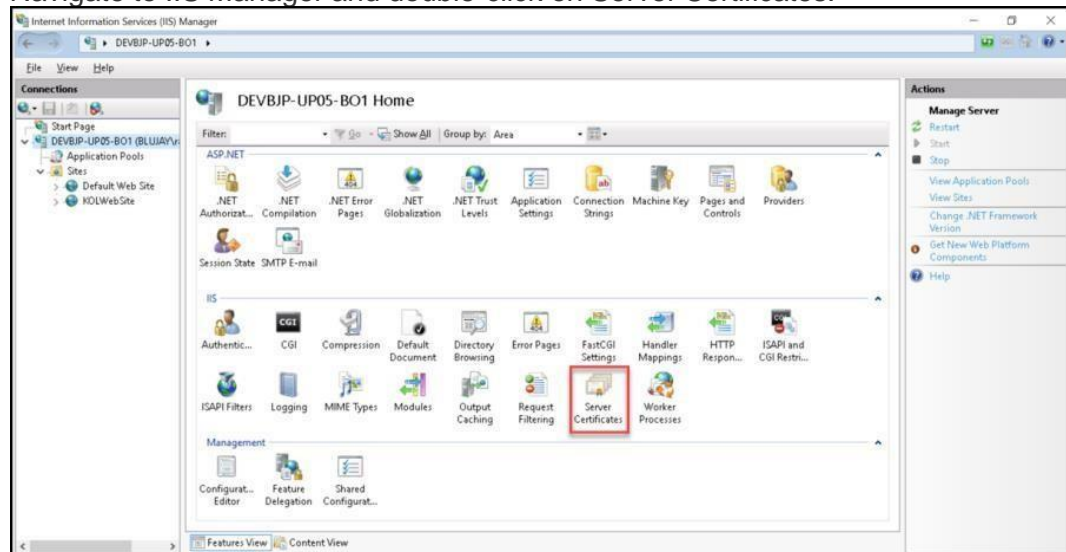
5. Search for the word 'SSLCertificateKeyFile' and replace the <Certificate key file> as per the certificate received from certification authority, as shown below:



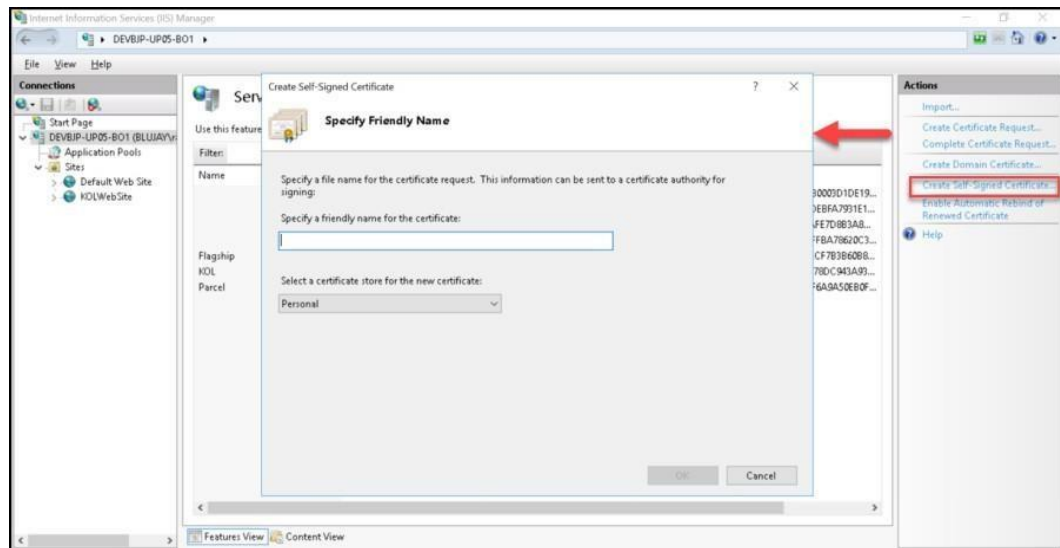
6. Restart Apache2.4 Service.

Enabling HTTPS on IIS Server

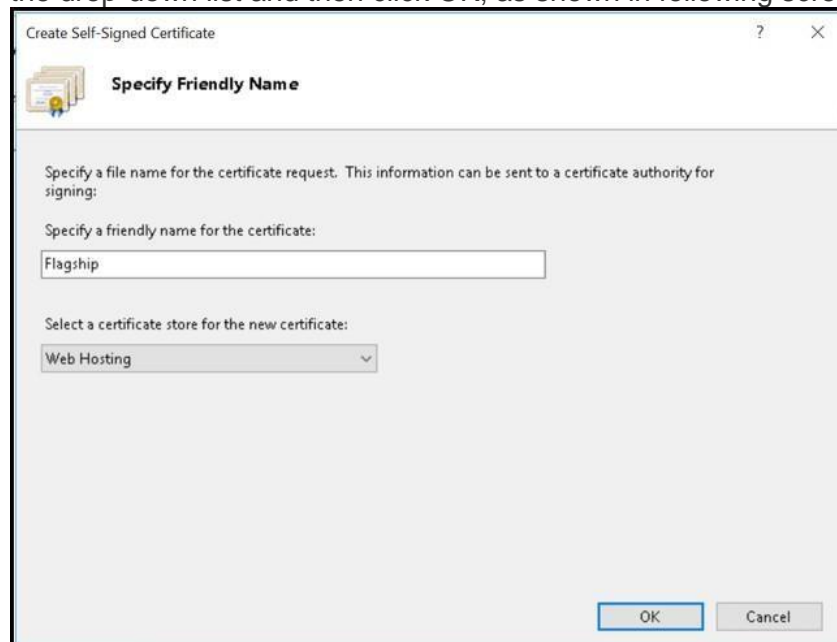
1. Navigate to IIS Manager and double-click on Server Certificates.



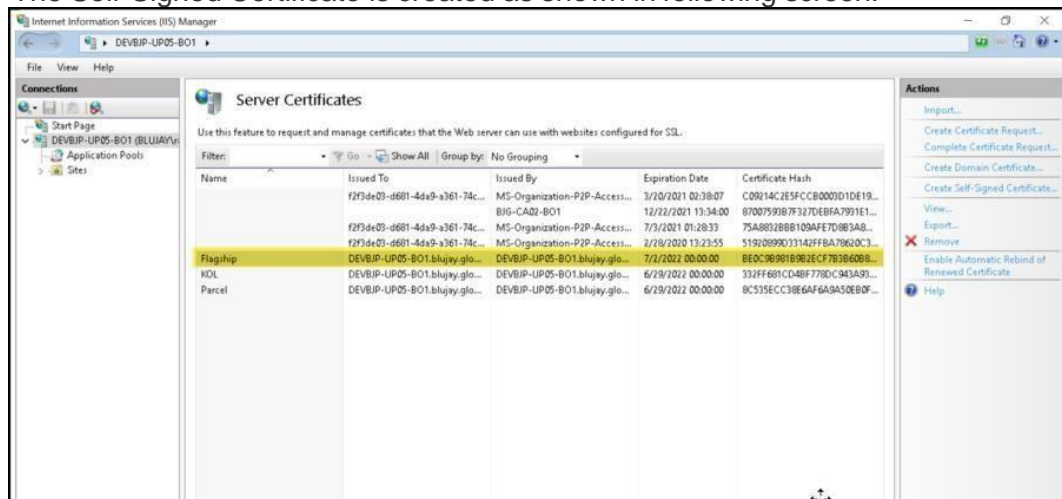
2. In the Actions panel, click **Create Self-Signed Certificate...** The Create Self-Signed Certificate dialog box appears, as shown in following screen.



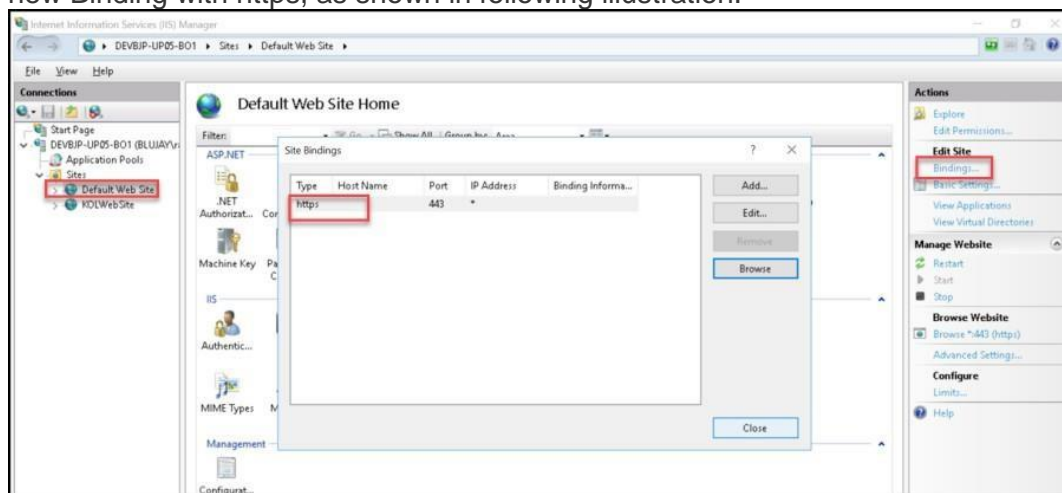
3. Specify a friendly name for the certificate in the provided field (For example: Flagship) and select a certificate store for the new certificate (Web Hosting) from the drop-down list and then click OK, as shown in following screen.



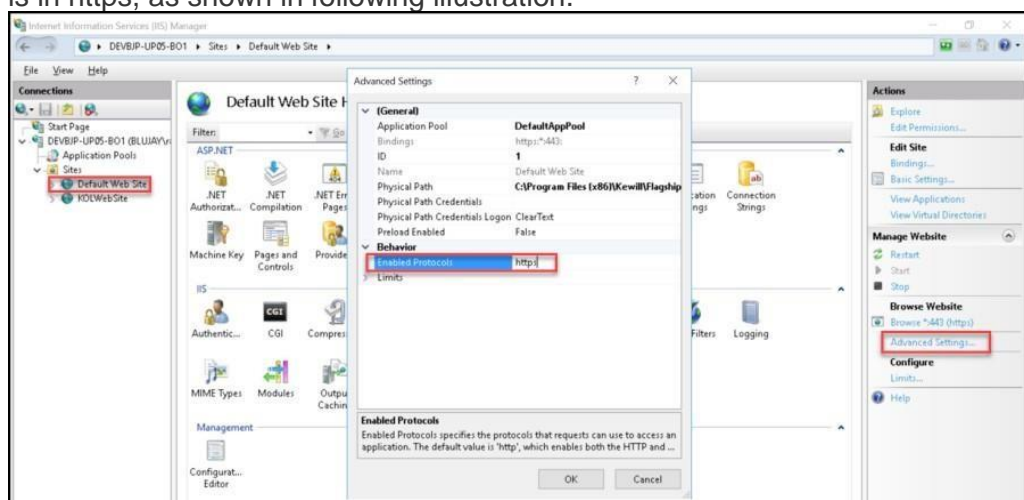
The Self-Signed Certificate is created as shown in following screen.



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.

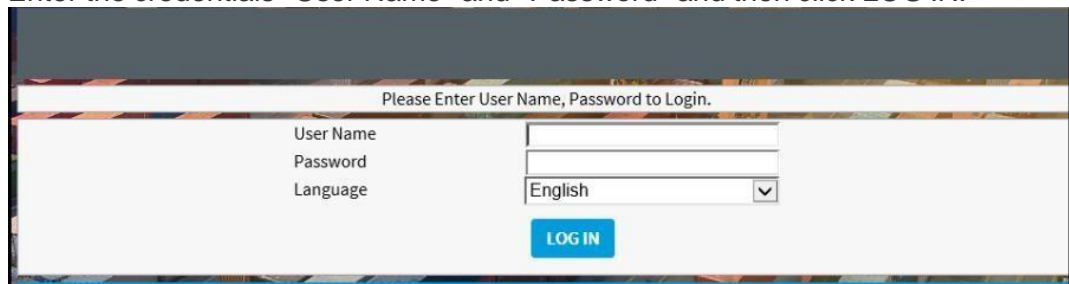
```
#If the pem file exists in a different folder then provide full path for the PEM file
#Ex:C:\certificates\ucm.pem (local path)
#\<machinename\IP>\certificates\ucm.pem (remote path)
pemFilePath=C:\Program Files (x86)\Kewill\Flagship\WebGUI\ucm\internal\ucm.pem
pemPassPhrase=blujayucm
```

- Restart BluJayUCMServer Service.

Accessing the Parcel Application

To access the Parcel Application, follow these steps:

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



Importing UPS World Wide Validation Data after the Upgrade

The UPS Worldwide Validation (WWV) Distribution is a set of data files distributed monthly by UPS that a customer needs to import after the upgrade.

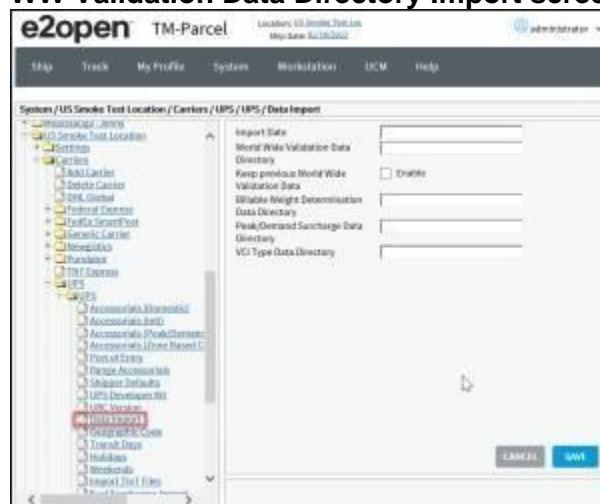
To import the UPS Worldwide Validation files, carry out the following steps:

- 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:\WWW_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 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

Save to import the files or click CANCEL to cancel out of this screen. **Parcel UPS WW Validation Data Directory Import screen**



Note: If the parcel is integrated with CBRM/AES/XML Interface, then you have to

upgrade OL to v24.1.0.2 and Plugin Installer to v 24.1.0.1 You can find the upgrade instructions for OL and Plugin Installer in respective installers.

