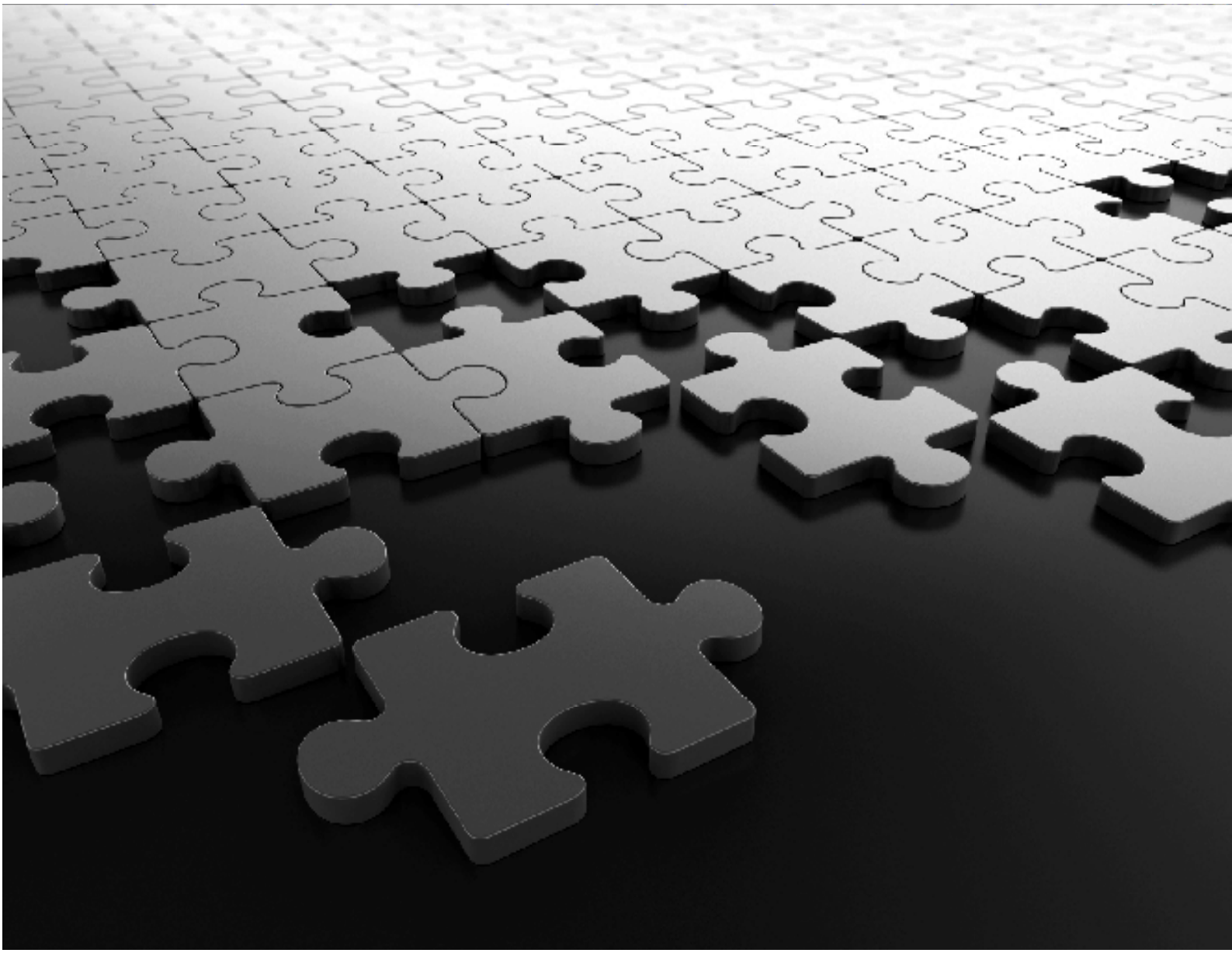
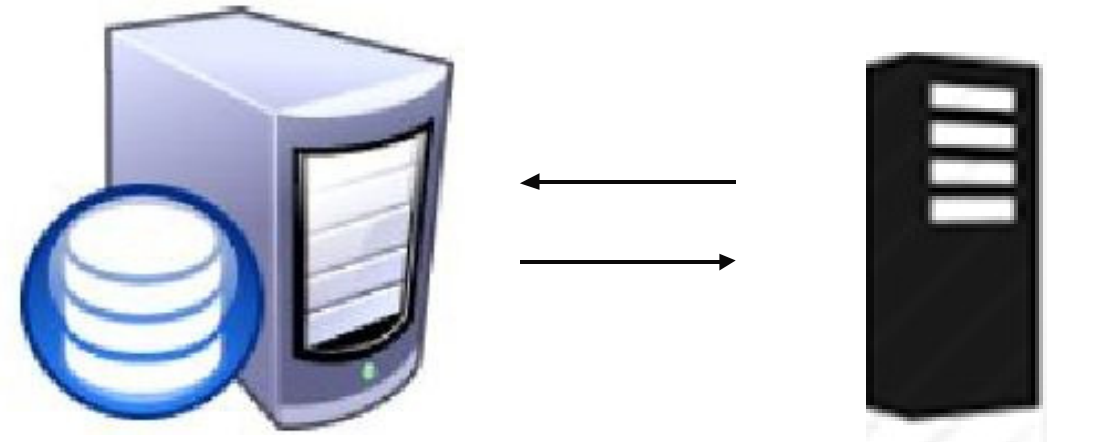
COSEC INTEGRATE
User Manual



MATRIX
SECURITY SOLUTIONS

MATRIX
SECURITY SOLUTIONS

COSEC INTEGRATE
User Manual



Documentation Disclaimer

Matrix Comsec reserves the right to make changes in the design or components of the product as engineering and manufacturing may warrant. Specifications are subject to change without notice.

This is a general documentation for all variants of the product. The product may not support all the features and facilities described in the documentation.

Information in this documentation may change from time to time. Matrix Comsec reserves the right to revise information in this publication for any reason without prior notice. Matrix Comsec makes no warranties with respect to this documentation and disclaims any implied warranties. While every precaution has been taken in the preparation of this system manual, Matrix Comsec assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Neither Matrix Comsec nor its affiliates shall be liable to the buyer of this product or third parties for damages, losses, costs or expenses incurred by the buyer or third parties as a result of: accident, misuse or abuse of this product or unauthorized modifications, repairs or alterations to this product or failure to strictly comply with Matrix Comsec operating and maintenance instructions.

Warranty

For product registration and warranty related details visit us at:
https://www.matrixcomsec.com/warranty/#access-control-time-attendance

Copyright

All rights reserved. No part of this system manual may be copied or reproduced in any form or by any means without the prior written consent of Matrix Comsec.

Version 19
Release date: November 14, 2024

Contents

Introduction *1*
Export to MS SQL/ORACLE *4*
Export to Postgre Server *21*
Export to CSV *24*
Export to MySQL *38*
Export to Text *45*
Export to DB2 ..... *63*
Export to People Works *68*
Export FP Template to File *75*
Custom Export- FP Template *84*
Export to Progress OpenEdge *88*
Import from MS SQL/Oracle/Postgre *96*
Import from Active Directory *111*
Importing Data from a Customized SAP *115*
Import Events *117*
Import from My SQL *125*
Import from Progress OpenEdge *128*
Import from Excel *134*
Integrate Alert *138*
BACnet Server Configuration *140*

Introduction

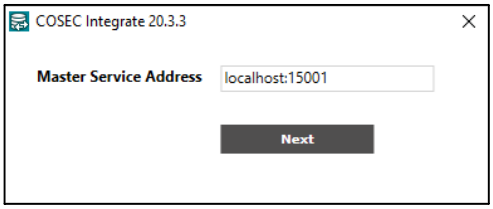
The COSEC INTEGRATE module enables the administrator to configure the following functionalities.

- Export data from the COSEC database to a third party MS SQL or Oracle database.
- Import user data from external data sources like MSSQL, Oracle, Postgre and the Microsoft Active Directory.
- Import User data from customized SAP table in MSSQL or Oracle.
- Export Device data and event logs to predefined tables in Postgre database.
- Import event data from 3rd party database (MS SQL and Oracle).
- Configure BACnet Server parameters to enable integration of BACnet with COSEC.

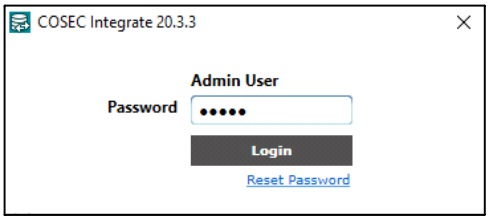
The COSEC installer utility has the COSEC INTEGRATE module option which needs to be selected for this application to be installed.

To access this application, double click on the COSEC INTEGRATE Module icon on the computer desktop.

Enter the Master Service Address and click Next.



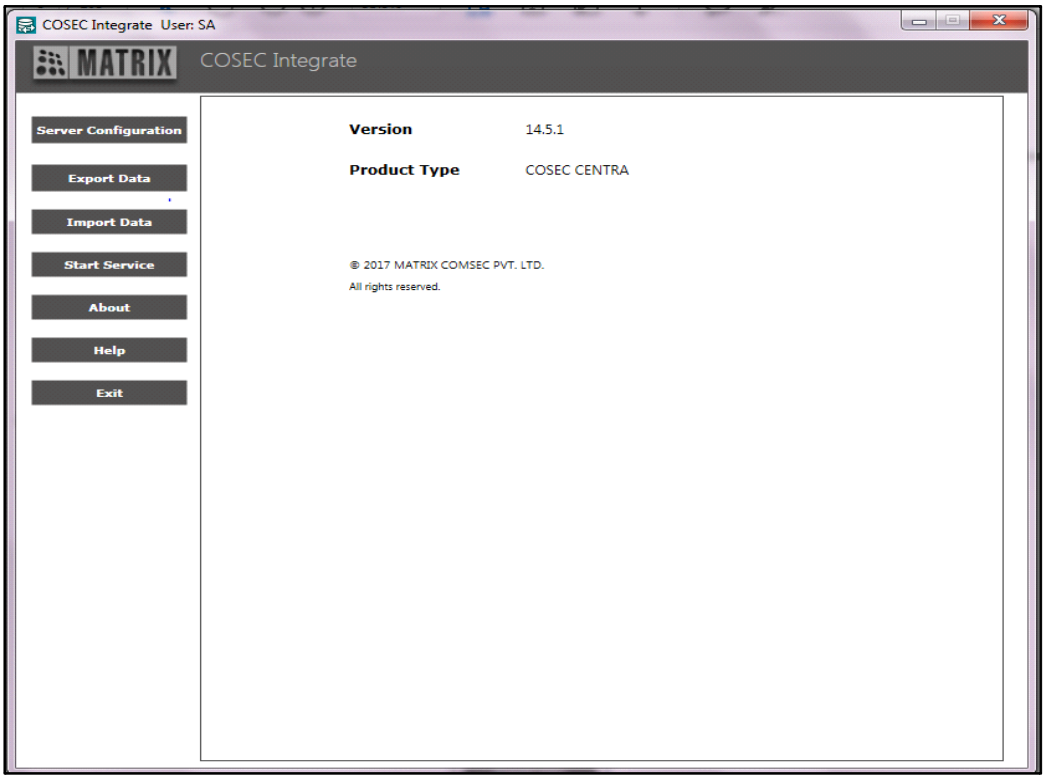
Enter the password of the admin user and click Login.



The Reset Password option enables the user to reset the password in the event of the admin user forgetting the set password. Contact the authorized dealer or Matrix support for the reset code.

For COSEC Integrate to work properly, it must be ensured that actual DB fields as well as their renamed versions (if any, i.e. if DB field is renamed with an alias during export template configuration) are both included in the template configuration. This shall be applicable to all exports.

Click on the **Login** button after entering the password. The COSEC INTEGRATE home page appears as shown.



The COSEC INTEGRATE service needs to be stopped prior to starting the configuration of the various COSEC INTEGRATE parameters. Click on the **Stop Service** button as shown.

To know about the Export and Import from other database and BACnet Server Configuration click on the following links.

"Export to MS SQL/ORACLE"
"Export to MySQL"
"Export to CSV"
"Export to Text"
"Export to Postgre Server"
"Export to DB2"
"Export to People Works"
"Export FP Template to File"
"Custom Export- FP Template"
"Export to Progress OpenEdge"

"Import from MS SQL/Oracle/Postgre"
"Import from My SQL"
"Importing Data from a Customized SAP"
"Import from Active Directory"
"Import Events"

“Import from Progress OpenEdge”
“BACnet Server Configuration”

Export to MS SQL/ORACLE

The application allows the administrator to map the data fields of the COSEC application database to the data fields of another SQL/Oracle database.