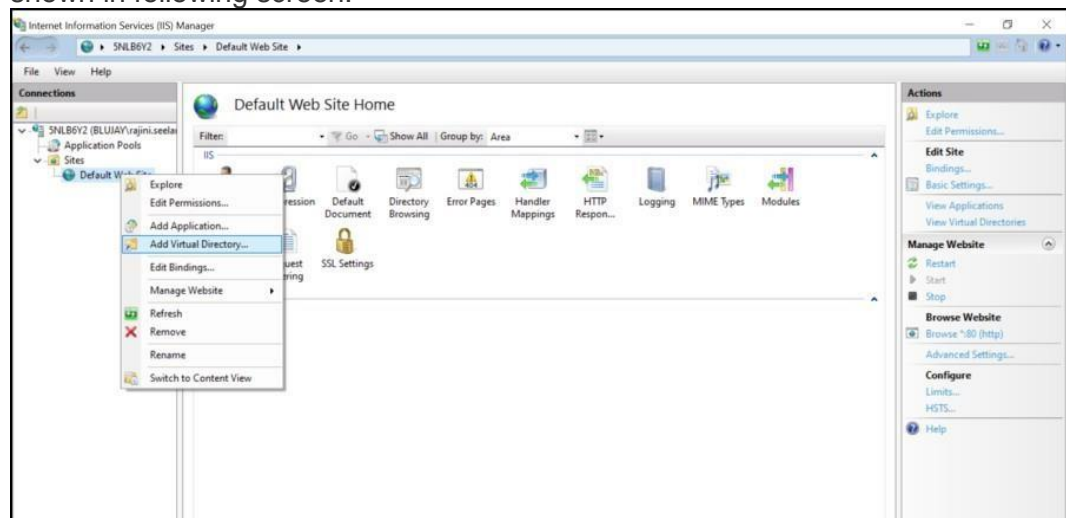
Add Update Virtual Directory in IIS

The Virtual Directory in IIS is used for viewing the labels and reports.

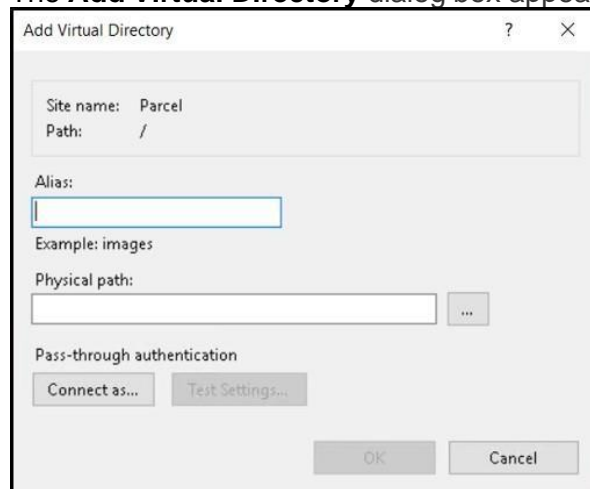
This section describes about to how add and update the virtual directory in IIS.

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.

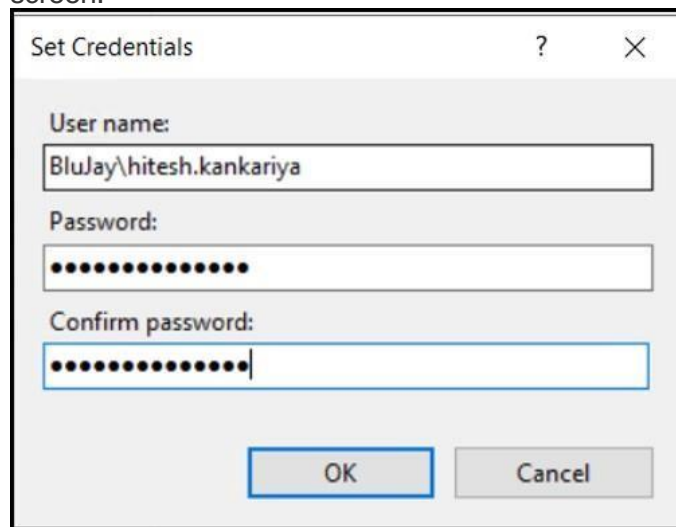


4. In **Alias:** field, enter "parceloptions".
5. In **Physical path:** field, click ... and browse for Parcel Artifact Folder Path. **For Example:** C:\Parcel Artifact Folder

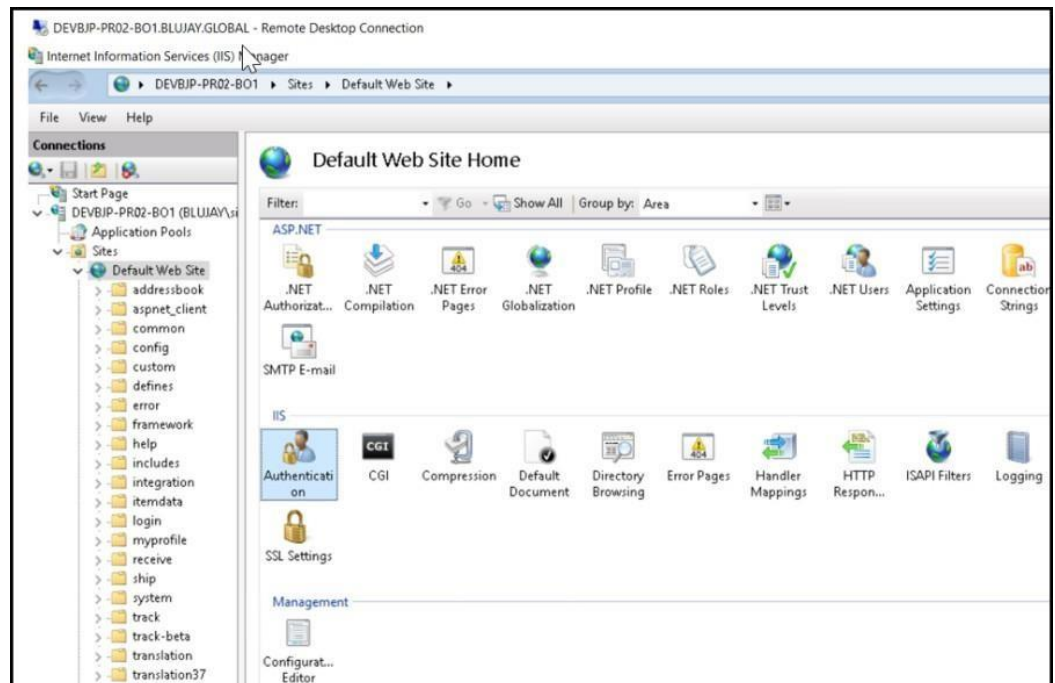
- Click Connect as...The Edit Anonymous Authentication Credentials dialog box appears, as shown in following screen.



- The Edit Anonymous Authentication Credentials dialog box, accept the default 'Specific user:' option and then click Set...
- The Set Credentials dialog box appears.
- In the Set Credentials dialog box, enter Username, Password and Confirm Password in the respective fields and then click OK, as shown in following screen.

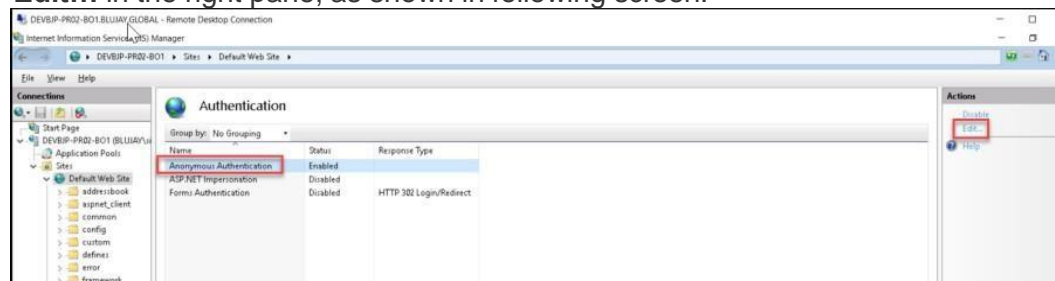


- Click OK in the Add Virtual Directory dialog box.
- Click Default Web Site and then double-click on **Authentication** on in the right-pane, as shown in following screen.



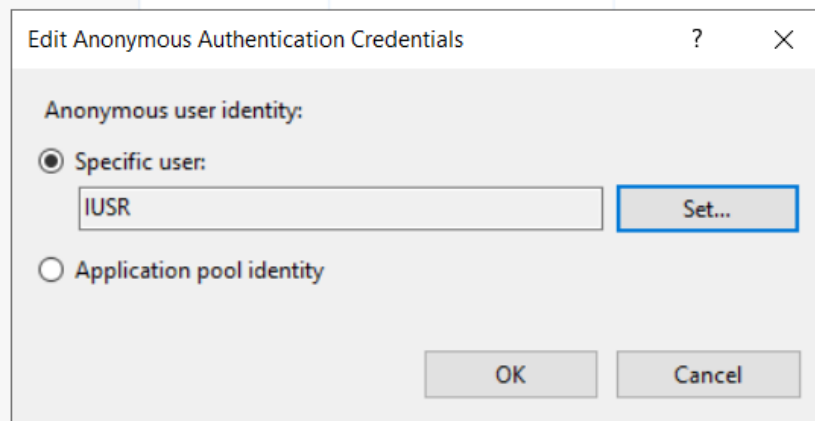
The Authentication screen displays.

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



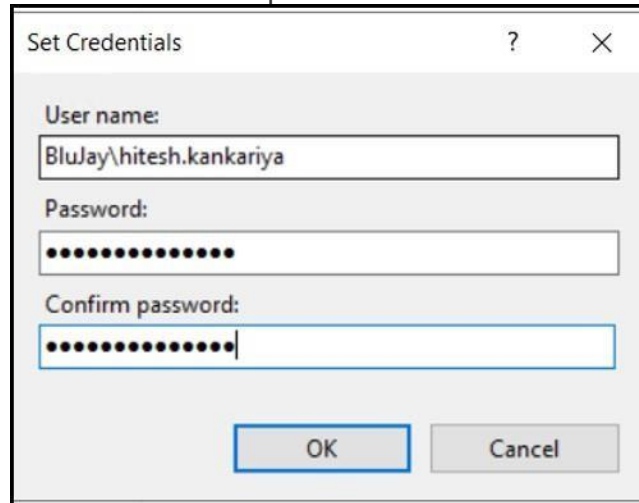
The Edit Anonymous Authentication Credentials dialog box appears.

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

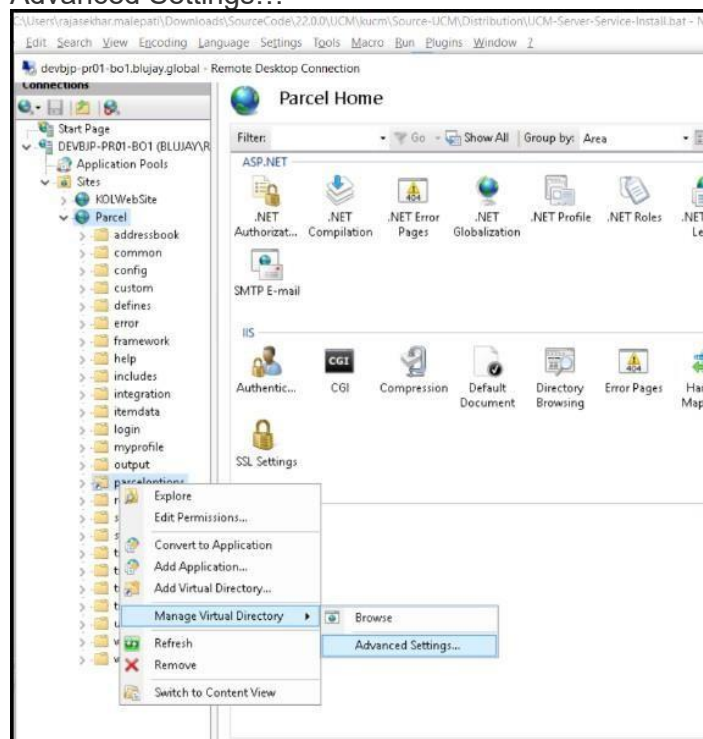



The Set Credentials dialog box appears.

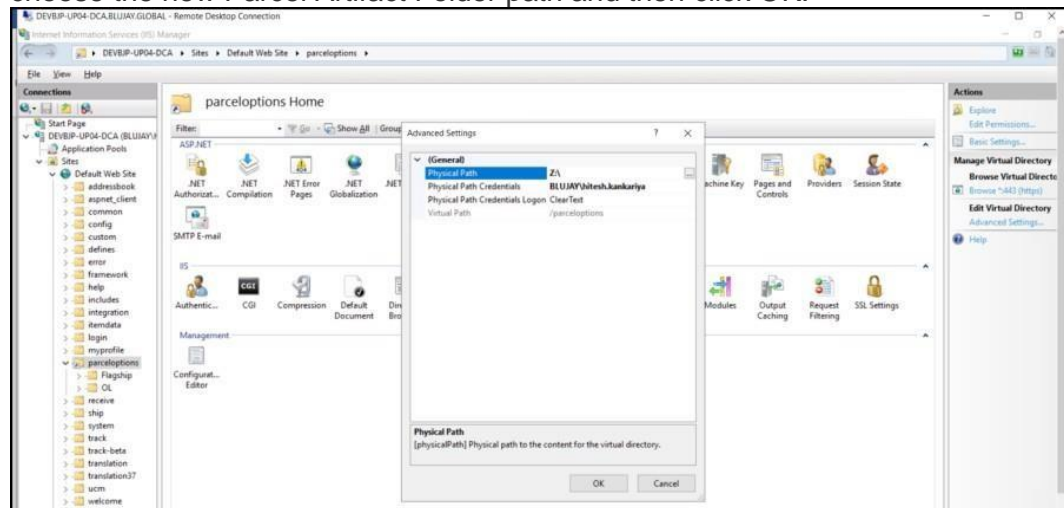
14. In the Set Credentials dialog box, enter Username, Password and Confirm Password in the respective fields and then click OK.



15. Click OK
16. Restart IIS Service. To update virtual directory in IIS, follow these steps:
17. Right-click on the created virtual directory, click Manage Virtual Directory > Advanced Settings...



18. In the Advanced Settings window, click  next to the *Physical Path* and choose the new Parcel Artifact Folder path and then click OK.