Integrate supports:

- *Export to Oracle from version Oracle 10g to Oracle 23AI.*
- *Export to MS SQL from version SQL Server 2005 to SQL Server 2022*

SQL Server 2005 and SQL Server 2008 R2:

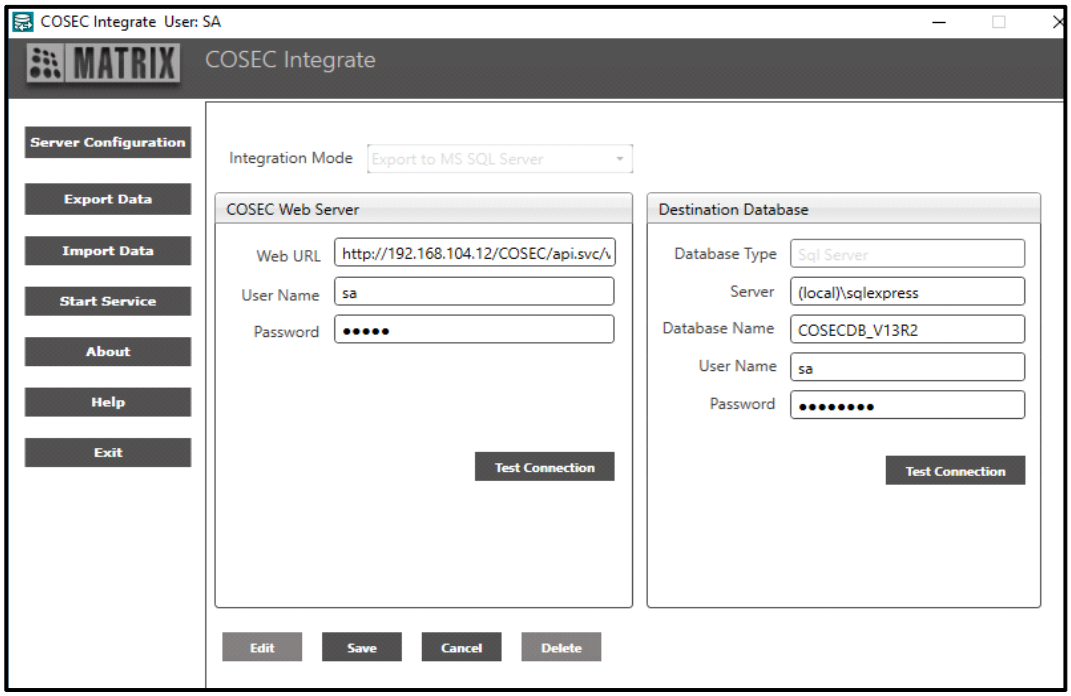
- *for installation you need Windows 7 or below versions.*
- *to establish remote connections in these versions from the PC in which Integrate is installed, make sure you have enabled TLS 1.0 and 1.1 (that is, Best Practices settings).*

Server Configuration

Click on the **Server Configuration** button to configure the Web server and Destination database for Export and Source database for Import.

Depending on the Integration mode selected, you must configure **Destination Database/ Destination Location/ Source Database**.

Select the **Export to MS SQL Server** option in the **Integration Mode** field.



Click on the **Edit** button.

In the **COSEC Web Server** section:

- Specify the web URL of the API service of the COSEC WEB application as shown above.
- Enter the User Name and Password of the system administrator (sa) as set in the COSEC WEB application.

In the **Destination Database** Server section:

- The **Database Type** will be SQL SERVER.
- **Server**: Enter the database server name in the following format - **Database server name\Instance Name** e.g. dbserver\sqlexpress.
- **Database Name**: Specify the database name of the destination database as per the site settings. Eg: COSECDB_V13R2 is the destination database which is newly created from Database Utility. You can export the data to this database.

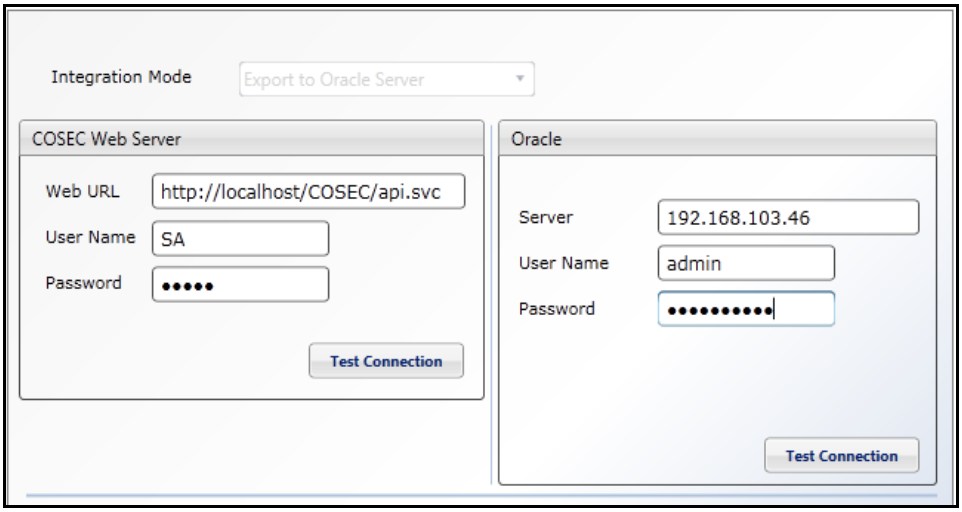
For newly created database, ensure that you have set the password in COSEC Web application. Then only Test connection from COSEC Integrate with Web server will be successful.

- **User Name**: Specify the database administrator ID in this field. This is the user name which you have set while installing SQL Server Management Studio in your computer.
- **Password**: Enter the password of the Database administrator as per the site settings. This is the password which you have set while installing SQL Server Management Studio in your computer.

The **Test Connection** button is provided to test the connections with the web server as well as the SQL Server database.

Click on **Save** once done.

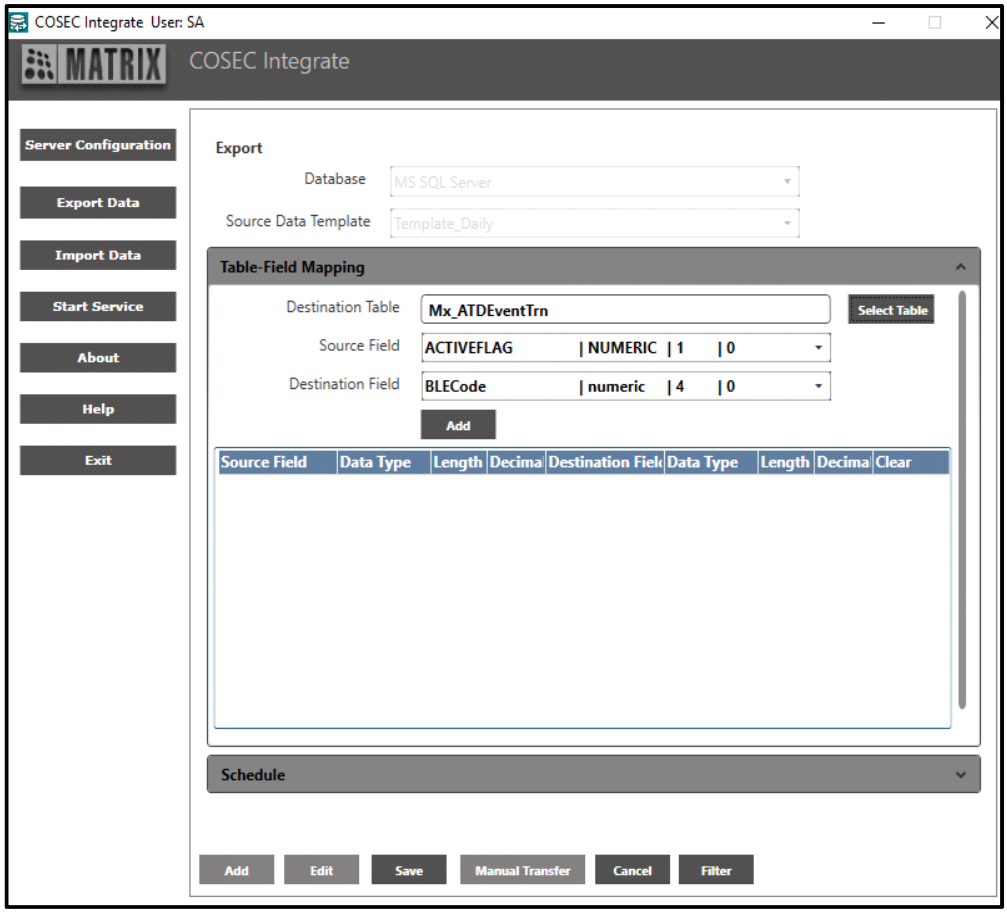
In the event of selecting the **Export to Oracle Server** option in the **Integration Mode** field, specify the Oracle server destination address as well as the user name and the password (case-sensitive for Oracle Server) in the respective fields as shown.



Test the connection and Save the configuration.

Export Data Configuration

This option enables the Admin user to map the fields from the COSEC database tables to fields in a third party database. Click on the **Export Data** button. The following page appears.



The COSEC INTEGRATE application provides four data templates in line with the default **Database Views** as shown. The COSEC System provides the following four Database views which would provide the relevant field options to be mapped with the fields of a destination database.

- Monthly Attendance Summary, for details refer to “Monthly Attendance Summary”
- Daily Attendance Detail, for details refer to “Daily Attendance Detail”
- Attendance Events, for details refer to “Attendance Events or Access Control Events -Schedule”
- Access Control Events, for details refer to “Attendance Events or Access Control Events -Schedule”

The following templates can be configured from COSEC Web which can be exported to other database.

- First and Last Attendance Events
- Daily Attendance Template1
- Daily Cafeteria Events
- Monthly Cafeteria Summary
- Monthly Job Summary
- User Details

For details, refer “Custom Template - User Details Template-Schedule”

Each of the above database views would provide the relevant fields whose values can be exported from the COSEC database. Select the required data template and click on the **Edit** button.

Export

The **Destination Table** can be selected by clicking the **Select Table** button. Table Selection window appears as shown below. The desired table can be selected by scrolling or searching.

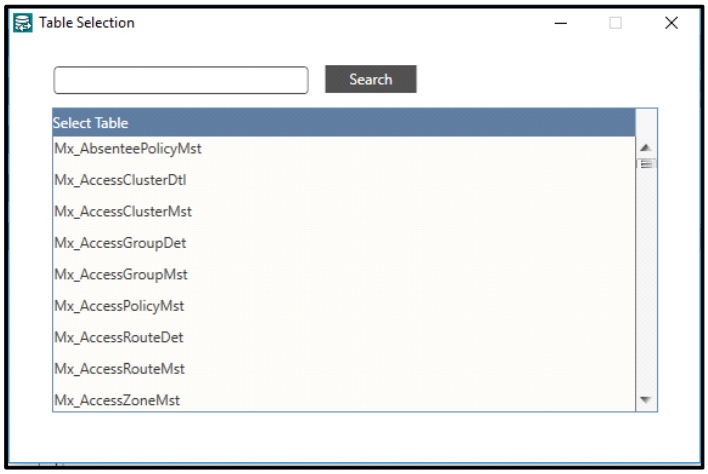
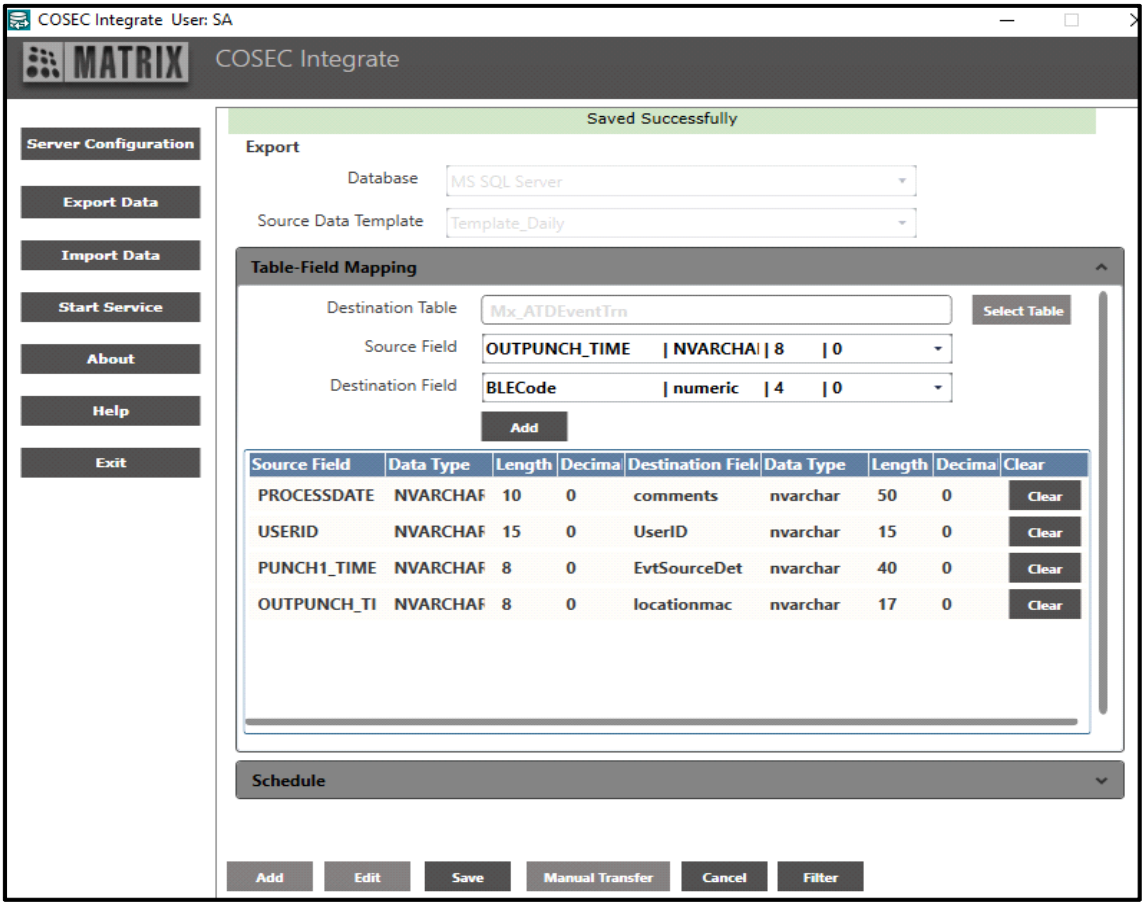


Table Field Mapping

Now the Admin user can start the mapping of the fields from the source database to that of the destination database as shown.