19. Restart IIS Service.

Moving Apache from one drive to other drive

To move Apache from one drive to another drive, follow these steps:

1. Stop Apache2.4 service.
2. Open command prompt with administrator privileges.
3. Navigate to the ..Apache-httpd\Apache24\bin folder (Ex: C:\Program Files (x86)\Apache-httpd\Apache24\bin)
4. Run **httpd.exe -k uninstall** command. The following message displays:
"The 'Apache2.4' service has been removed successfully".
5. Move 'Apache-httpd' folder from existing drive (Ex: C: to destination drive (Ex: E:
6. Again, go to command prompt and navigate to ..Apache-httpd\Apache24\bin folder (Ex: E:\Apache-httpd\Apache24\bin)
7. Run **httpd.exe -k install** command.
The following message displays:
"The 'Apache2.4' service is installed successfully".
8. Start Apache2.4 service.

Configuring Persistence XML File

As part of upgrade installation, we need to add e2netdb persistence unit in the persistence.xml file to support integration with UCM service and Watermill Connector service.

Steps to update Persistence XML File:

1. Go to <ArtifactLocationPath>\Flagship\ucm\java\META-INF folder.

2. Edit the persistence.xml file, to add below e2netdb persistence unit **after** `<persistence-unit name="com.kewill.ucm.upgrade">` end tag.

```
<persistence-unit name="com.kewill.ucm.e2netdb">
    <description>Transactional persistence unit for e2net db</description>
    <provider>org.hibernate.ejb.HibernatePersistence</provider>
    <class>com.kewill.ucm.watermillconnector.e2netdb.entities.ParcelManifestI
nfo</class>
    <class>com.kewill.ucm.watermillconnector.e2netdb.entities.ParcelManifestS
hipmentInfo</class>
    <class>com.kewill.ucm.watermillconnector.e2netdb.entities.ParcelPackageI
nfo</class>
    <exclude-unlisted-classes>true</exclude-unlisted-classes>
    <properties>
        <property name="javax.persistence.jdbc.driver"
value="com.mysql.jdbc.Driver"/>
        <property name="javax.persistence.jdbc.url"
value="jdbc:mysql://localhost:3306/e2netdb?autoReconnect=true&character
Encoding=UTF-8"/>
        <property name="javax.persistence.jdbc.user" value="sn_usr"/>
        <property name="javax.persistence.jdbc.password" value="shipnowdb"/>
        <property name="hibernate.dialect"
value="org.hibernate.dialect.MySQL5Dialect"/>

        <property name="hibernate.show_sql" value="false"/>
        <property name="hibernate.connection.release_mode"
value="AFTER_TRANSACTION"/>
        <property name="hibernate.connection.useUnicode" value="true" />
        <property name="hibernate.connection.charSet" value="UTF8" />
        <property name="javax.persistence.lock.timeout" value="5000"/>
        <!-- TODO: review the implications of using update with team -->
        <!-- <property name="hibernate.hbm2ddl.auto" value="update"/> -->
        <property name="hibernate.connection.provider_class"
value="org.hibernate.service.jdbc.connections.internal.C3P0ConnectionProvider"
/>

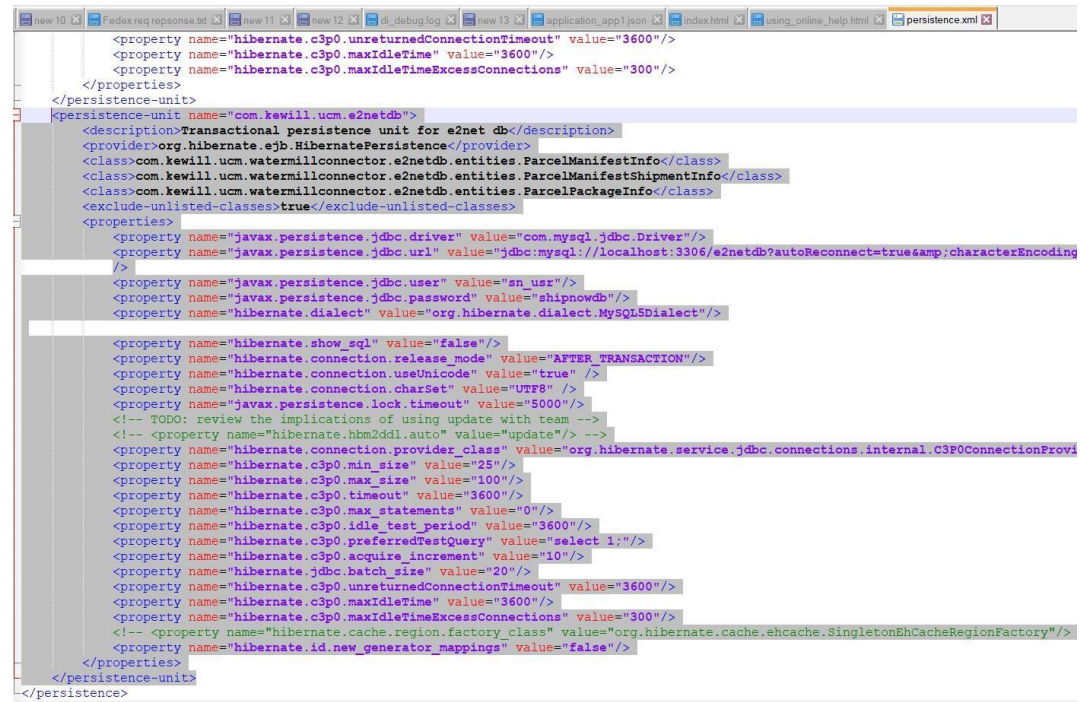
        <property name="hibernate.c3p0.min_size" value="25"/>
        <property name="hibernate.c3p0.max_size" value="100"/>
        <property name="hibernate.c3p0.timeout" value="3600"/>
        <property name="hibernate.c3p0.max_statements" value="0"/>
        <property name="hibernate.c3p0.idle_test_period" value="3600"/>
        <property name="hibernate.c3p0.preferredTestQuery" value="select 1;"/>
        <property name="hibernate.c3p0.acquire_increment" value="10"/>
        <property name="hibernate.jdbc.batch_size" value="20"/>
        <property name="hibernate.c3p0.unreturnedConnectionTimeout"
value="3600"/>
        <property name="hibernate.c3p0.maxIdleTime" value="3600"/>
        <property name="hibernate.c3p0.maxIdleTimeExcessConnections"
value="300"/>
        <!-- <property name="hibernate.cache.region.factory_class"
value="org.hibernate.cache.ehcache.SingletonEhCacheRegionFactory"/> -->
```

```

        <property name="hibernate.id.new_generator_mappings" value="false"/>
    </properties>
</persistence-unit>

```

Please refer to the screenshot attached below.



3. Save the persistence.xml file.
4. Restart the BluJayUCMServer.

dbdefines.php Changes

Unable to load Warehouse page

Add the below line in file <ArtifactsAndLogs>\Flagship\WebGUI\defines\dbdefines.php.

```
define( 'PERIPHERAL_AGENT_URL', "https://localhost:9070" );
```

Save and Close the file and try to reload the warehouse page.

Reconfigure SSL Settings

Encrypt DB Communication

Note

These steps are applicable for TM-Parcel customers upgrading to 24.1.0 from SSL enabled versions (TM Parcel using MySQL Secure Connection). Please update the passwords of all the existing users before enabling SSL. See Update Password to Bcrypt section for details.

1. On Application Server, navigate to the parcel configuration file (shipnow.ini) and open the shipnow.ini in a text editor.
For Example:
<Parcel Artifact Folder>\Flagship\bin\shipnow.ini
2. Turn on encryption as follows:
ENCRYPT_DB_COMMUNICATION=ENABLE_ENCRYPTION=y
3. Reconfigure SSL settings in ODBC Connector. Refer *Configuring SSL Settings in MySQL Connector/ODBC*.

Update SSL Settings

Note

These steps are applicable for TM-Parcel customers upgrading to 24.1.0 from SSL enabled versions (TM Parcel using MySQL Secure Connection).

1. Navigate to the <Parcel Artifact Folder>/Flagship/java/conf/configuration.properties file and update the useSSL and requireSSL fields as 'true'.
 - useSSL:true
2. Navigate to the C:\ProgramData\MySQL\MySQL Server 8.0\my.ini and update 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
```

Add Custom Configurations from Previous Version my.ini file

Note

This task is applicable for all upgrade scenarios.

Reconfigure custom configurations present in previous version **my.ini** (back up file) file into the new version my.ini file at
C:\ProgramData\MySQL\MySQL Server 8.0.

Restart Services

Enable and restart the following services:

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

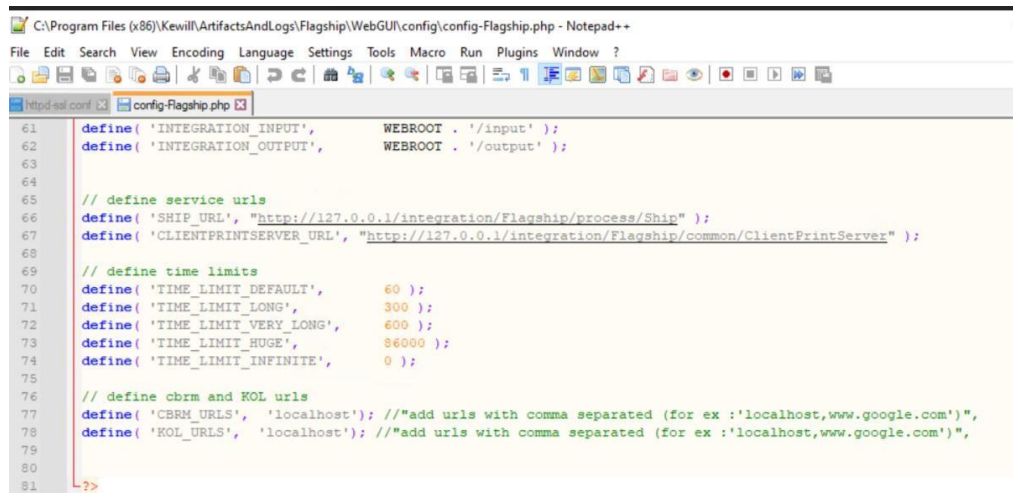
Converting MyISAM to InnoDB

For version 23.2.0 and above, TM-Parcel installs fresh MySQL 8.0.32 version. If you have DB engine as InnoDB in your previous version of TM-Parcel, follow these steps:

1. Convert MYISAM to InnoDB. Refer *TM-Parcel Instructions Document Converting MyISAM to InnoDB* document for details.
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, and reset the DB engine type from MyISAM to InnoDB. For example:
 - a. default-tmp-storage-engine=InnoDB
 - b. default-storage-engine=InnoDB

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