- Select the **Source field** from the COSEC database.
- Select the **Destination field** from the drop down options to map with the source field.
- Click on the **Add** button. The mapped fields will be visible in the bottom grid.

In the case of Attendance Events and Access Control Events the user needs to map the UserID and the EventDateTime_D source fields to fields in the destination table.

Map the UserID, PMonth and Pyear source fields to appropriate fields in the destination table in the case of the Monthly Attendance Summary.

Map the UserID and ProcessDate_D source fields to appropriate fields in the destination table in the case of the Daily Attendance Detail.

The mapping between the following data types is allowed. Only a warning message is shown in case of mismatch in data types.

Source data type	Destination data type
Text (char, varchar,varchar2...)	Number (numeric, int, bigint, smallint, float, number, double,int32...)
Text	Datetime formats(depending on the date format configured for DB server. If format matches, the record will be accepted)
Number	Text
Date Time	Text

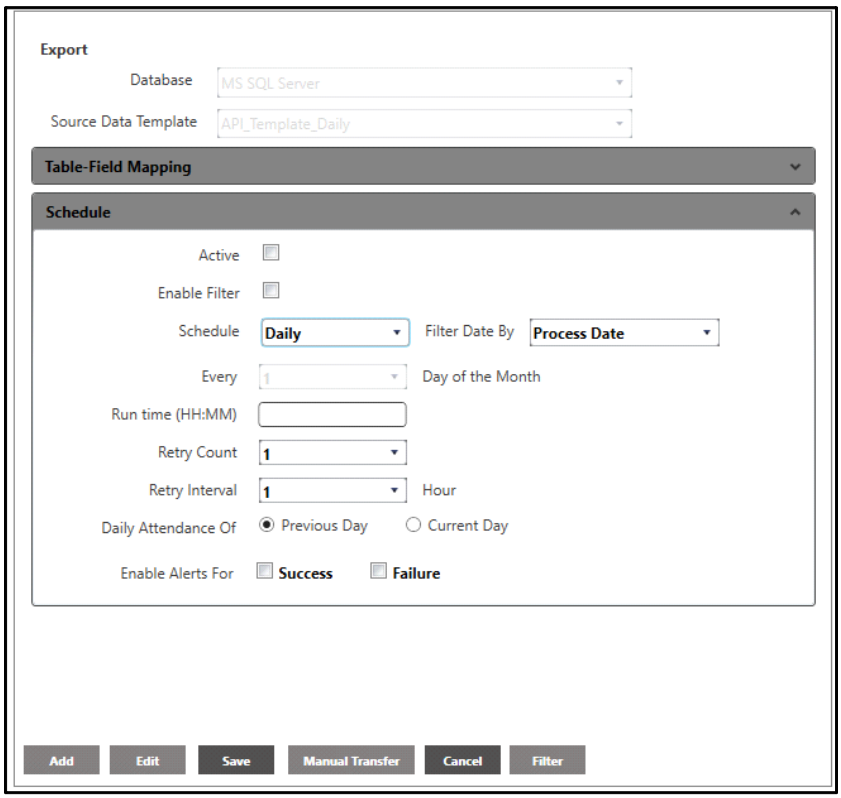
The mapping from Number and Date time to Date time and Number respectively is restricted.

Schedule

The **Schedule** section enables the Admin user to schedule the data export process. The schedule option vary based on the selected Source Data Template.

Daily Attendance Detail

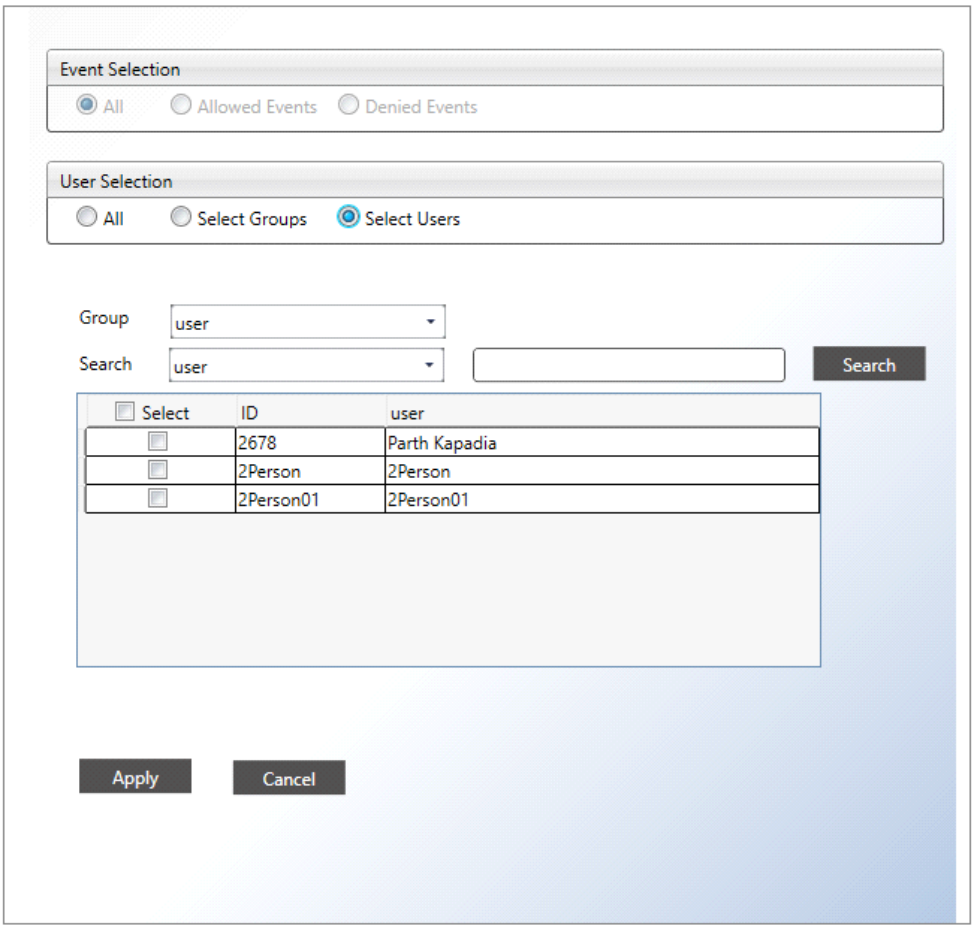
The **Daily Attendance detail** will have the following options as shown.



- Check the **Active** box to enable the schedule.
- The **Enable Filter** option is provided to enable the administrator to filter the events/users whose data is to be exported. Check this check box and click on the **Filter** button.

  The Event Selection and User Selection Filters pop-up appears.

Event Selection is applicable when Template selected is API_Template_ATDEvents or API_Template_ACSEvents or Template_ATDEvents or Template_ACSEvents.

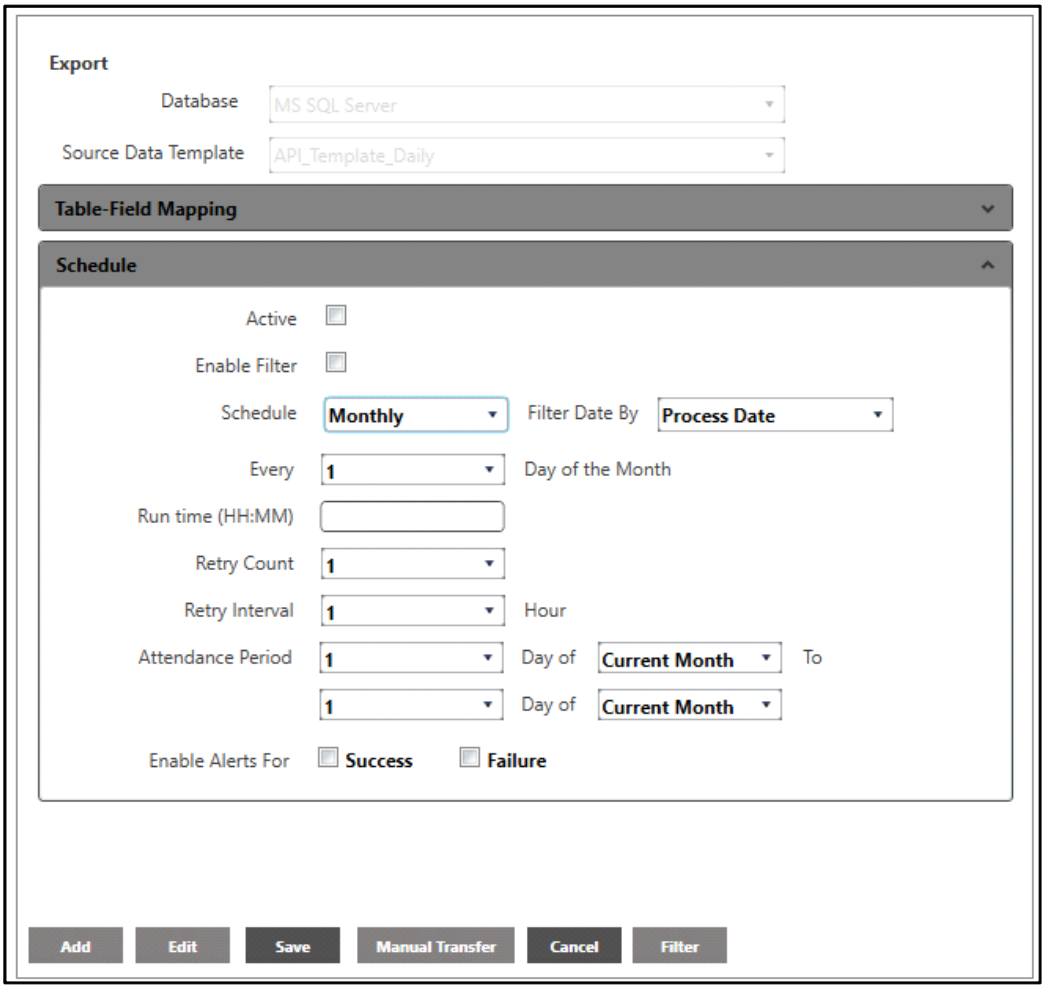


- **User Selection:** Select the desired option — All, Select Groups or Select Users.
  - If you select **All**, data of all the users will be exported.
  - If you select **Selected Groups**, the list of Groups appear in the grid.Select the check boxes of the desired Groups whose data is to be exported.
  - If you select **Selected Users**, the list of Users appear in the grid.Select the check boxes of the desired Users whose data is to be exported.

- Click **Apply** to save the configurations done or click **Cancel** to discard. The Filter pop-up closes.