```

61 define( 'INTEGRATION_INPUT',      WEBROOT . '/input' );
62 define( 'INTEGRATION_OUTPUT',     WEBROOT . '/output' );
63
64
65 // define service urls
66 define( 'SHIP_URL', "http://127.0.0.1/integration/Flagship/process/Ship" );
67 define( 'CLIENTPRINTSERVER_URL', "http://127.0.0.1/integration/Flagship/common/ClientPrintServer" );
68
69 // define time limits
70 define( 'TIME_LIMIT_DEFAULT',      60 );
71 define( 'TIME_LIMIT_LONG',        300 );
72 define( 'TIME_LIMIT_VERY_LONG',   600 );
73 define( 'TIME_LIMIT_HUGE',        86000 );
74 define( 'TIME_LIMIT_INFINITE',    0 );
75
76 // define cbrm and KOL urls
77 define( 'CBRM_URLS', 'localhost' ); //add urls with comma separated (for ex : 'localhost,www.google.com')
78 define( 'KOL_URLS', 'localhost' ); //add urls with comma separated (for ex : 'localhost,www.google.com')
79
80
81

```

Additional Optional Steps

Setting up a Corporate Address Book

Overview

You can import Personal and Global Address Books as CSV files directly into the Parcel UI using the Import function on the Address Book screen, as well as adding addresses to these address books directly from the UI.

However, for security reasons, a Corporate Address Book must be set up directly in the MySQL database that Parcel uses for this purpose. You can do this by using SQLyog or another database administration tool to import the Corporate Address Book in the form of a CSV file into the Corporate Address Book table in the database.

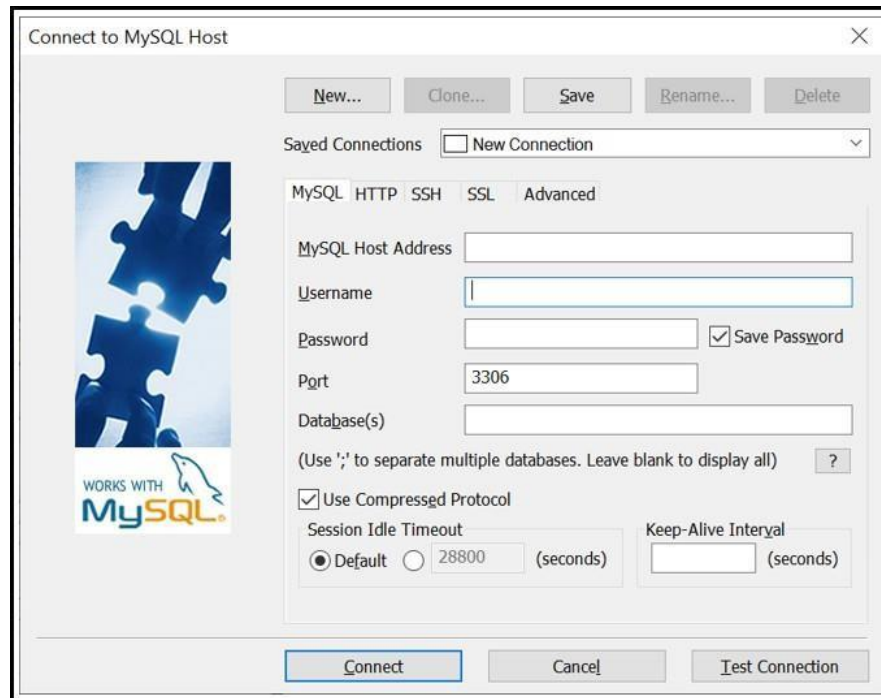
The following example procedure describes how to set up a Corporate Address book using SQLyog with a sample CSV file. Follow a similar procedure with other database administration tools.

Note: You can now configure.

Corporate Address Book setup - example procedure

To set up a Corporate Address Book in Parcel:

1. Create the database table required for the Corporate Address Book using the database script provided. For additional information on this, see the following Help topic in the Parcel User Guide (Online Help): "Corporate DSN".
2. Create your Corporate Address Book using Excel (suggested) or some other application that lets you create CSV files. Refer to the field mapping section of the Import tab on the Parcel Address book screen. Create a header row with column headings that match those on the Address Book screen. **Note:** You do not need to create columns corresponding to all the Address Book fields. See the Address Book topics in the Parcel Help for more information on creating and using address books.
3. With SQLyog open, connect to the Parcel MySQL database. Enter the IP address of the Parcel instance in the **MySQL Host Address** field, and any other required information, and then click **Connect**.



Connect to MySQL Host

New... Clone... Save Rename... Delete

Sayed Connections ☐ New Connection

MySQL HTTP SSH SSL Advanced

MySQL Host Address

Username

Password ☒ Save Password

Port 3306

Database(s)

(Use ';' to separate multiple databases. Leave blank to display all) ?

☒ Use Compressed Protocol

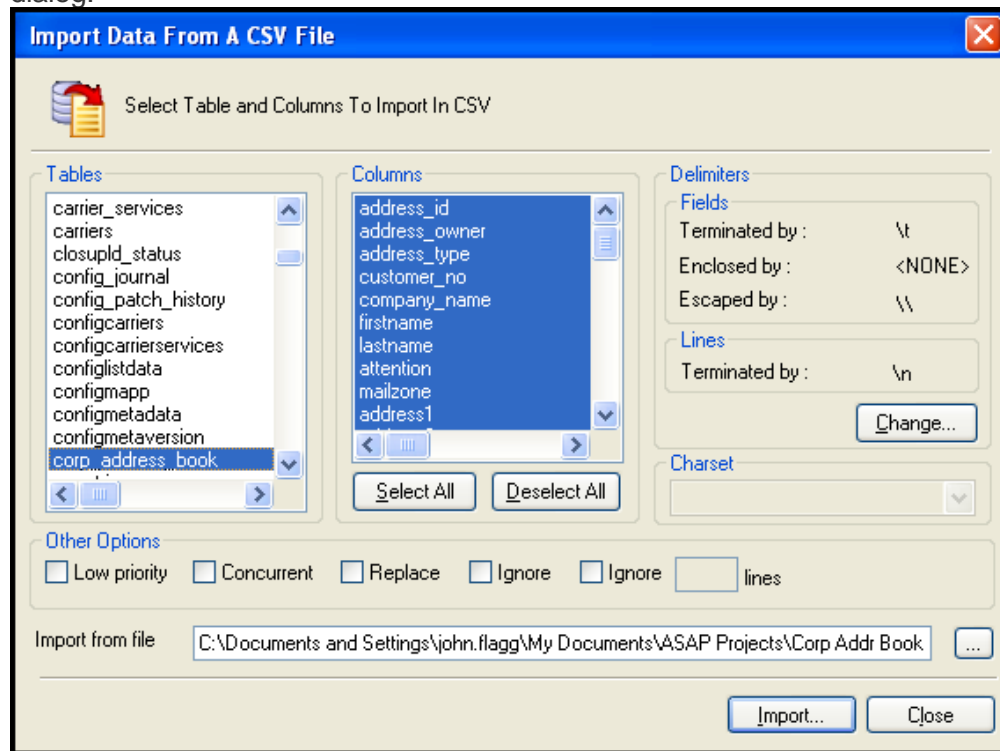
Session Idle Timeout ☒ Default ☐ 28800 (seconds)


Keep-Alive Interval (seconds)

Connect Cancel Test Connection

4. In the left panel, expand the sordb database portion of the tree.
5. Find the corp_address_book table in the list, select this table, and then select Table > View Data to ensure that the table is not already populated with address book data.

6. Select Table > Import data from CSV to open the Import Data From a CSV File dialog.



7. Ensure that the corp_address_book table is selected in the Tables list, and then click  to select the CSV file to import. **Note:** All columns in the Table are selected by default. If your CSV file is correctly formatted (with blank columns indicated), you can use this setting. The fields with data will be populated correctly and those with no data will be left blank.
8. Click Import, and then select Table>View Data to ensure that the corp_address_book table populated correctly with your Address Book data.
9. Open the Corporate Address book in Parcel and verify that the values for the fields display correctly. You can now use the Corporate Address book as you would any other address book. (For information on this, see the Address Book topics in the Parcel Help.) **Note:** When you select an entry from the Corporate Address Book, the text in the Address book fields will be "grayed out," indicating that the fields are not editable directly. You must make any desired changes in the original CSV file, and then re-import it.

Checking Settings

When upgrading from a previous version of Parcel, you should check your settings both before and after running the installation process, especially if you want to retain existing settings. To check Parcel settings, use SQLyog or another database management tool to display the contents of the didb.settings table in the MySQL database. You can use queries to check settings for specific domains and subdomains. With the didb database selected, use the following form:

```
select * from settings where domain = '<domain_name>' and sub_domain
```

= '<subdomain_name>'

For example, to find settings for the JavaVM (see previous section), use:

select * from settings where domain = 'core' and sub_domain = 'javavm'

To find settings for the Database Service Connection (see previous section), use:

select * from settings where domain = 'dbs-connection'

Supporting UCM Integration on HTTPS

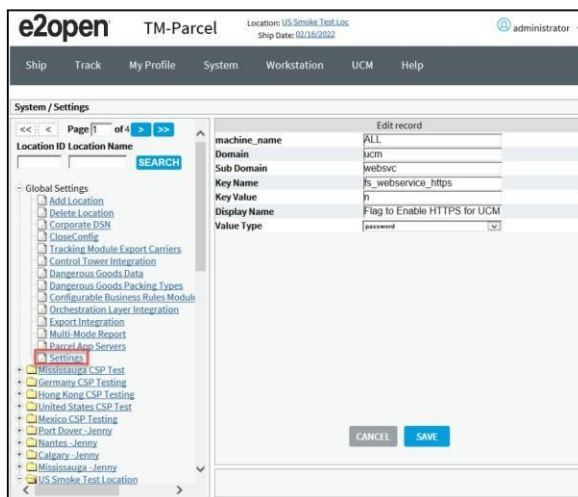
To support UCM Integration on HTTPS, update 'fs_webservice_https' under Global Settings > Settings

- 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 settings displays, as shown in the following screen.



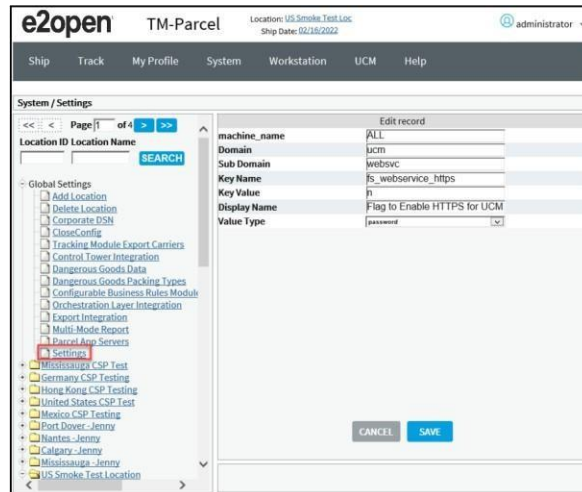
Converting UCM from HTTPS to HTTP

Note: Make sure Parcel is in http.

1. 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>\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.

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:

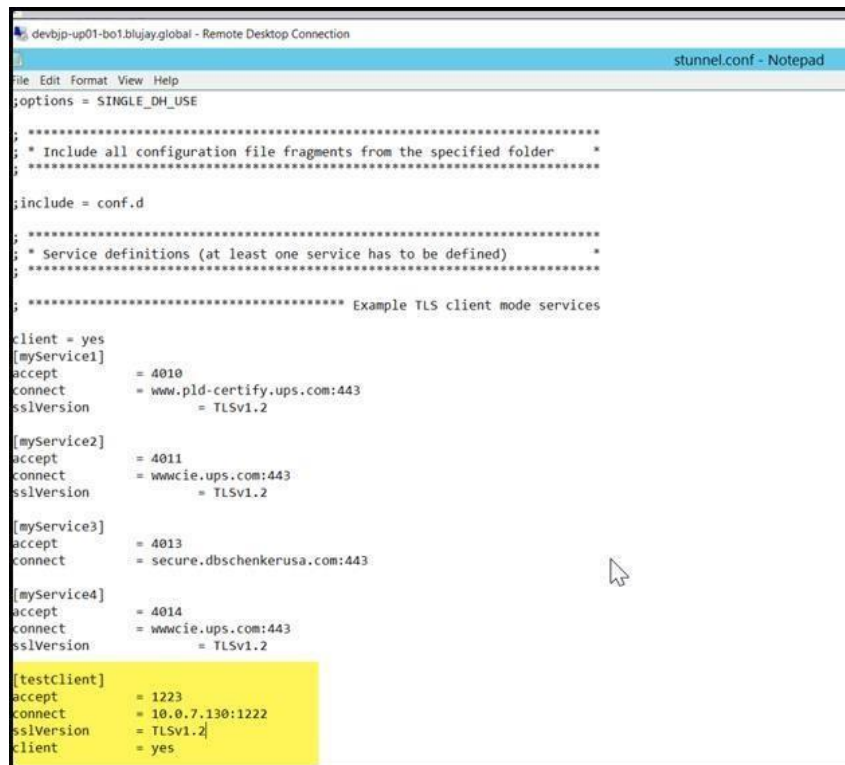
- Configuring the Stunnel Settings in Client Machine
- Configuring the Stunnel Settings in Server Machine

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:

- 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
- In the stunnel.conf file, add below service, as shown in following screen.
testClient accept = 1223
connect = \[Server IP Address\]:1222sslVersion = TLSv1.2
client = yes



```

devbjp-up01-bo1.blujay.global - 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     = 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
[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.
testServer
client = 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         = www.ie.ups.com:443
sslVersion      = TLSv1.2

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

[myService4]
accept          = 4014
connect         = www.ie.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

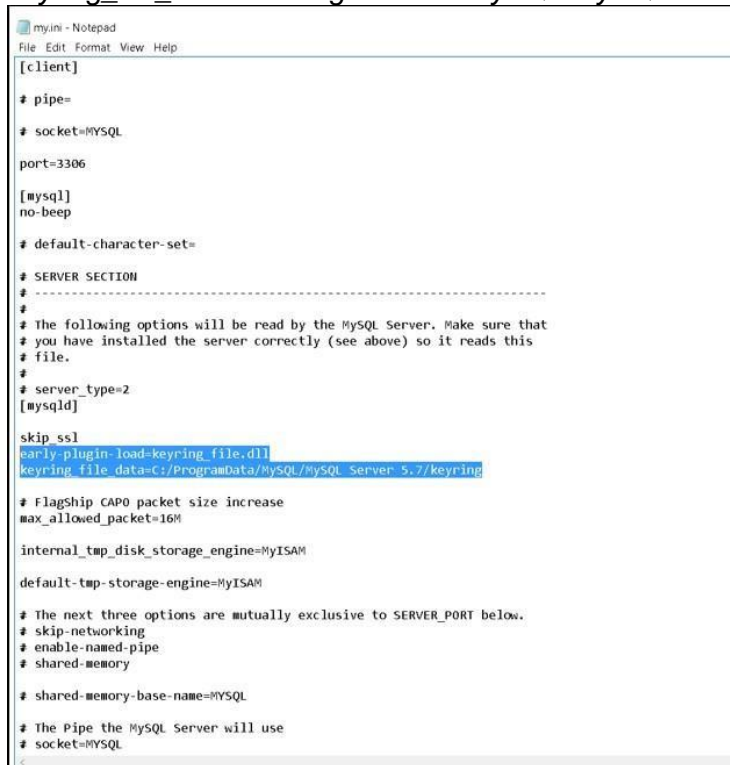
This section describes how to configure Transparent Data Encryption (TDE) in MySQL Server.

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 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.

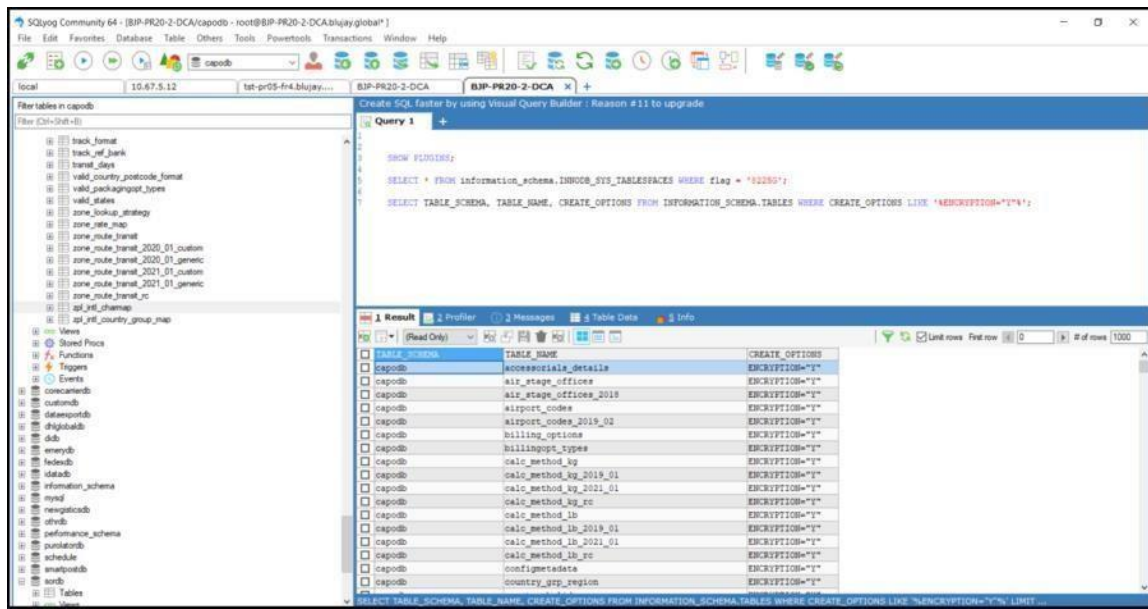
Execute the below command:

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:

1. 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:

2. 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';

3. 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:

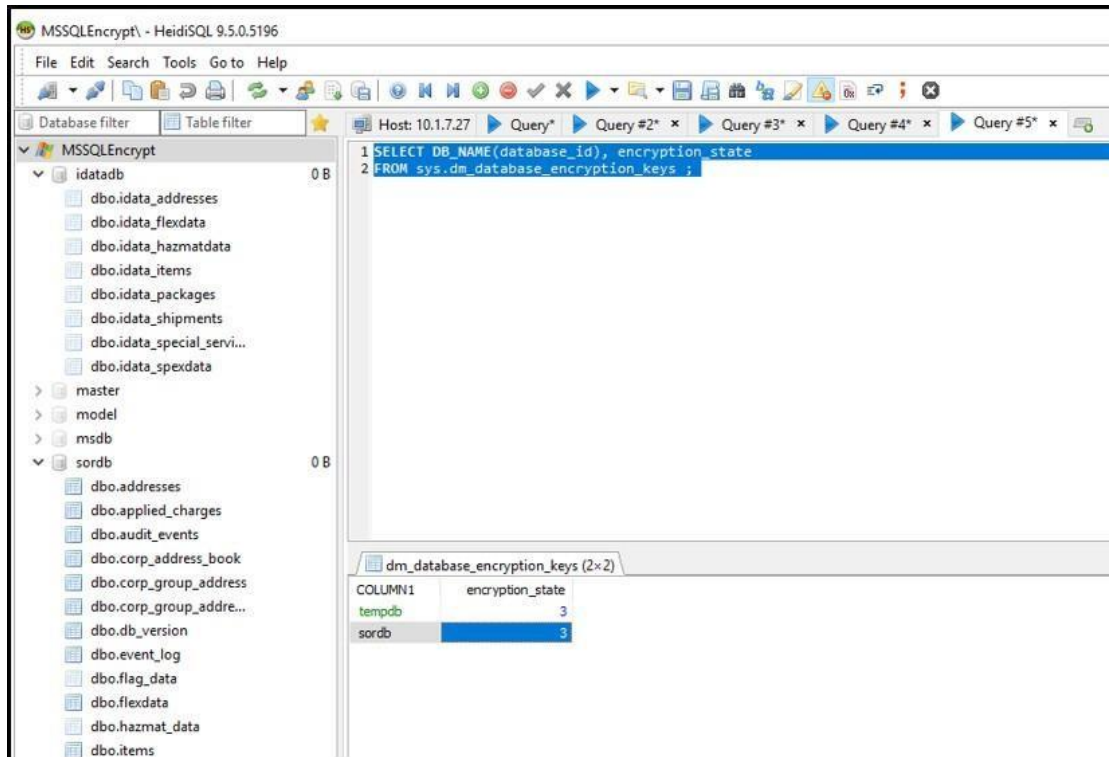
USE Master; CREATE CERTIFICATE '<TDECert>'

WITH SUBJECT = '<TDE Certificate>';

4. Create a Database Encryption KeyNow, 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;
5. Backup the Private Encryption Key and CertificateNow, 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');
6. Turn TDE OnFinally, 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.

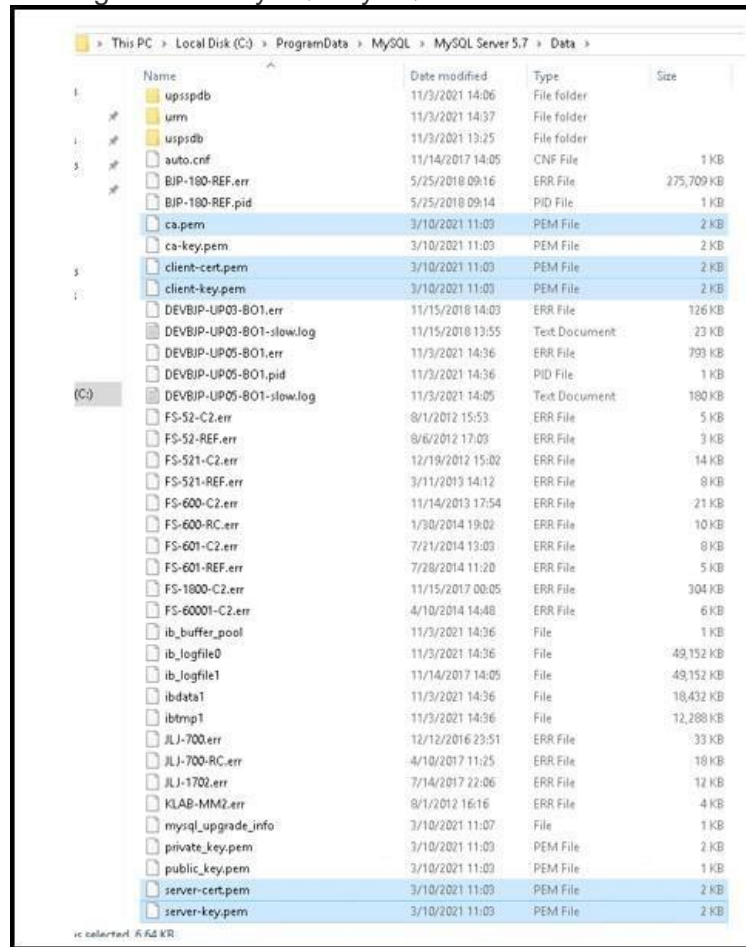
In-order to set up encrypted connections, configuration changes are required to both the database server and, in the Application (Modules).

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).
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
```

- Restart the MySQL Service.

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

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=client-cert.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.
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
requireSSL	Set this field to allow the connection between MySQL and the Services. Valid values are: <ul style="list-style-type: none"> • true • false <p>The 'requireSSL' settings should be 'true' at Java Services and SSL settings should be configured at MySQL.</p>
verifyServerCertificate	Set this field to verify the MySQL Server certificate. Valid values are: <ul style="list-style-type: none"> • true • false <p>If verifyServerCertificate is set to true, then you need to configure trustCertificateKeyStoreUrl and trustCertificateKeyStorePassword fields.</p>
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

Fields	Description
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>
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>

String	Description
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\client-cert.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 then 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 shown in the next step (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 'SSL' tab is selected. The 'Connection Parameters' section shows 'Data Source Name' as 'didb', 'Description' as 'MySQL ODBC 8.0 Unicode Driver DSN', 'TCP/IP Server' as '127.0.0.1', 'Port' as '3306', 'User' as 'sn_usr', 'Password' as masked, and 'Database' as 'didb'. The 'SSL' tab contains fields for 'SSL Key' (D:\SSL_keys\client-key.pem), 'SSL Certificate' (D:\SSL_keys\client-cert.pem), 'SSL CA File' (D:\SSL_keys\ca.pem), 'SSL CA Path' (D:\SSL_keys), 'SSL Cipher' (DHE-RSA-AES128-GCM-SHA), 'SSL Mode' (dropdown), and 'RSA Public Key' (empty). There are also checkboxes for 'Disable TLS Version 1', 'Disable TLS Version 1.1', and 'Disable TLS Version 1.2'. The 'Details <<' button is highlighted.

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>

Fields	Description
SSL CA File	Enter the Certificate Authority (CA) certificate file in PEM format. For Example: <SSL Certificates Path>\<ca.pem>
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-RSA-AES128-GCM-SHA256:AES128-SHA". This should be also used in Application (Modules).

6. Click OK.

Generating a Self-Signed SSL Certificate using OpenSSL

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.**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>

```

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
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.

You will be prompted for export password, which you can leave blank.

6. 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:

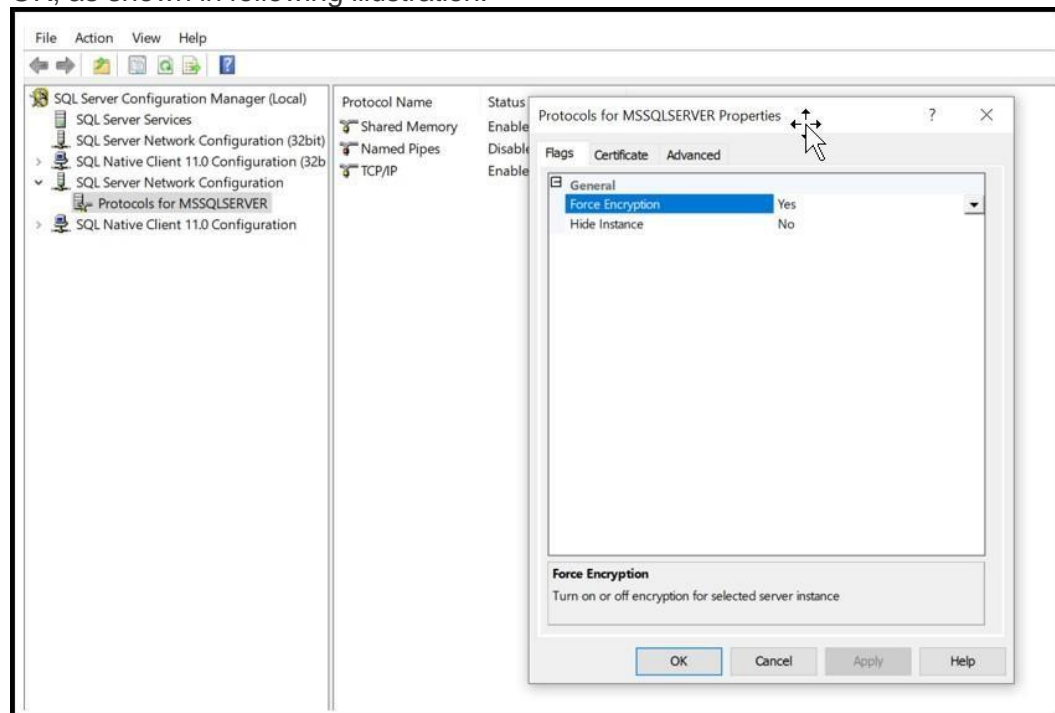
1. For encrypted connection SSL Certificates are required. These can be generated in any of the following methods: Get SSL Certificates from Certificate Authority (CA). These certificates should be in PEM format. Get SSL Certificates using openssl, as shown in **Generating a Self-Signed SSL Certificate using OpenSSL** section. Now, import it to the certificate store on MSSQL using Microsoft Management Console.
2. 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.
3. From the **File** menu, select **Add/Remove Snap-in...** The Add/Remove Snap-in dialog box appears.
4. 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.
5. 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.
3. 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.



4. 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]:IA
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>

```

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
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 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 keytool.exe file in \ucm\java\jre\bin folder:**For Example:**C:\Program Files (x86)\Kewill\Flagship\ucm\java\jre\bin
2. 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
keytool: This is the main tool to generate the certificate in the keystore file.
<Keystore file>: Provide the name of the Keystore file.
For Example:keystore
3. 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".
```

4. 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-importkeystore: To import a single entry or all entries from a source keystore to a destination keystore.

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

For Example:keystore

<Destination keystore name>: Provide the Destination keystore name.