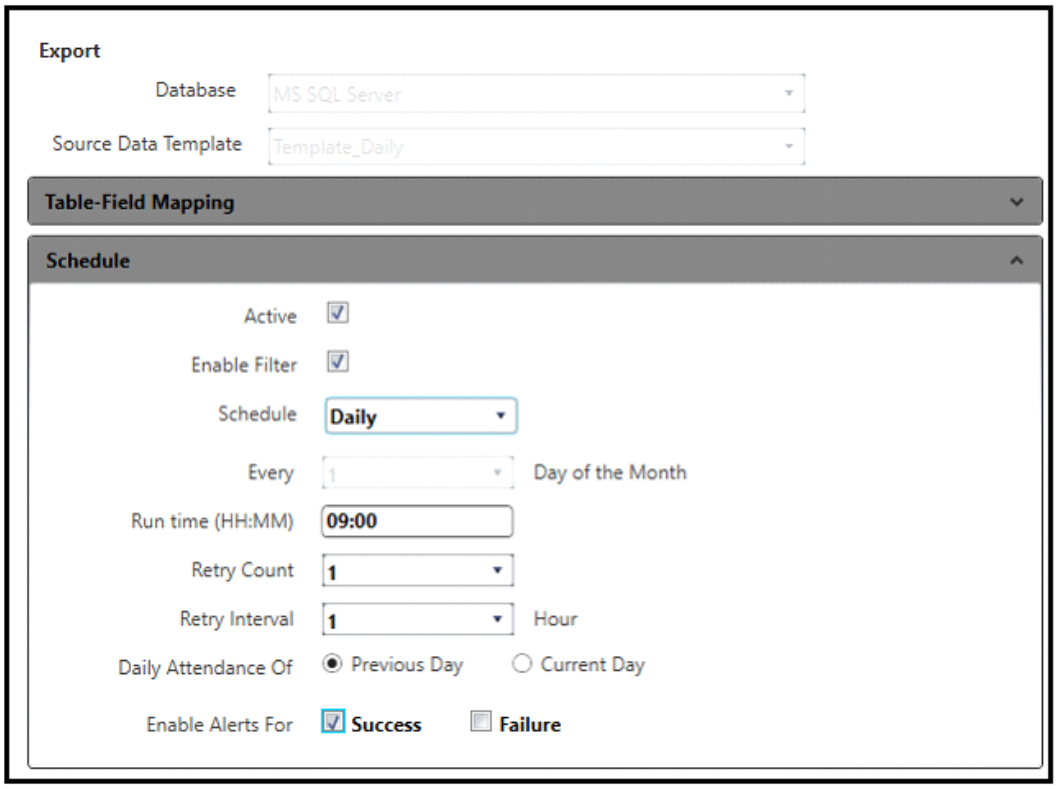
- In **Schedule,** select the desired option for data transfer— **Daily** or **Monthly**.

- On selection of **Monthly** option, user can set data transfer process to run only once in a month. By default, **Monthly** option would be selected.



- If you select Monthly, configure the **Attendance Period**, that is, the starting and the ending day of the attendance period for which the data is to be exported. Select the from Day of the Current/Previous Month to the Day of the Current/Previous Month

- When selecting **Daily** option for Schedule, the options appears as shown.



- If you select **Daily**, configure the **Daily Attendance of**. Configure to transfer data for either **Previous Day** attendance data or **Current Day** attendance data with respect to schedule run day.
- In **Every __ Day of the Month**, specify the day of the month on which the export process is to be run.
- Specify the **Run time** in HH:MM format when the export process is to be run.
- Set the **Retry Count** to retry again for export in case of export failure.
- Set the **Retry Interval** in hours from the drop down list. This parameter specifies the time period between successive retries.
- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

  Select the check boxes as per your requirement:

  Select **Success** check box to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

  Select **Failure** check box to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

  If you require Alerts for both the above events, select both the check boxes.

  In case of partial data transfer, that is, if both the above check boxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

  Example: There are in total 100 records which are to be transferred.

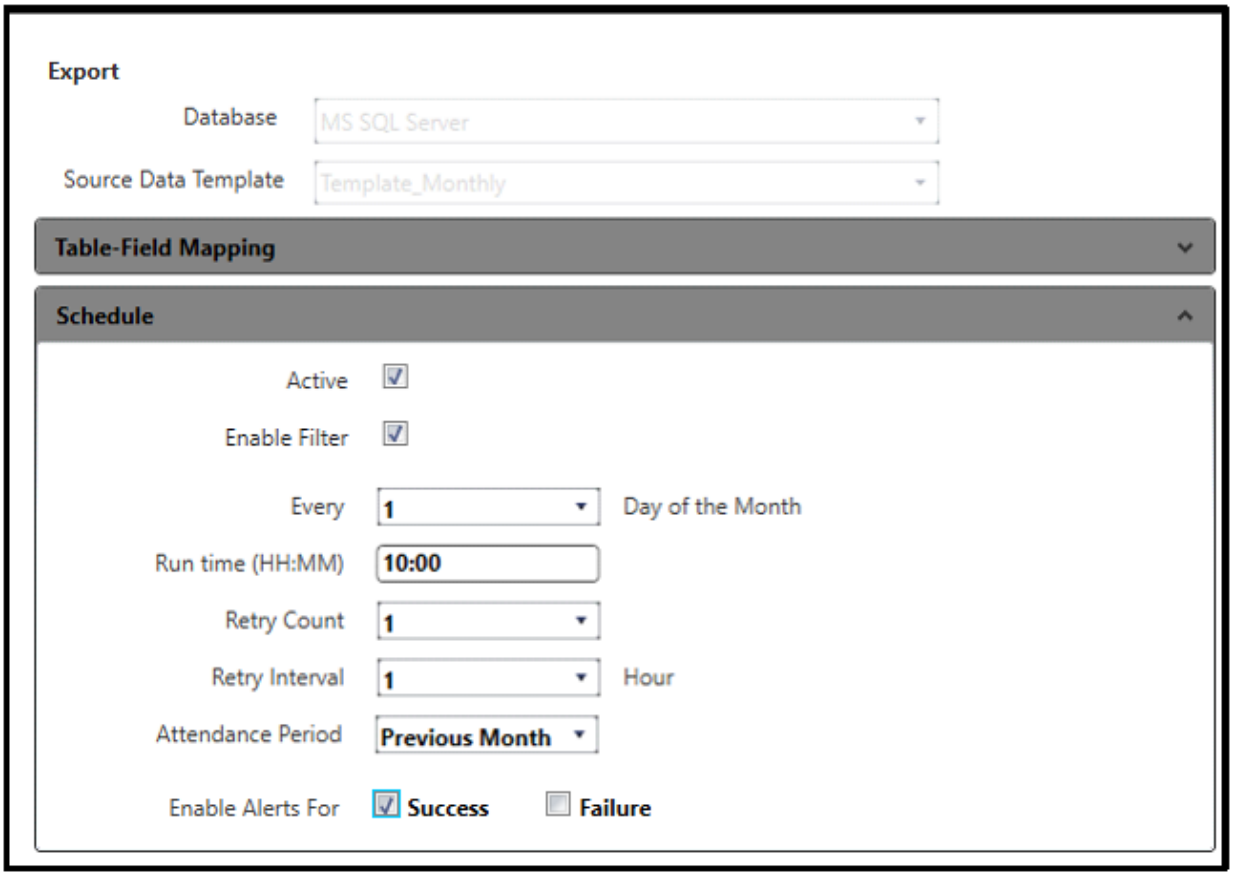
Now, out of 100 records, only 60 records are transferred Successfully and the remaining 40 records have Failed. Such data transfers are known as partial data transfers.

So here the connection status will be Failure and an alert will be sent to the configured COSEC Server along with the reason for failed data transfer.

It is to be supported for all integrate modes defined in COSEC Integrate where enable alerts provision is present i.e. for all the integration modes except for Custom Export-FP Template & Export FP Template to File.

Monthly Attendance Summary

The **Monthly Attendance Summary** will have the following unique options as shown.



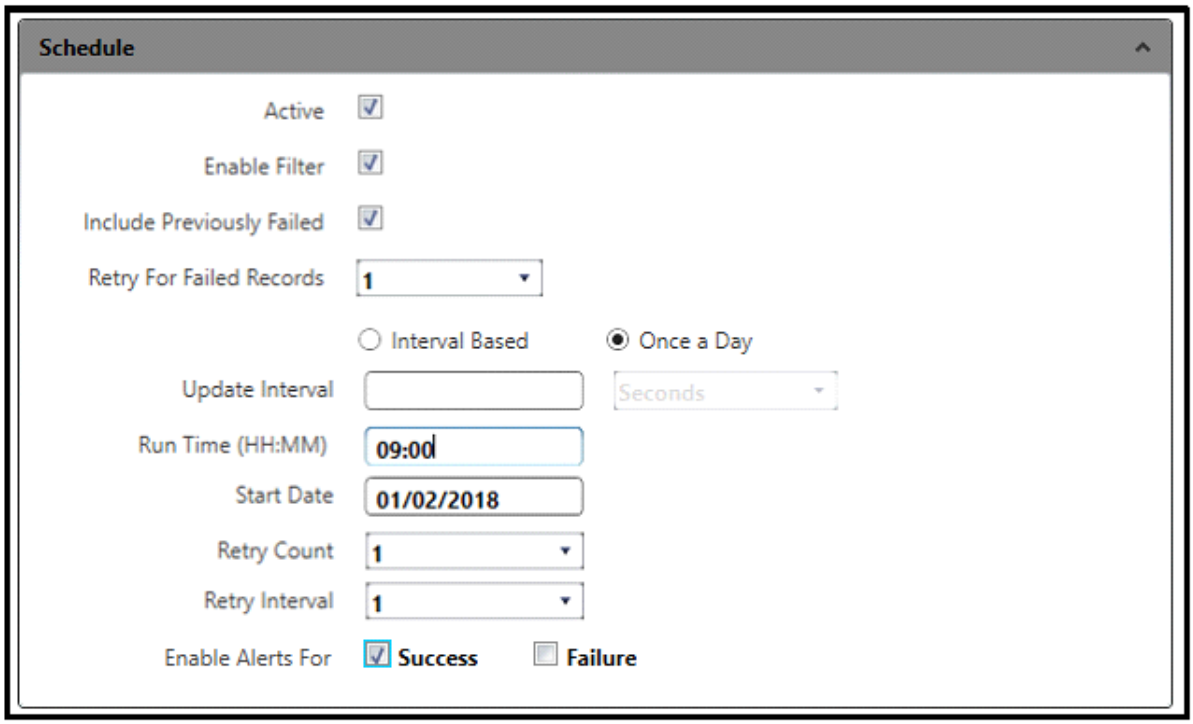
- The configuration of the parameters is similar to Daily Attendance Details, except the below mentioned parameter.

- Select the **Attendance Period** for which the monthly Attendance summary data is to be exported.The Admin user can select either the **Previous Month** or **Current Month** option.

  For details of other parameters, refer to “Daily Attendance Detail”.

Attendance Events or Access Control Events -Schedule

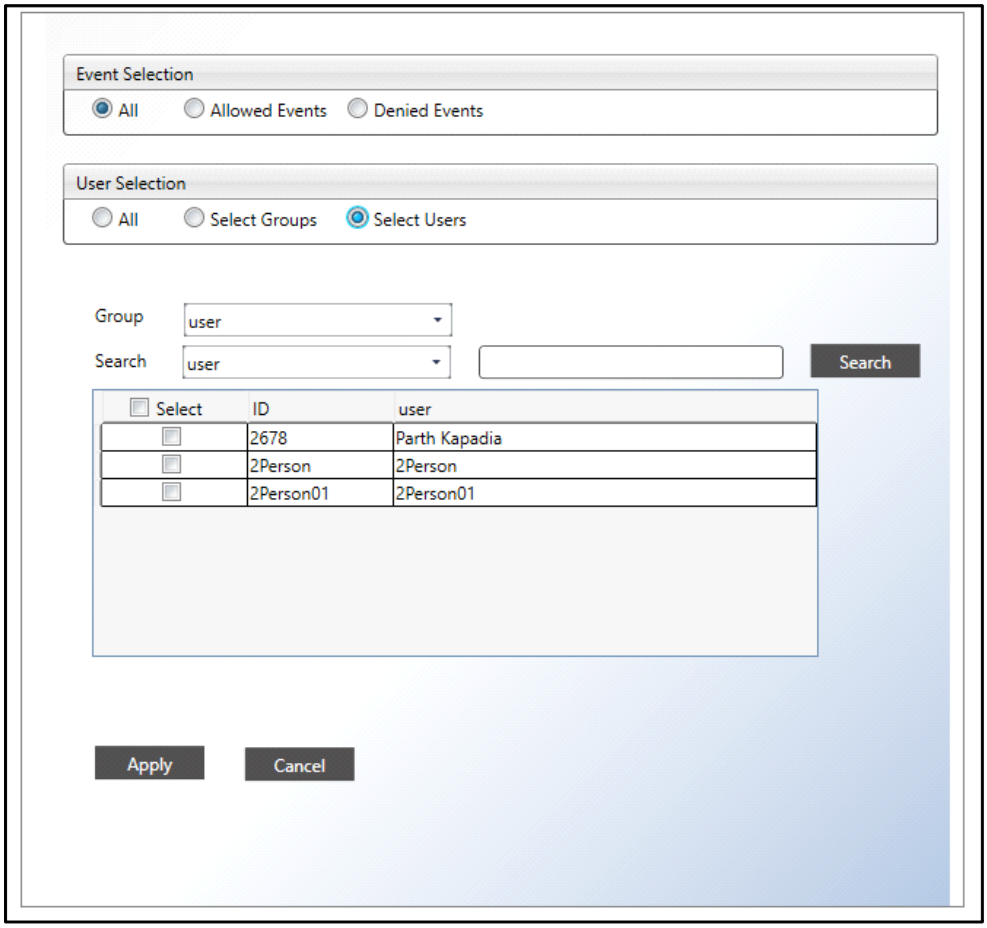
The following schedule options will be available.



- Select the **Active** check box to enable the schedule.
- The **Enable Filter** option is provided to enable the administrator to filter the events/users whose data is to be exported. Check this check box and click on the **Filter** button.