For Example:myKeystore

<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
```

5. 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.

1. 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 SORDDDB 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

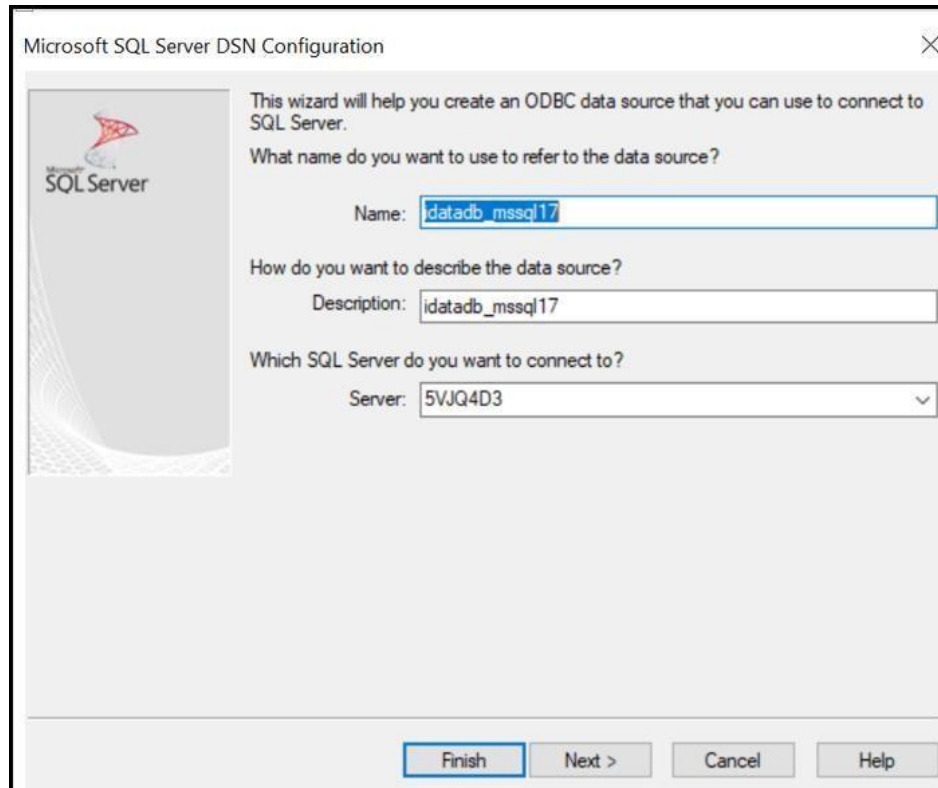
Prerequisite:

- 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:

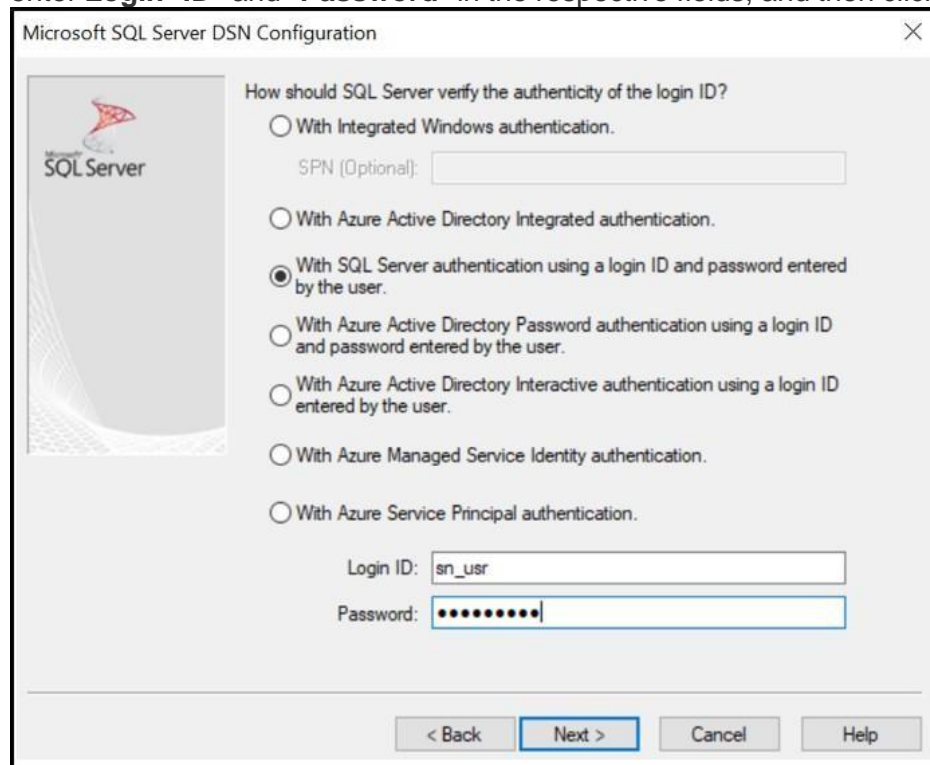
1. Open ODBC Data Source Administrator (32-bit) window.
2. Select the *System DSN* tab, click Add... and select 'ODBC Driver 17 for SQL Server' drive or later and then click Finish. **Note:** For secure encryption only 'ODBC Driver 17 for SQL Server' driver and above are supported. The Microsoft SQL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

In this fields...	Do this..
Name	Enter the data source name. For Example: idatadb_mssql17
Description	Enter the description. For Example: idatadb_mssql17
Server	Select the SQL Server you want to connect from the drop-down list.



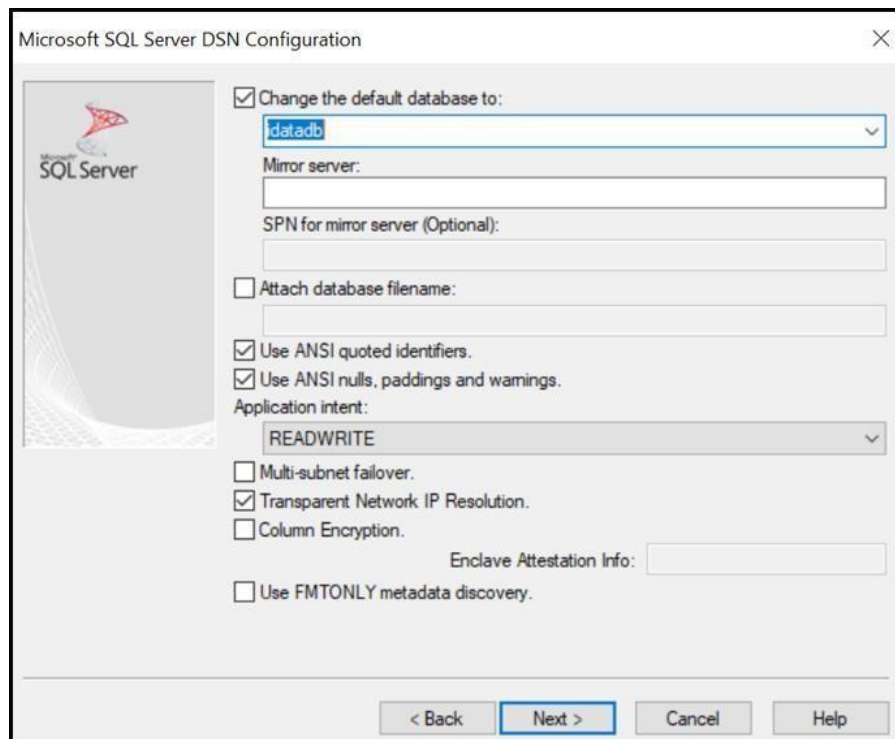
3. In Microsoft SQL Server DSN Configuration screen, select 'With SQL Server authentication using a login ID and password entered by the user.' option and

enter **Login *ID*** and ***Password*** in the respective fields, and then click Next.

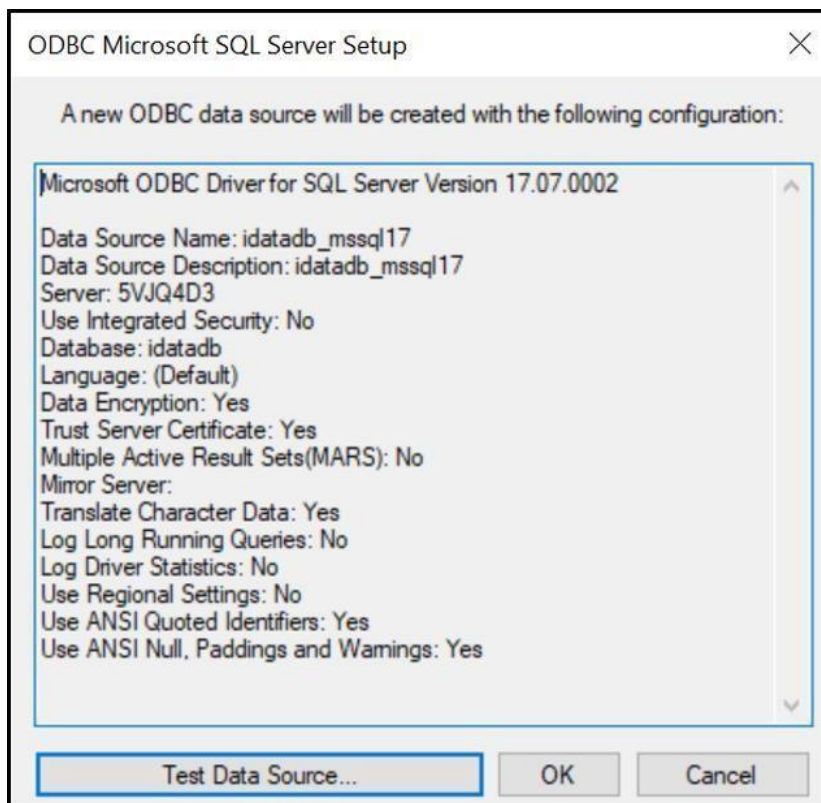
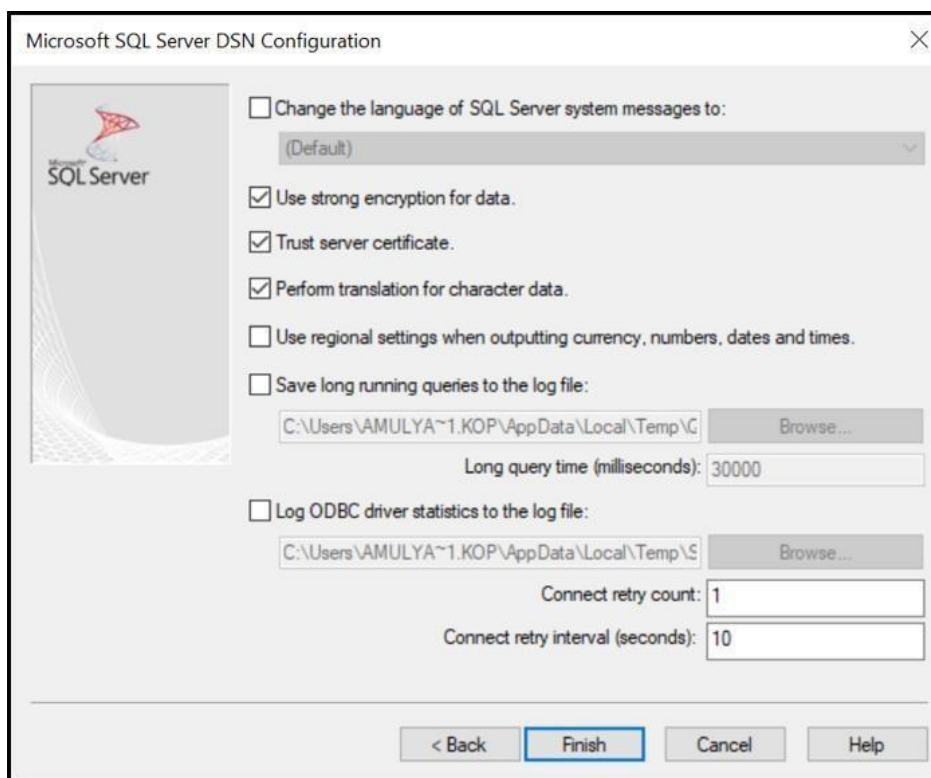


The screenshot shows the 'Microsoft SQL Server DSN Configuration' dialog box. On the left is the Microsoft SQL Server logo. The main area is titled 'How should SQL Server verify the authenticity of the login ID?'. It contains several radio button options: 'With Integrated Windows authentication.', 'With Azure Active Directory Integrated authentication.', 'With SQL Server authentication using a login ID and password entered by the user.' (which is selected), '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.', and 'With Azure Service Principal authentication.'. Below these options are two text input fields: 'Login ID:' with the value 'sn_usr' and 'Password:' with a masked password '••••••••'. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

4. 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.
idatadb
sordb



The screenshot shows the 'Microsoft SQL Server DSN Configuration' dialog box, Step 2. On the left is the Microsoft SQL Server logo. The main area is titled 'Change the default database to:'. Below this is a drop-down menu with 'idatadb' selected. There are two empty text input fields for 'Mirror server:' and 'SPN for mirror server (Optional):'. Below these is a checkbox 'Attach database filename:' which is unchecked, followed by an empty text input field. There are three checked checkboxes: 'Use ANSI quoted identifiers.', 'Use ANSI nulls, paddings and warnings.', and 'Application intent:'. The 'Application intent:' dropdown menu is set to 'READWRITE'. There are three unchecked checkboxes: 'Multi-subnet failover.', 'Transparent Network IP Resolution.', and 'Column Encryption.'. Below these is a text input field for 'Enclave Attestation Info:'. At the bottom are four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.



5. 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
dbs-connection	sordb	name	Enter the sordb name. For example: sordb
dbs-connection	sordb	username	Enter the sordb username. For example: sn_usr
dbs-connection	sordb	password	Enter the sordb password. For Example: shipnowdb
dbs-connection	sordb	driver	Change to com.microsoft.sqlserver.jdbc.SQLServerDriver
dbs-connection	sordb	url	Enter the URL in jdbc:sqlserver://localhost:1433;databaseName=sordb format. For Example: jdbc:sqlserver://5VJQ403.blujay.global:1433;databaseName=sordb

domain	sub_domain	key_name	key_value
dbms-connection	soradb	trustStore_path	Enter the trustStore path. For Example: C:\Users\Blujay\myTrustStore
dbms-connection	soradb	trustStore_password	Enter the trustStore password. For Example: test123
dbms-connection	soradb	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	soradb_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	dbms-connection	soradb	name	soradb
ALL	dbms-connection	soradb	type	JDBC
ALL	dbms-connection	soradb	url	jdbc:sqlserver://5VJQ4D3.blujay.global:1433;Data
ALL	dbms-connection	soradb	username	sn_usr
ALL	dbms-connection	soradb	password	shipnowdb
ALL	dbms-connection	soradb	driver	com.microsoft.sqlserver.jdbc.SQLServerDriver
ALL	dbms-connection	soradb	dialect	
ALL	dbms-connection	soradb	trustStore_path	C:\Users\Amulya.Koppula\myTrustStore
ALL	dbms-connection	soradb	trustStore_password	test123
ALL	dbms-connection	soradb	use_secure_encryption	y

6. IDATADB

domain	sub_domain	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

domain	sub_domain	key_name	key_value
core	idata	password	Enter the password. For example: shipnowdb
dbs-connection	idatadb	name	Enter the idatadb name. For example: idatadb
dbs-connection	idatadb	username	Enter the idatadb username. For example: sn_usr
dbs-connection	idatadb	password	Enter the idatadb password. For Example: shipnowdb
dbs-connection	idatadb	driver	Change to com.microsoft.s qlserver.jdbc.SQ LServerDriver
dbs-connection	idatadb	url	Enter the URL in jdbc:sqlserver:// localhost:1433;d atabaseName=id atadb format For Example: jdbc:sqlserver:1 0.0.8.47:1433;dat abaseName=idat adb
dbs-connection	idatadb	trustStore_path	Enter the trustStore path. For Example: C:\myTrustStore
dbs-connection	idatadb	trustStore_pass word	Enter the trustStore password. For Example: test123

domain	sub_domain	key_name	key_value
dbms-connection	idatadb	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	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_separately	n
ALL	dbms-connection	idatadb	name	idatadb
ALL	dbms-connection	idatadb	type	JDBC
ALL	dbms-connection	idatadb	url	jdbc:sqlserver://10.0.8.47:1433;databaseName=idatadb
ALL	dbms-connection	idatadb	username	sn_usr
ALL	dbms-connection	idatadb	password	shipnowdb
ALL	dbms-connection	idatadb	driver	com.microsoft.sqlserver.jdbc.SQLServerDriver
ALL	dbms-connection	idatadb	dialect	
ALL	dbms-connection	idatadb	trustStore_path	C:\myTrustStore
ALL	dbms-connection	idatadb	trustStore_password	test123
ALL	dbms-connection	idatadb	use_secure_encryption	y

Configuring Oracle to Use Encrypted Connection

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

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


```
mkdir wallets
cd wallets
```

For Example:

```
oracle@parcel-orcl02-fr4 bin$
```

```
mkdir Wallets
```

```
oracle@parcel-orcl02-fr4 bin$ cd Wallets
```

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
```

- 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 >
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
```

2. 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
```

3. 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
```

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
```

4. 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
```

5. 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$
```