  The Event Selection and User Selection Filters pop-up appears.

Event Selection is applicable when Template selected is API_Template_ATDEvents or API_Template_ACSEvents or Template_ATDEvents or Template_ACSEvents.



- **Event Selection:** Select the desired option — All, Allowed Events or Denied Events.
  - If you select **Both**, all Allowed and Denied events will be exported.
  - If you select **Allowed Events**, only Allowed events will be exported.
  - If you select **Denied Events**, only Denied events will be exported.

- **User Selection:** Select the desired option — All, Select Groups or Select Users.
  - If you select **All**, data of all the users will be exported.
  - If you select **Selected Groups**, the list of Groups appear in the grid.Select the check boxes of the desired Groups whose data is to be exported.
  - If you select **Selected Users**, the list of Users appear in the grid.Select the check boxes of the desired Users whose data is to be exported.

- Click **Apply** to save the configurations done or click **Cancel** to discard. The Filter pop-up closes.

- **Include Previously Failed Records:** By enabling this check box, the records which are failed to export previously will be exported in the next retry.

  The IN-OUT Attendance events and Access Control events of user which are failed to export during database connection error will be exported when database connection is restored.

Only failed records due to Destination Table connectivity issue should be considered for this functionality.

- **Retry for Failed Records:** Select the number of times for which the failed records will be tried again for export.

- Select the desired option for the frequency at which the application will update the destination database — Interval Based, Once a Day

  Interval Based
  If you select this option configure the **Update Interval** and **Start Date**.

- Specify the **Update Interval** in seconds, minutes or hours to define the frequency at which the application will update the destination database.

  Once a Day
  If you select this option configure the **Run Time**, **Retry Count** and **Retry Interval**.

- Select the **Once a Day** option to schedule the export once every day at a scheduled **Run Time (HH:MM)**.

- Specify the **Start Date** from which the export process is to be initiated. The records from the start date to the present date will be exported.

- Specify the **Retry count** as the number of times for which system will try again to export the failed records with an interval gap of hours set in **Retry Interval**.

- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

  Select the check boxes as per your requirement:

  Select **Success** check box to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

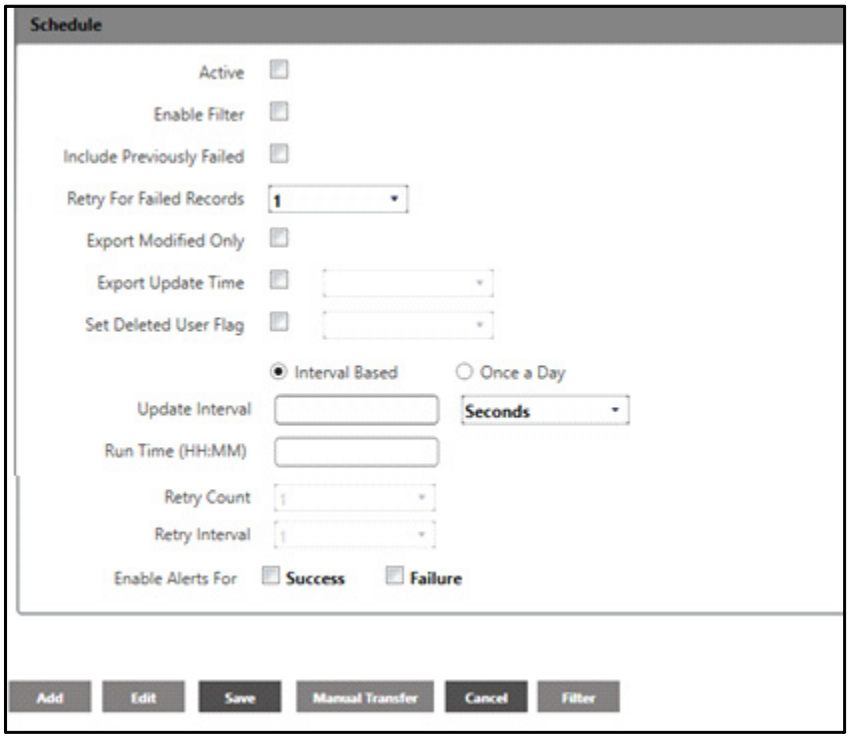
  Select **Failure** check box to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

  If you require Alerts for both the above events, select both the check boxes.

  In case of partial data transfer, that is, if both the above check boxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

Custom Template - User Details Template-Schedule

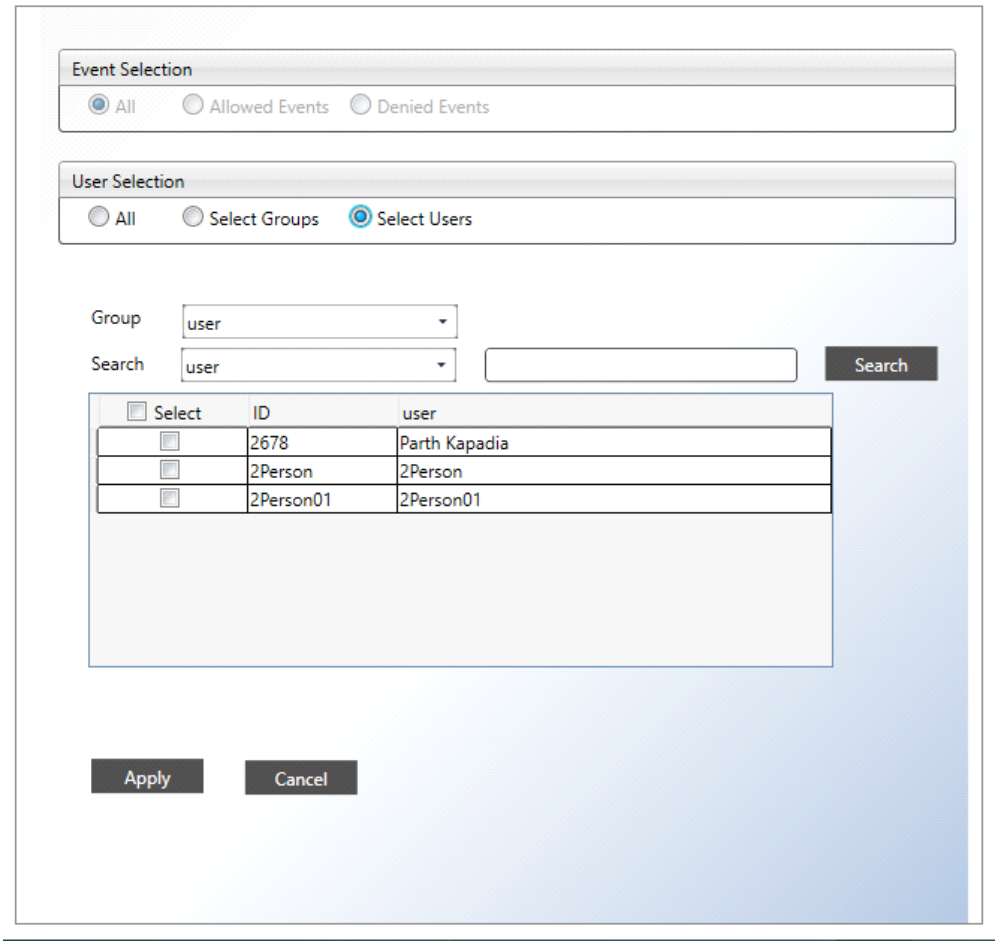
This is not a default template.Custom Templates can be added from the COSEC Web. These are then visible in the Integrate. To add Custom Templates refer to the User Guide, Admin Module > System Utilities > Export Data.



- Check the **Active** box to enable the schedule.
- The **Enable Filter** option is provided to enable the administrator to filter the events/users whose data is to be exported. Check this check box and click on the **Filter** button.

  The Event Selection and User Selection Filters pop-up appears.

Event Selection is applicable when Template selected is API_Template_ATDEvents or API_Template_ACSEvents or Template_ATDEvents or Template_ACSEvents.



- **User Selection:** Select the desired option — All, Select Groups or Select Users.
  - If you select **All**, data of all the users will be exported.
  - If you select **Selected Groups**, the list of Groups appear in the grid.Select the check boxes of the desired Groups whose data is to be exported.
  - If you select **Selected Users**, the list of Users appear in the grid.Select the check boxes of the desired Users whose data is to be exported.

- Click **Apply** to save the configurations done or click **Cancel** to discard. The Filter pop-up closes.

- **Include Previously Failed:** By enabling this check box, the records which are failed to export previously will be exported in the next retry.

- **Retry for Failed Records:** Select the number of times for which the failed records will be tried again for export.

- **Export Modified Only:** Enabling this check box will export only the changed or updated user details. Eg: at 10:00 hrs, details of 100 users is exported. At 14:00 hrs (interval based export) the change in 20 users is found. So details of only 20 users will be exported.

- **Export Update Time:** When the export of only modified records is done, then the time at which modified records were exported will get updated for the respective records in destination fields. Eg: For the modified 20 users, the timing will be displayed as 14:00 hours in the destination table..

    - You can select the field from the drop down list where the export timing of modified records will be updated. Eg: Suppose you select Edatetime from the options, then the date time of export process will be displayed in Edatetime column of destination server.

- **Set Deleted User Flag:** Suppose the user is deleted from the COSEC system. But that user is already exported in the destination table. So by enabling this you can set the flag to 1 for the respective deleted users when next export will be done.

    - Select the field where the flag is to be updated.

- Select the desired option for the frequency at which the application will update the destination database — Interval Based, Once a Day

  Interval Based
  If you select this option configure the **Update Interval** and **Start Date**.

- Specify the **Update Interval** in seconds, minutes or hours to define the frequency at which the application will update the destination database.

  Once a Day
  If you select this option configure the **Run Time**, **Retry Count** and **Retry Interval**.

- Select the **Once a Day** option to schedule the export once every day at a scheduled **Run Time (HH:MM)**.

- Specify the **Retry count** as the number of times for which system will try again to export the failed records with an interval gap of hours set in **Retry Interval**.

- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

  Select the check boxes as per your requirement:

  Select **Success** check box to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

  Select **Failure** check box to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

  If you require Alerts for both the above events, select both the check boxes.

  In case of partial data transfer, that is, if both the above check boxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

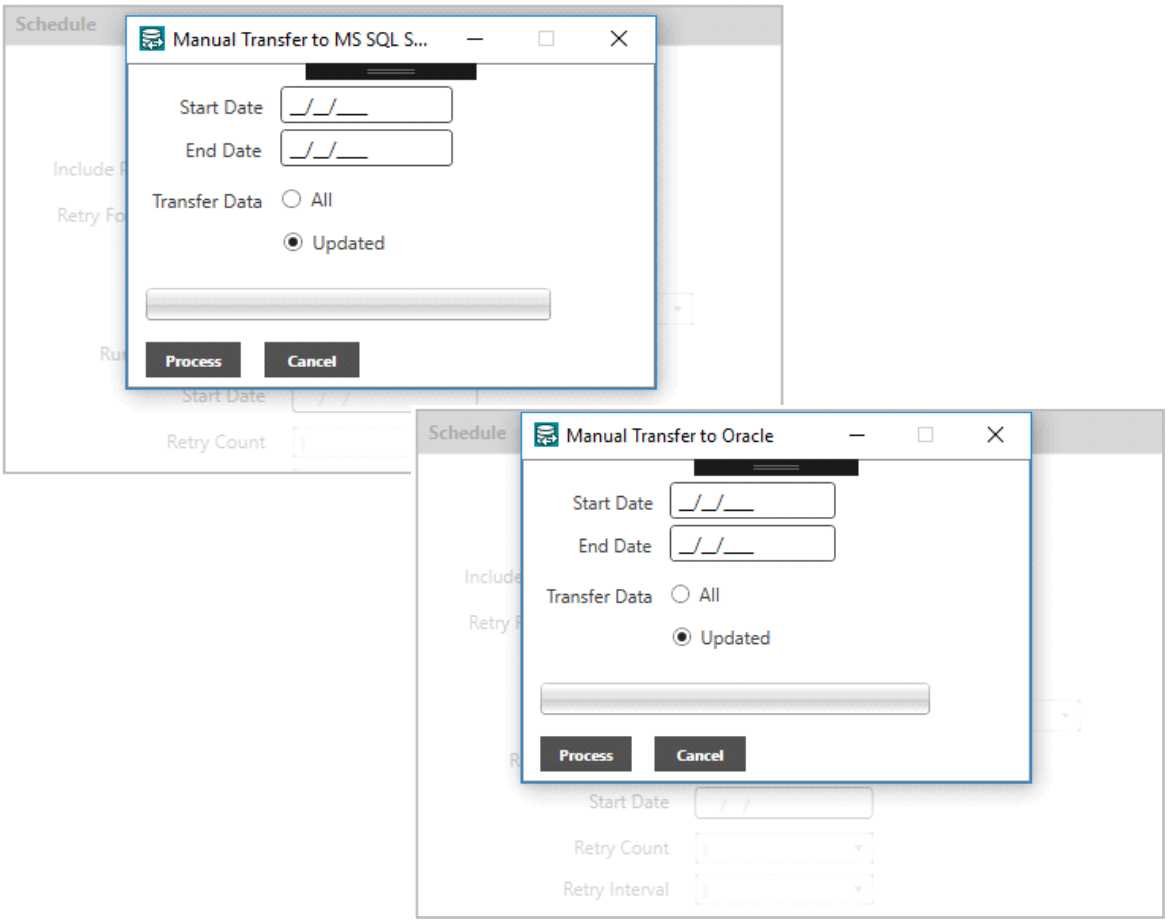
Manual Transfer

The Manual Transfer option provides the Admin user the flexibility to export data of a specific time period as and when required. In order to access this functionality click on the **Stop Service** button to stop the COSEC INTEGRATE service.