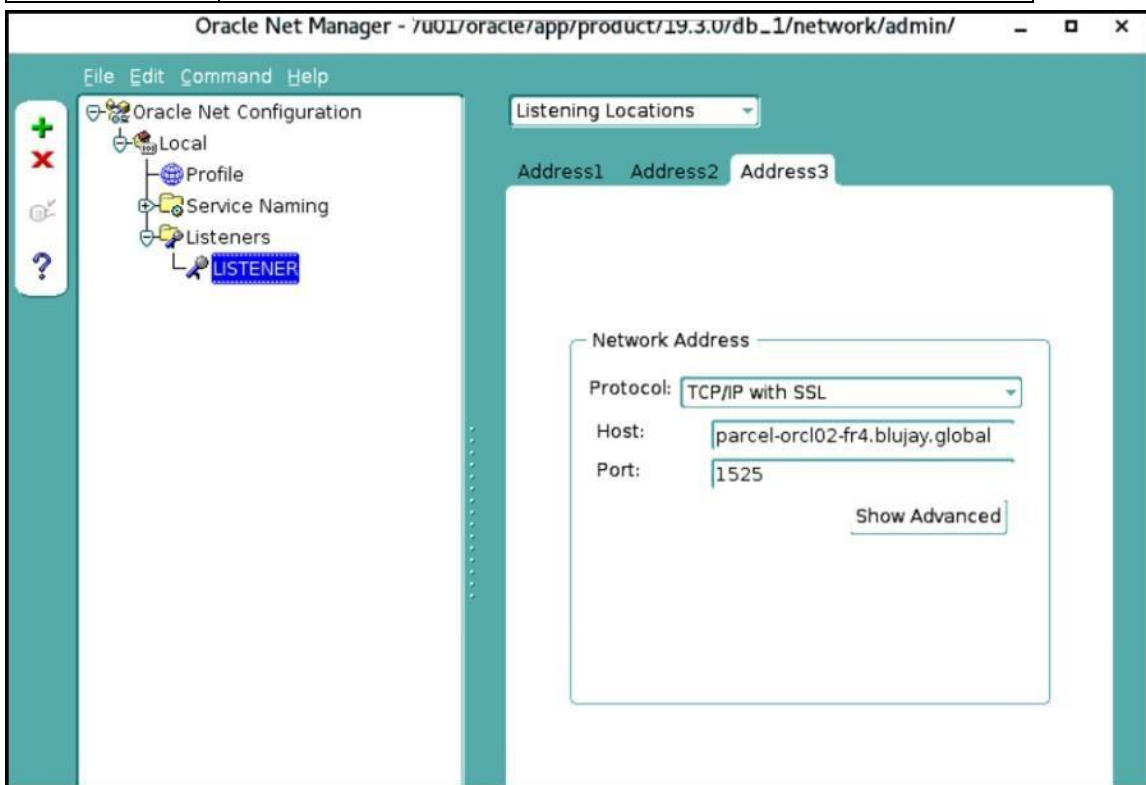
```
orapki wallet add -wallet ./client_wallet -trusted_cert -cert ./server_wallet/cert.txt -pwd
oracle123
```

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.
2. Launch the Net Manager tool. To open network manager, execute the below command: `netmgr`
3. Navigate to Local > Listeners > Listener.
4. 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



Click File > Save Network Configuration to save the configuration settings.

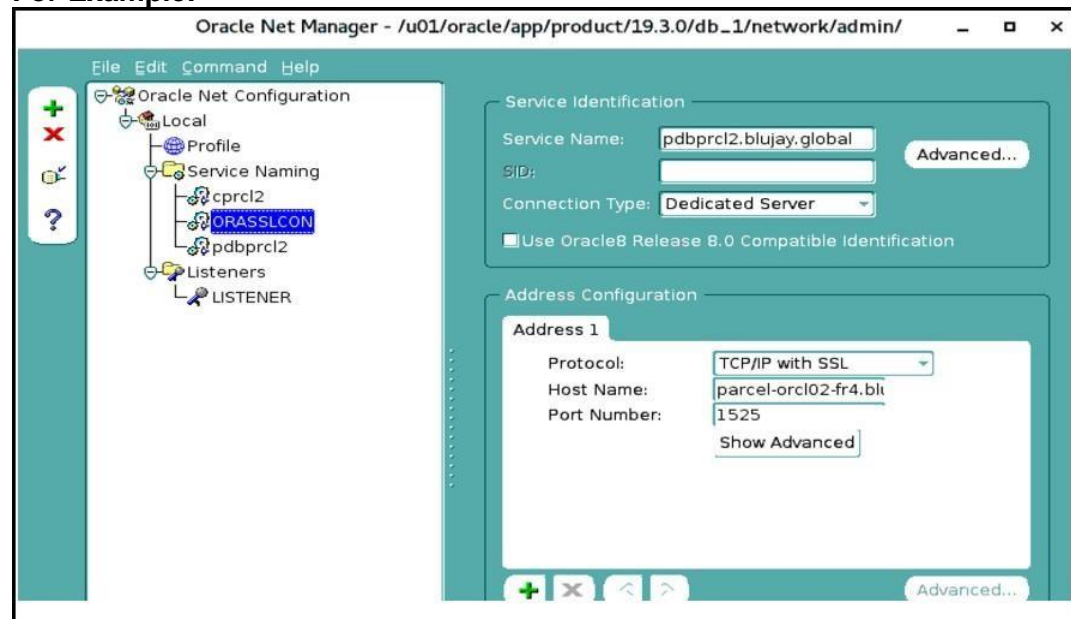
The listener.ora network configuration file that you created looks as show below:

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>))  
)  
)
```

1. Configure the tnsnames.ora file.
2. Navigate to Local > Service Naming.
3. Click Edit > Create. The Net Service Name Wizard: Welcome screen displays.
4. Enter the name that you want to use to access the database or service in the *Net Service Name* field and click Next.
5. Select the 'TCP/IP with SSL (Secure Internet Protocol)' protocol used for the database you want to access.
6. Enter the TCP/IP host name for the computer where the database is located in the **Host Name** field.
7. Enter the TCP/IP port number for Oracle database in the *Port Number* field and click Next.
8. Enter the service name of the database that you want to access in the **Service Name** field.
9. Select the database connection type as 'Dedicated Service' from *Connection Type* drop-down list and click Next.
10. Click Test... if you want to test the connection of the wizard or else click Finish to create the net service name.
11. Click File > Save Network Configuration to save the network configuration settings. The tnsnames.ora network configuration file that you created looks as show below:

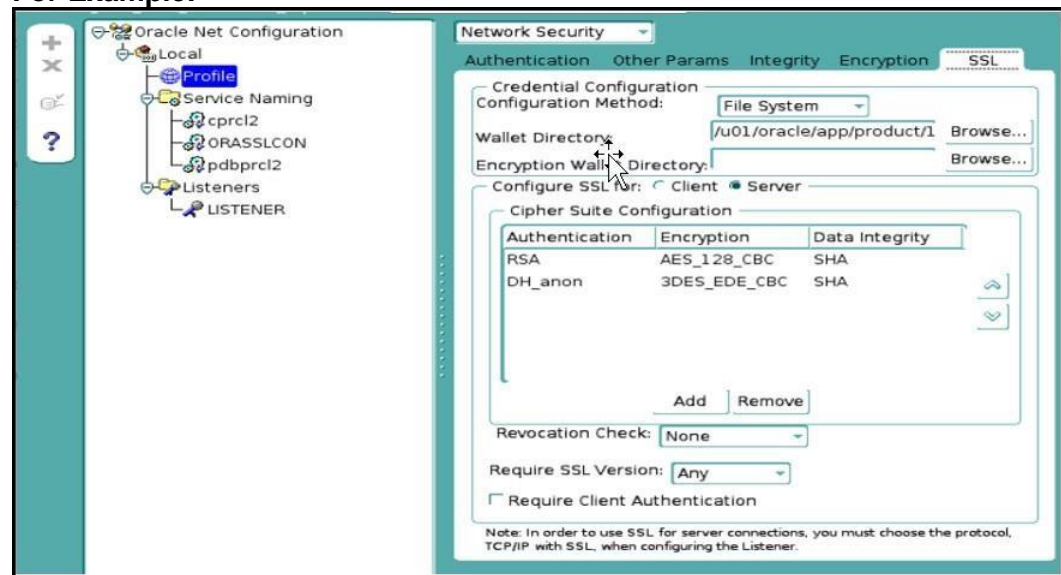
For Example:

```

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

```

1. Configure the sqlnet.ora file.
2. Navigate to Local > Profile.
3. Select 'Network Security' from the drop-down list.
4. Click **SSL** tab and then select Server option, if you do not have an SSL form.
5. In the Credential Configuration panel, select 'File System' from the *Configure Method* drop-down list and click Browse... and specify the Sever Wallet Directory.
6. In the Cipher Suite Configuration panel, leave the default settings in **Revocation Check**, **Require SSL Version** and **Require Client Authentication** fields.
7. Select Cipher Suite as RSA AES_128_CBC_SHA.
8. 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>)
)

```


)
)

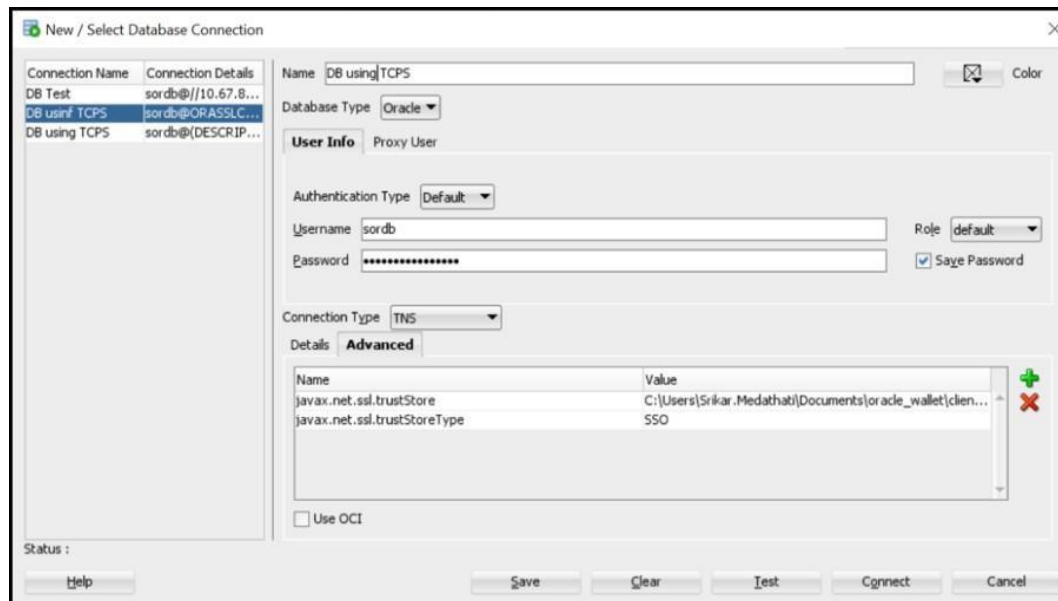
1. Run Oracle SQL Developer locally. The Oracle SQL Developer home page displays.
2. In the **Connections** pane, right-click and select **New Connection**. The New / Select Database Connection dialog box appears.
3. In the New / Select Database Connection dialog box, enter the database connection details 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	Network Alias: Select ORASSLCON from the drop-down list. Note: This name is same as tns name which we have added.
	Advanced: Specify the trustStore file path received from the server side and trustStore path as SSO.

The screenshot shows the 'New / Select Database Connection' dialog box. On the left, a list of connections is shown: 'DB Test', 'DB using TCP', 'DB using TNS', and 'DB using TNS'. The 'DB using TNS' connection is selected. The main area contains the following fields and options:

- Name:** DB using TNS
- Database Type:** Oracle
- User Info:** Proxy User
- Authentication Type:** Default
- Username:** sordb
- Password:** (masked with asterisks)
- Role:** default
- Save Password:** (checked)
- Connection Type:** TNS
- Details:**
 - Network Alias:** ORASSLCON
 - Connect Identifier:** (empty)

At the bottom, there are buttons for 'Help', 'Save', 'Clear', 'Test', 'Connect', and 'Cancel'.



4. 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.

1. 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	Enter the sordb User ID. For Example: sordb

2. Click Test Connection to test the sordb connectivity to the database and enter password in the *Password* field and then click OK.
3. 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

Click Test Connection to test the idatadb connectivity to the database and enter password in the *Password* field and then click OK.

Do the changes in **didb.settings** table for SORDB and IDATADB, see "**Adding DSN for MSSQL Database Connection**" section, **Step 6**

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. Navigate to `..\Kewill\Flagship\bin` directory. 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"

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

The screenshot shows the e2open Global Parcel application interface. At the top, it displays 'Location: JP SMOKE Test' and 'Ship Date: 01/31/2024'. Below this is a navigation bar with links: Ship, Track, My Profile, System, Workstation, UCM, and Help. The main content area is titled 'System / Settings' and shows a list of settings on the left and an 'Edit record' form on the right. The 'Settings' item in the left list is highlighted with a red box. The 'Edit record' form contains the following fields:

Edit record	
machine_name	ALL
Domain	ui-app
Sub Domain	global
Key Name	output_dir
Key Value	C:\\Program Files (x86)\\Kewill\\A
Display Name	Manifest (DPRN) output directo
Value Type	password

At the bottom of the form are 'CANCEL' and 'SAVE' buttons.

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

4. Update PHP.INI File.
5. Navigate to the following location and open the php.ini file in a text editor: For Apache – ..\\Kewill\\Flagship\\php\\php.ini
For IIS – ..\\Kewill\\Flagship\\phpnts.php.ini
6. 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.