Click the **Export Data** button.

On the **Export Data** page, edit and save the export settings as per your requirement.

Click the **Manual Transfer** button. The following window appears for *Manual Transfer to MS SQL Server* and for Oracle *Manual Transfer to Oracle*.



Enter the **Start Date** and **End Date**.

Select the **Transfer Data** mode— **All** or **Updated**.

All: All the past data falling within the selected date range will be transferred.

Updated: All the updated data falling within the selected date range will be transferred.

Click the **Process** button. The data of the specified time period will be exported to the destination table.

Export to Postgre Server

The application allows the administrator to export device data and event logs from the COSEC application database to predefined tables of the Postgre SQL database. The Postgre SQL database needs to have the following tables in the database:

- **devices**
- **device logs**

The devices table holds the basic data of the COSEC devices like deviceid, serial number (MAC address), ipaddress. This information can be obtained by viewing the ControllerList view of the COSEC database. The MAC addresses however can be directly obtained from the devices. This table holds information on the last ping time and the last log download date for each of the devices.

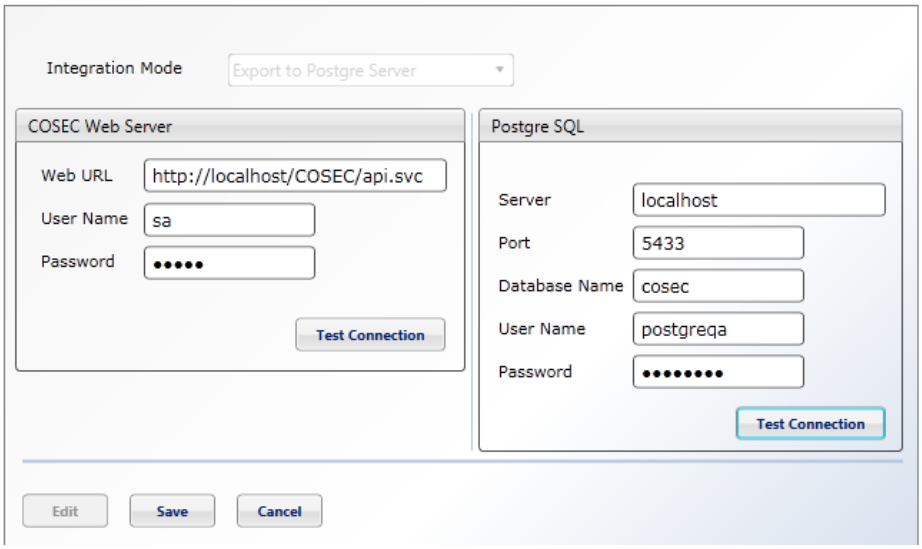
The devicelogs table receives the event logs from the COSEC database received from each of the COSEC devices.

Server Configuration

In order to configure this functionality click on the **Server Configuration** button. Select the **Export to Postgre SQL (CGG)** option in the **Integration Mode** field.

Integrate supports Export to Postgre SQL from PostgreSQL 10.23 to PostgreSQL 12.18

Click on **Edit**. The following page appears.



In the **COSEC Web Server** section:

- Specify the web url of the api service of the COSEC WEB application as shown.
- Enter the User Name and Password of the sa user as set in the COSEC WEB application.

In the **Postgre SQL** section:

- **Server**: Enter the Postgre database server IP address or its network name.
- **Port**: Specify the TCP connection port as configured in the Postgre database server.
- **Database Name**: Specify the destination database name of the Postgre database.
- **User Name**: Specify the database owner ID in this field.
- **Password**: Enter the password of the Database owner as per the site settings.

The **Test Connection** button is provided to test the connections with the web server as well as the Postgre SQL Server database.

Click on **Save** once done.

The administrator can now start the COSEC INTEGRATE service by clicking on the **Start Service** button as explained earlier.

The Admin can now perform Export Data Configuration which is same as MSSQL/Oracle. For more information, refer *"Export Data Configuration"* of MSQL/Oracle Server.

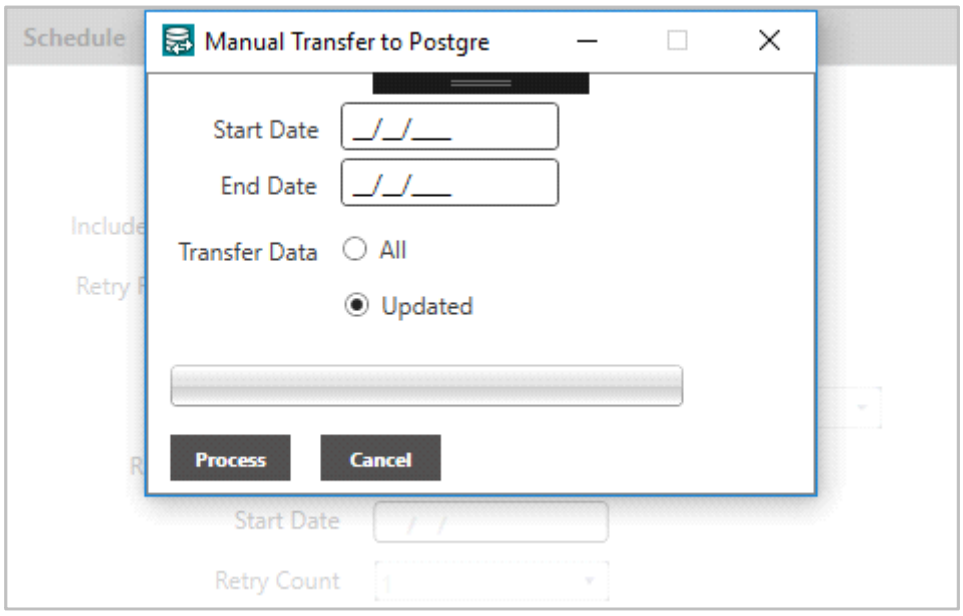
Manual Transfer

The Manual Transfer option provides the Admin user the flexibility to export data of a specific time period as and when required. In order to access this functionality click on the **Stop Service** button to stop the COSEC INTEGRATE service.

Click the **Export Data** button.

On the **Export Data** page, edit and save the export settings as per your requirement.

Click the **Manual Transfer** button. The following window appears for *Manual Transfer to Postgre*.



Enter the **Start Date** and **End Date**.

Select the **Transfer Data** mode— **All** or **Updated**.

All: All the past data falling within the selected date range will be transferred.
Updated: All the updated data falling within the selected date range will be transferred.

Click the **Process** button. The data of the specified time period will be exported to the destination table.

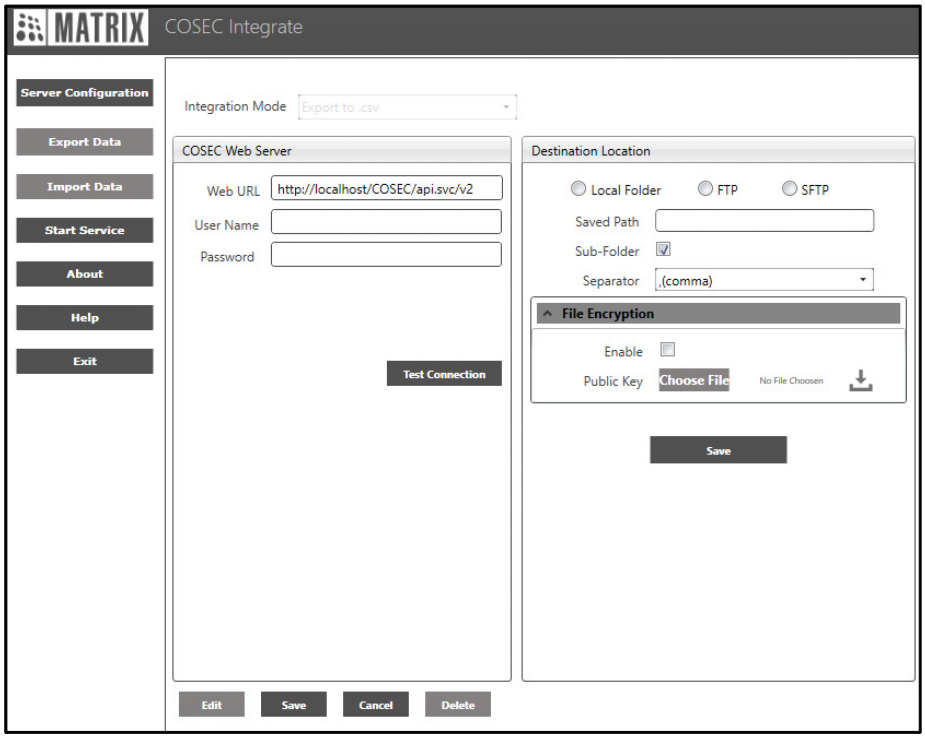
Export to CSV

The application allows the administrator to export data related to various user events to a **.csv file** which can be stored at a specific location on FTP/SFTP server or in a local folder on the hard disk.

Click **Server Configuration.**

In **Integration Mode** select **Export to .csv**.

Click **Edit** to configure the parameters.



Under **COSEC Web Server** configure the following:

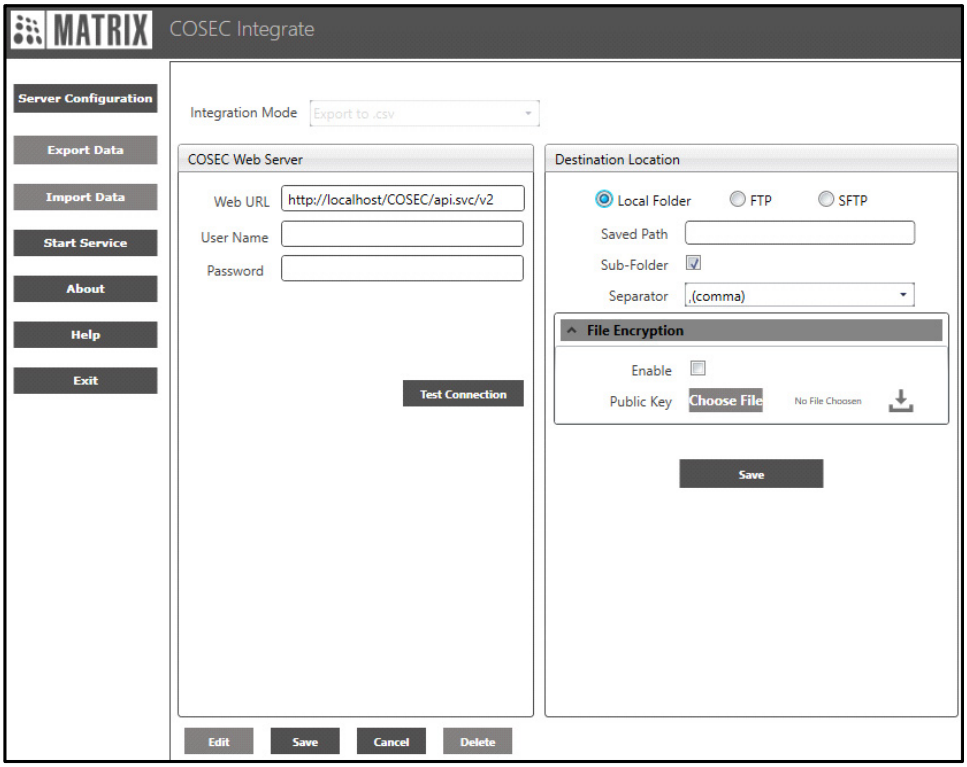
- **Web URL:** Specify the Web URL of the API service of the COSEC WEB Server application.
- **User Name:** Enter the User Name as **sa** as set for the COSEC WEB Server application.
- **Password:** Enter the Password as set for the COSEC WEB Server application.
- Click **Save**.
- Click **Test Connection** to confirm that the connectivity is established with the COSEC WEB Server application.

Under **Destination Location**, configure the following:

- Select the desired option — Local Folder, FTP or SFTP.

Local Folder

- If you select **Local Folder**, configure the following:



- **Saved Path:** Specify the Path at which the exported files are to be stored.
- **Sub-Folders:** Select the Sub-Folders check box to enable a folder hierarchy to be created at the export destination for the exported file.
- **Separator:** Select the separator which will be used to separate the fields in the exported file.