1. Save and close the php.ini file.
2. Update httpd.conf file (For Apache only)
3. Navigate to the following location and open the httpd.conf file in a text editor:...\Apache-httpd\Apache24\conf
4. 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>
```

5. 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.

6. Save and close the httpd.conf file.
7. Update Parcel options in Virtual Directory (For IIS Machine only) For information, see [Add/Update Virtual Directory in IIS](#) section.
8. 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	sub-domain	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.

e2open Global Parcel

Location: JP SMOKE Test
Ship Date: 02/02/2024

administrator

ShipTrackMy ProfileSystemWorkstationUCMHelp

System / Settings

<<<Page 1 of 4>>>

Location IDLocation Name

SEARCH

Global Settings

Add Location

Delete Location

Corporate DSN

CloseConfig

Custom Data Mapping

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_nameALL

Domainintegration

Sub Domainetwoproxy

Key Nameenable_ums_integration

Key Valuey

Display NameUMS Integration

Value Typepassword

CANCEL

SAVE

machine_name	domain	sub-domain	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.

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

114

e2open Global Parcel Location: [JP SMOKE Test](#) Ship Date: [01/31/2024](#) 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
- ☐ Close Config
- ☐ Custom Data Mapping
- ☐ 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_e2proxy_integration
Key Value	y
Display Name	E2Proxy Integration
Value Type	password

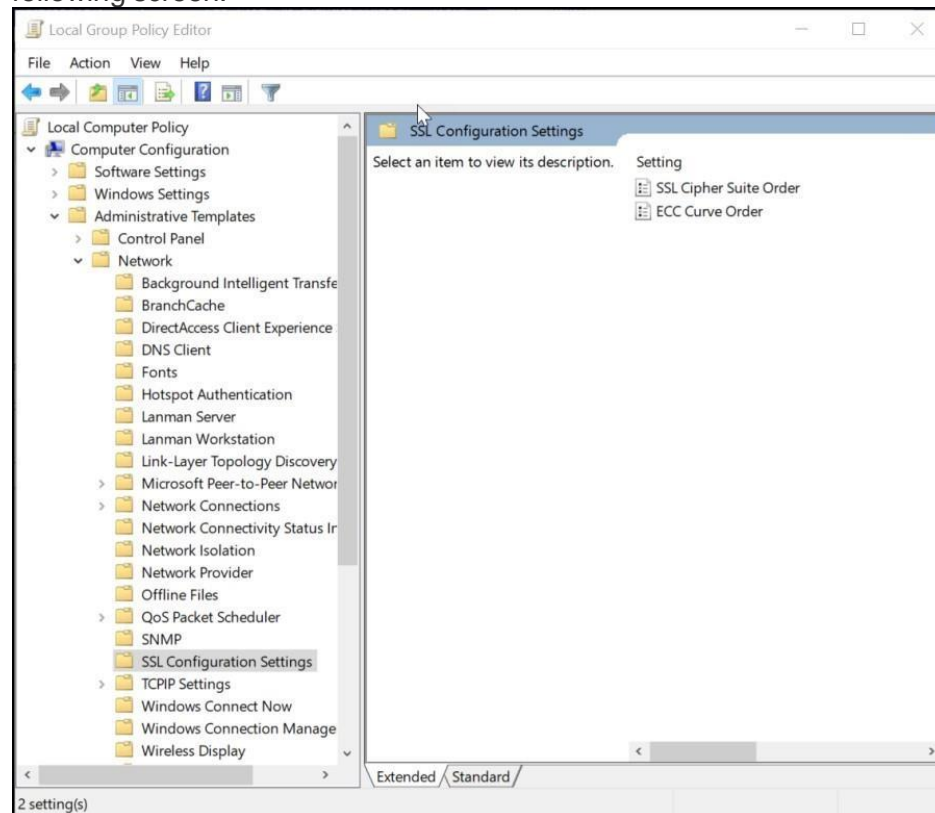
CANCEL SAVE

Disabling Weak SSL Cipher Suites in IIS

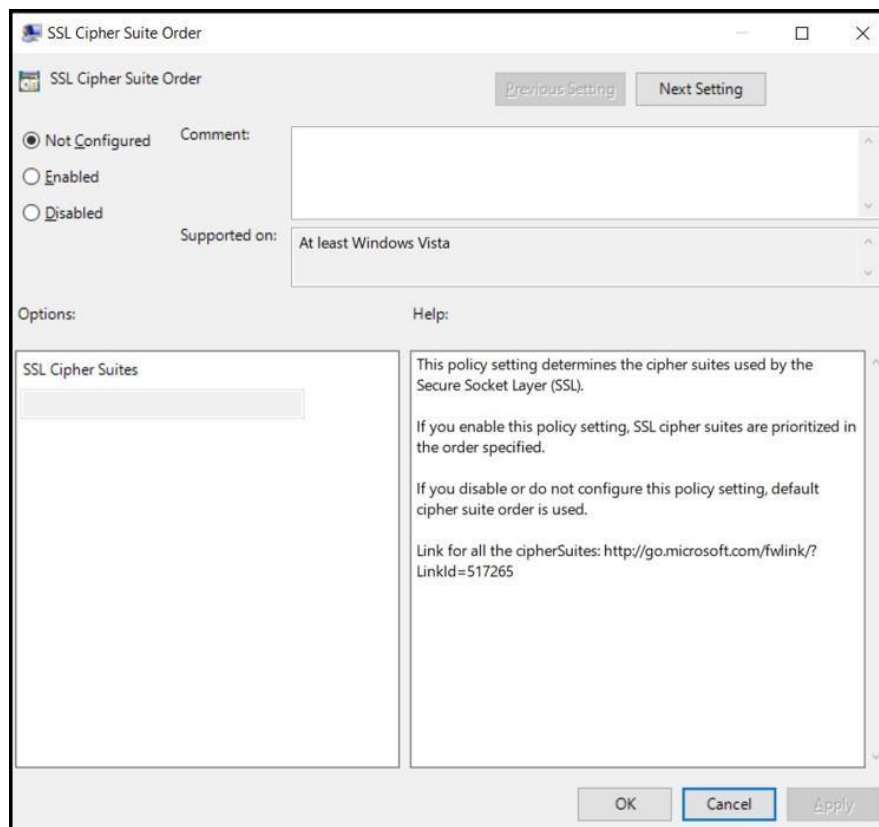
The user needs to disable weak SSL cipher suites in IIS for security purpose. This section describes about how to disable the weak SSL cipher suites in IIS. To disable Weak SSL Cipher Suites in IIS, follow these steps:

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 show in following screen.



"Client"

"Server"

- i. Right-click the "Client" and "Server" subkey and create a new DWORD (32-bit) Value called 'DisabledByDefaultEnabled'. (New > DWORD (32-bit) Value > DisabledByDefaultEnabled).
- ii. Leave the default value as '0'.
- iii. Right-click the "Client" and "Server" subkey and create a new DWORD (32-bit) Value called 'Enabled'. (New > DWORD (32-bit) Value > Enabled).
- iv. Leave the default value as '1'.
- v. Close the Registry Editor.
- vi. Restart the Server Machine.

Troubleshooting Upgrade Installation

Overview - Troubleshooting

If any errors occur during the installation, they appear in a popup 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:

BJ222Install_<yyyymmdd_mm_ss>.log

For Example: BJ231Install_20240108122_15_5.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.

Common Problem	Cause/Suggestion for Resolution
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.

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 the 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, e2open LLC 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 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
This required step re-initializes the configuration.xml file with the correct paths.
5. Copy the flagshipProperties.xml file from the <Parcel Artifact Folder>{color} 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.
6. 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 re-installing 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 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 2.4
MySQL - you must stop this service even if you are not uninstalling MySQL.
All Kewill Services
Stunnel SSL Wrapper
3. Navigate to the Add/Remove Programs screen from the Control Panel.
4. In the *Add/Remove* Programs list, select *Flagship* or *Kewill Flagship{*, 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 (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_svc
 - JTrack
 - Kewill TSN Communication Service
 - MySQL (delete only if you uninstalled MySQL!)
 - Notification Service
 - SchedulerSvc
 - Stunnel 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. Re-start your computer.

Printing Reports

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.

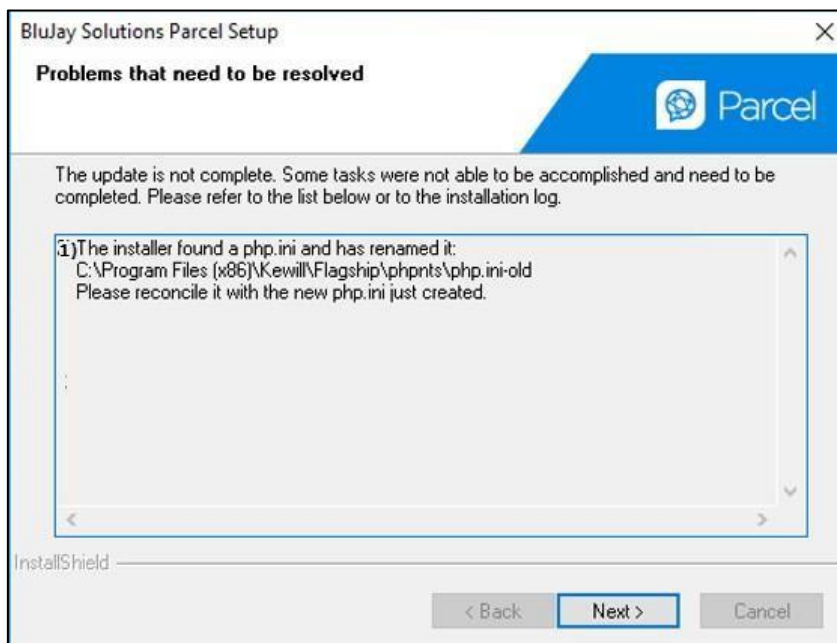
Error Message related to powershell

In case "Windows cannot find 'powershell.exe'" error message appears, please follow these steps:

1. Please find **fixPathEnvironmentVariable.ps1** file in 21.1.0 Installer.
2. Open PowerShell command prompt with Administrator privileges
3. Navigate to folder where **fixPathEnvironmentVariable.ps1** file copied
4. Run **Set-ExecutionPolicy RemoteSigned** command
5. Type **Y** for Execution Policy change.
6. Run **fixPathEnvironmentVariable.ps1** script
7. Press Enter to exit.
8. Restart the system.
9. After restart, now continue with **Step 3** in **Upgrading Parcel** section.

Pending tasks during upgrade on an IIS environment

If you are upgrading to TM-Parcel 24.1.0 on an IIS environment, the following error may occur before completing the upgrade installation process:



The error message screen appears before the final step (restarting the machine) of the upgrade installation process.

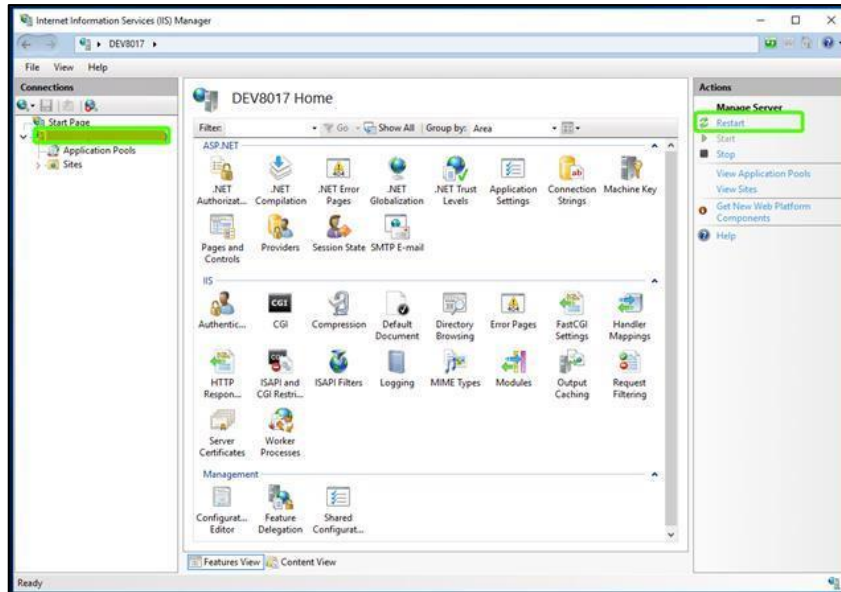
Perform these steps to resolve the error:

1. Navigate to the path mentioned in the Setup Wizard, for example, *C:\Program Files (x86)\Kewill\Flagship\phpnts*.
You will see two php.ini files in the folder. Existing php.ini file has been renamed to **php.ini-old** and a new file **php.ini** has been created.

2. Open the **php.ini** file in a text editor.
 - a. Remove the starting comments (#) for the below settings and set those with the following values:
 - `fastcgi.impersonate = 1`
 - `fastcgi.logging = 0`
 - `cgi.fix_pathinfo = 0`
 - `cgi.force_redirect = 1`
3. For Example: Change **#fastcgi.impersonate** to **fastcgi.impersonate=1**.

```
779 ; cgi.force_redirect is necessary to provide security running PHP as a CGI under
780 ; most web servers. Left undefined, PHP turns this on by default. You can
781 ; turn it off here AT YOUR OWN RISK
782 ; **You CAN safely turn this off for IIS, in fact, you MUST.**
783 ; https://php.net/cgi.force-redirect
784 ; cgi.force_redirect = 1
785
786 ; if cgi.nph is enabled it will force cgi to always sent Status: 200 with
787 ; every request. PHP's default behavior is to disable this feature.
788 ;cgi.nph = 1
789
790 ; if cgi.force_redirect is turned on, and you are not running under Apache or Netscape
791 ; (iPlanet) web servers, you MAY need to set an environment variable name that PHP
792 ; will look for to know it is OK to continue execution. Setting this variable MAY
793 ; cause security issues, KNOW WHAT YOU ARE DOING FIRST.
794 ; https://php.net/cgi.redirect-status-env
795 ;cgi.redirect_status_env =
796
797 ; cgi.fix_pathinfo provides "real" PATH_INFO/PATH_TRANSLATED support for CGI. PHP's
798 ; previous behaviour was to set PATH_TRANSLATED to SCRIPT_FILENAME, and to not grok
799 ; what PATH_INFO is. For more information on PATH_INFO, see the cgi specs. Setting
800 ; this to 1 will cause PHP CGI to fix its paths to conform to the spec. A setting
801 ; of zero causes PHP to behave as before. Default is 1. You should fix your scripts
802 ; to use SCRIPT_FILENAME rather than PATH_TRANSLATED.
803 ; https://php.net/cgi.fix-pathinfo
804 ; cgi.fix_pathinfo=0
805
806 ; if cgi.disable_path is enabled, the PHP CGI binary can safely be placed outside
807 ; of the web tree and people will not be able to circumvent .htaccess security.
808 ;cgi.disable_path=1
809
810 ; FastCGI under IIS supports the ability to impersonate
811 ; security tokens of the calling client. This allows IIS to define the
812 ; security context that the request runs under. mod_fastcgi under Apache
813 ; does not currently support this feature (03/17/2002)
814 ; Set to 1 if running under IIS. Default is zero.
815 ; https://php.net/fastcgi.impersonate
816 ; fastcgi.impersonate = 1
817
818 ; Disable logging through FastCGI connection. PHP's default behavior is to enable
819 ; this feature.
820 ; fastcgi.logging = 0
821
822 ; cgi.rfc2616_headers configuration option tells PHP what type of headers to
823
```

4. Configure any other changes required in the **php.ini** file, and then save the file.
5. Restart the IIS Service.



6. On the Parcel Setup screen, click Next and complete the upgrade installation process.