Click **File Encryption** collapsible panel and configure the following:

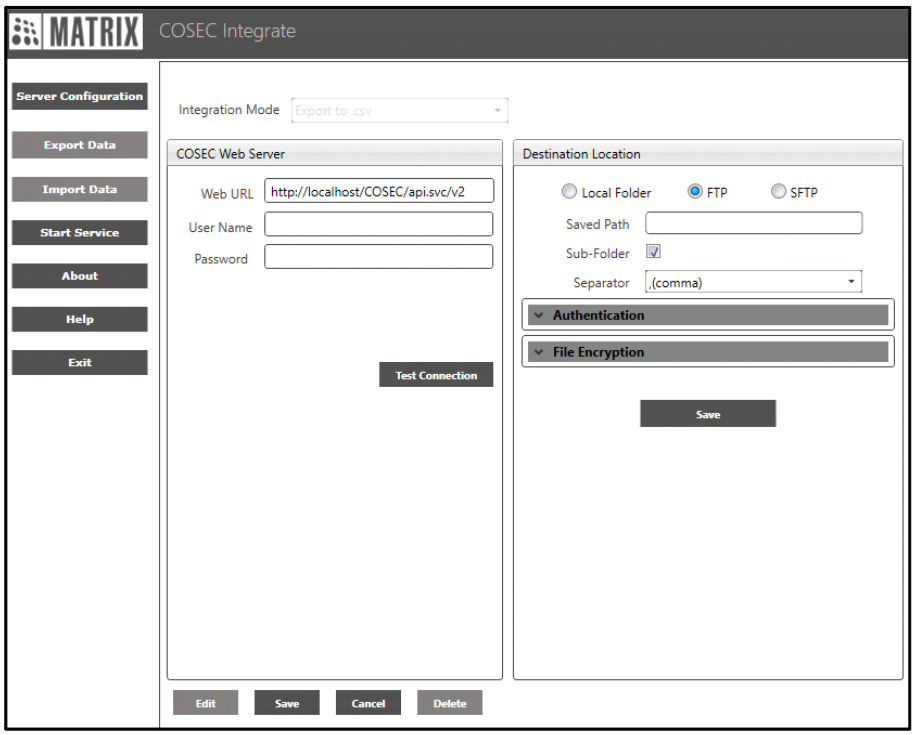
The file will be encrypted using PGP (Pretty Good Privacy) encryption method using AES algorithm.

- **Enable:** Select this check box to enable encryption. If enabled the file will be encrypted using the Public Key provided by the Third Party and then will be saved on the Path.
- **Public Key:** Click **Choose** and select the key file which is to be used for encryption. This will be provided by the Third Party. The maximum file size supported is 5MB.

- *If File Encryption check box is enabled, then Third Party must take the last updated file based on time stamping from the Saved Path.*
- Click **Save**.

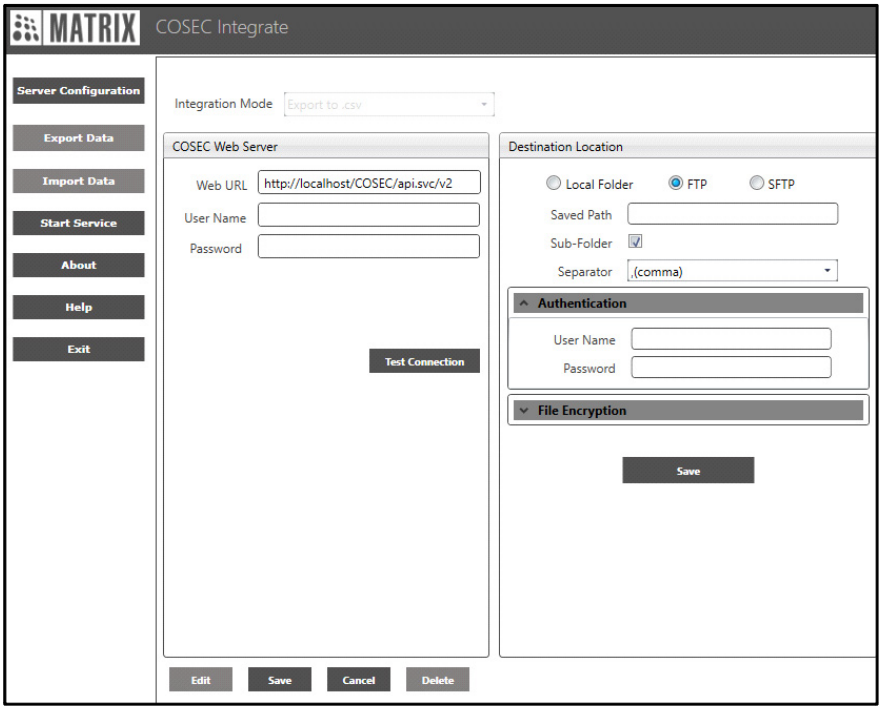
FTP

- If you select **FTP**, configure the following:



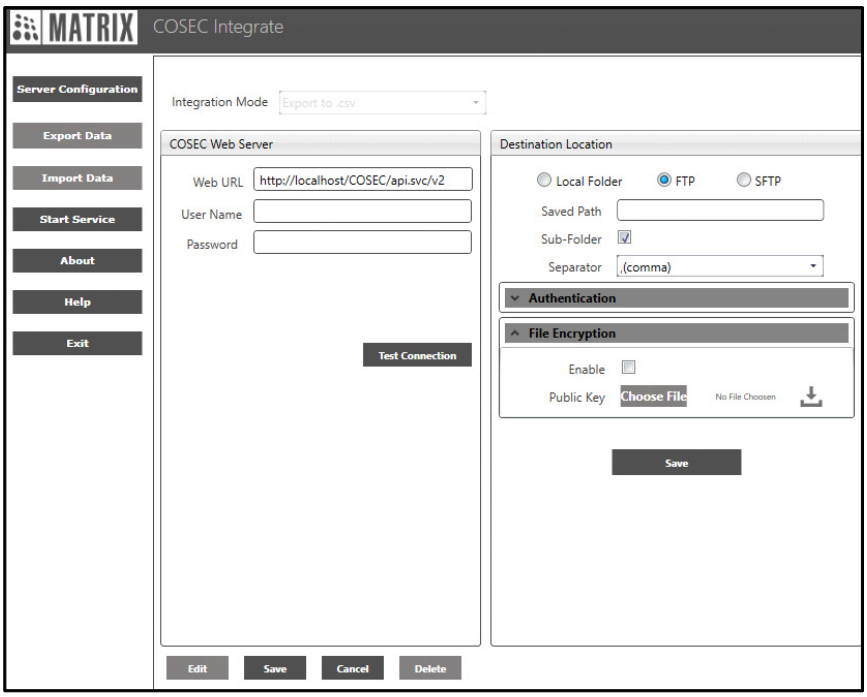
- **Saved Path:** Specify the Path at which the exported files are to be stored.
- **Sub-Folders:** Select the Sub-Folders check box to enable a folder hierarchy to be created at the export destination for the exported file.
- **Separator:** Select the separator which will be used to separate the fields in the exported file.

Click **Authentication** collapsible panel and configure the following:



- **User Name:** Enter the User Name to be used for authentication while accessing the Path.
- **Password:** Enter the Password to be used for authentication while accessing the Path.

Click **File Encryption** collapsible panel and configure the following:



The file will be encrypted using PGP (Pretty Good Privacy) encryption method using AES algorithm.

- **Enable:** Select this check box to enable encryption. If enabled the file will be encrypted using the Public Key provided by the Third Party and then will be saved on the Path.

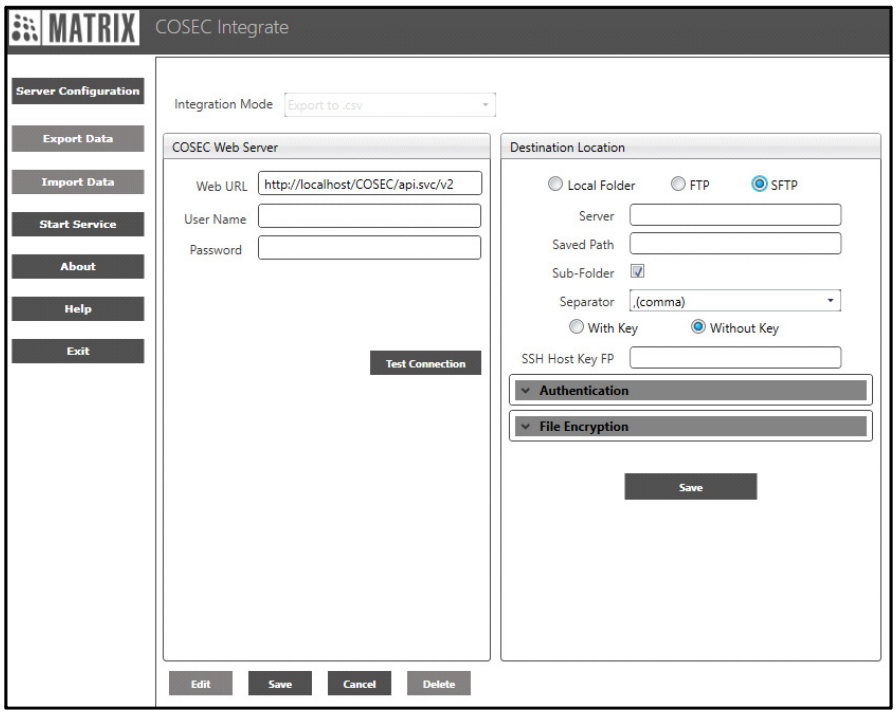
- **Public Key:** Click **Choose** and select the key file which is to be used for encryption. This will be provided by the Third Party. Maximum file size supported is 5 MB.

If File Encryption check box is enabled, then Third Party must take the last updated file based on time stamping from the Saved Path.

- Click **Save**.

SFTP

- If you select **SFTP**, configure the following:



- **Server:** Specify the SFTP Server IP Address where the exported files are to be stored.

  COSEC Integrate communicates with the SFTP Server using the default port number 22. If you wish to use any other port, then you need to configure the same in the format Server IP Address:Port. For example if Port 33 is to be used then configure the Server as 192.168.104.20:33.

- **Saved Path:** Specify the Path at which the exported files are to be stored.

- **Sub-Folders:** Select the Sub-Folders check box to enable a folder hierarchy to be created at the export destination for the exported file.

- **Separator:** Select the separator which will be used to separate the fields in the exported file.

- For additional authentication and security, you can select the desired option — **With Key** or **Without Key**.

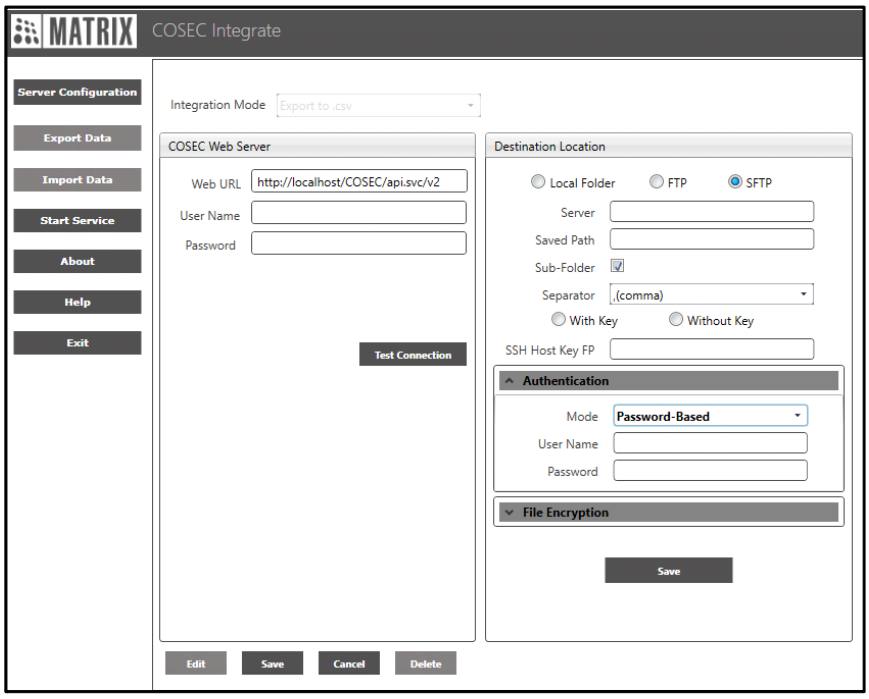
  If you select **With Key**, then configure the **SSH Host Key FP**.

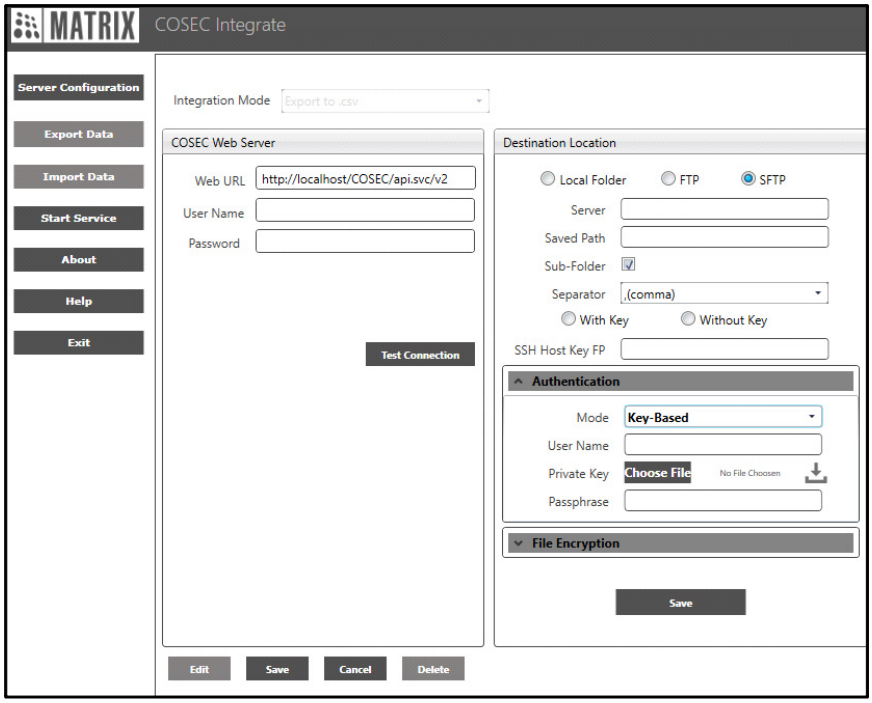
The **SSH Host Key FP** servers as a unique identifier for the Server. This is a cryptographic representation of the Servers Public Key. It is used to verify the authenticity of the Server during the connection process. It is used to ensure that the Server the client is connecting to is the same Server that it connected with previously.

This key is provided by the Administrator of the SFTP Server to the clients.

If you select **Without Key**, then no key is required.

Click **Authentication** collapsible panel and configure the following:





- **Mode:** Select the desired mode for authentication — **Password-Based**, **Key-Based**.

If you select **Password-Based,** configure the following:

In Password-Based, when a client signs in, the Server checks the User Name and Password combination and then approves/denies the request.

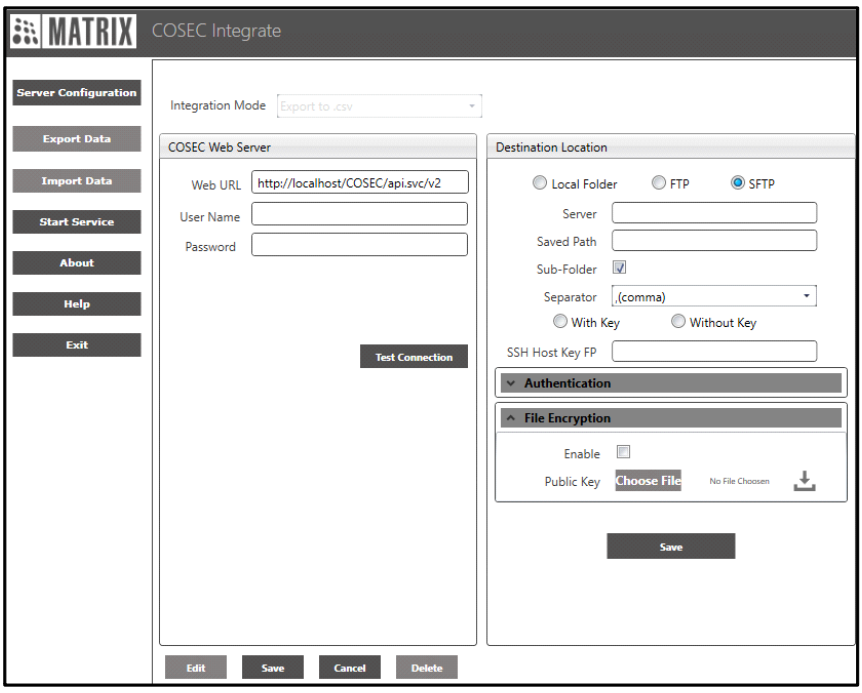
- **User Name:** Enter the User Name to be used for authentication while accessing the Path.
- **Password:** Enter the Password to be used for authentication while accessing the Path.

If you select **Key-Based,** configure the User Name, Private Key and Passphrase.

In Key-Based, when a client signs in, a pair of keys — Private and Public — are used for authentication. The Public Key is uploaded in the SFTP Server while the Private Key is provided to the client.

- **User Name:** Enter the User Name to be used for authentication while accessing the Path.
- **Private Key:** Click **Choose** and select the key file which is to be used for authentication.
- **Passphrase:** Enter the Passphrase. This is used in combination with the Private Key to acquire the SFTP Server access.

Click **File Encryption** collapsible panel and configure the following:



The file will be encrypted using PGP (Pretty Good Privacy) encryption method using AES algorithm.

- **Enable:** Select this check box to enable encryption. If enabled the file will be encrypted using the Public Key provided by the Third Party and then will be saved on the Path.

- **Public Key:** Click **Choose** and select the key file which is to be used for encryption. This will be provided by the Third Party. Maximum file size supported is 5 MB.

If File Encryption check box is enabled, then Third Party must take the last updated file based on time stamping from the Saved Path.

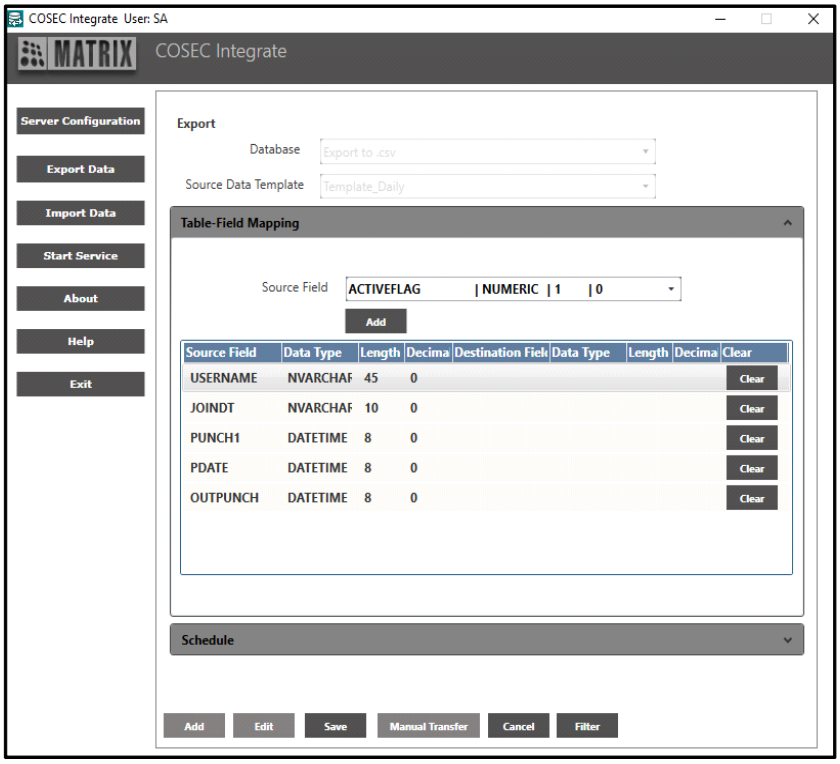
- Click **Save**.

Export Data Configuration

This option enables the Admin user to specify the fields whose values are to be exported to the .csv file.

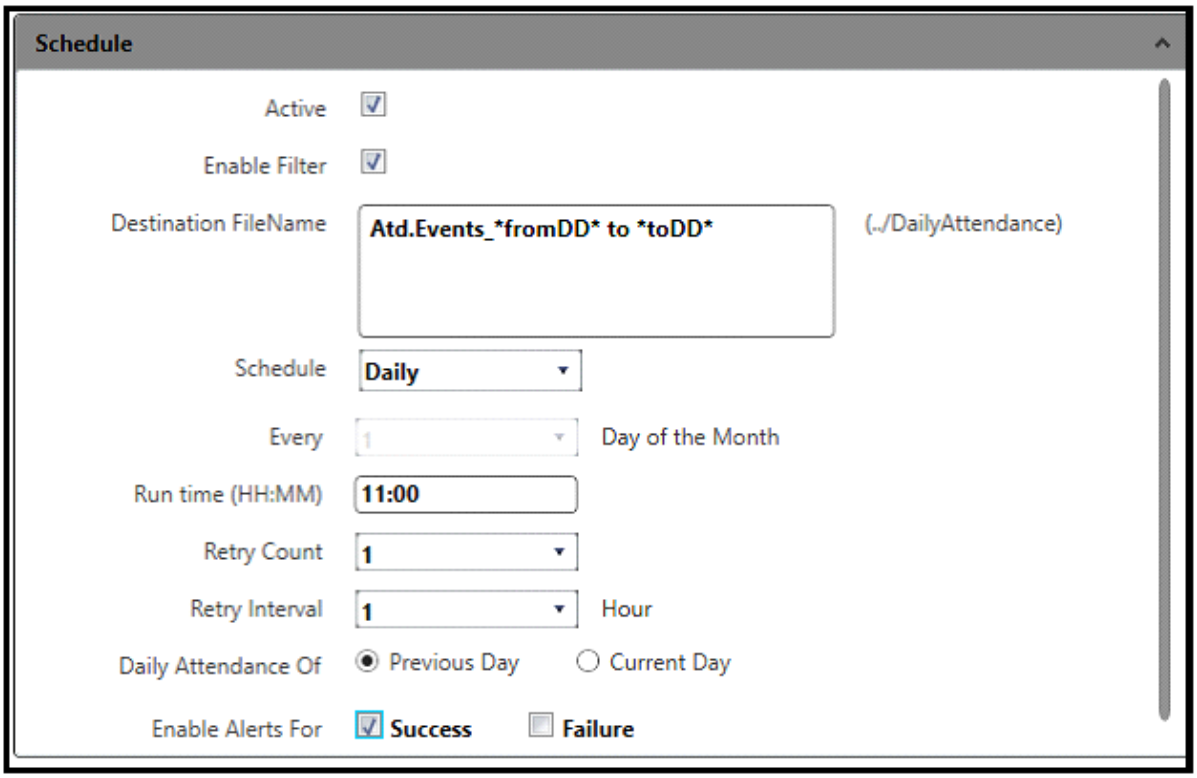
Each database views would provide the relevant fields whose values can be exported from the COSEC database.

Source Data Template: Select the required data template and click on the **Edit** button. Now the admin user can start the selection of the fields from the source database as shown.



Select the **Source field** from the drop down list and click on the **Add** button. The field will be added to the grid as shown above.You can remove a selected field by clicking on **Clear** button for the respective field.

The **Schedule** section enables the admin user to schedule the data export process. The schedule option vary based on the selected Source Data Template. The **Daily Attendance detail** will have the following options as shown.



- Check the **Active** box to enable the schedule.

- The **Enable Filter** option is provided to enable the administrator to filter the users whose data is to be exported. Check this box and click on the **Filter** button. The Multiple selection window appears. Select the users whose data is to be exported.

- **Destination FileName:** Enter a filename in this field. The max characters can be 200. The file name can include Alphanumeric characters, Special characters like **!@#$%^&()_-+=[]{};',.<space> A-Z a-z 0-9 and pair of asterisks(**).**

You can type '*' in the text-area. This will show the list of variables as per the template type. Select the desired variable. It will be added by appending '*' at the end. During the deployment of file, the current date-time values will be fetched and replaced instead of these variables.

1. When '' is typed in text area, another '*' will be added automatically as it is allowed only in pair.*
*2. When you are entering filename and the appearing variable list is disturbing then you can enter **ESC** key to hide the variables for the instance.*

Example of Variables:
***gdateDD*-** This variable will fetch and show the date on which the data is exported and file is generated. Similarly variables are available for month, year, hours. minute and seconds.

***fromDD*-** This variable will fetch and show the date value of the Start Date. Similarly variables are available for month and year. Suppose Start date is 1st date of current month. If current month is Feb so the value of variable will be “1”.

***toDD*-** This variable will fetch and show the date value of the End Date. Similarly variables are available for month and year. Suppose End date is Last date of current month. If current month is Feb so the value of variable will be “28”.

atdMM*- This variable will fetch and show the month value of attendance period. Similarly variables is available for year.

Example : A new template has been configured with Destination FileName = 'Atd. Events_*fromDD*-*fromMM*-*fromYY*_to_*toDD*-*toMM*-*toYY*

Now, this template is manually exported with date-range, 01-01-2016 to 02-01-2016. Thus, the exported file name will be Atd. Events_01-01-16_to_02-01-16.csv

The system creates a folder named **DailyAttendance** in the path as specified in the server configuration.

- **Schedule**: Select the option as **Daily** or **Monthly** to run the schedule
    - For **monthly schedule** specify the **day** of the month on which the export process is to be run. And select the **Attendance period** i.e. starting and the ending day of the attendance period for which the data is to be exported.

    - For **daily schedule** select the **Daily Attendance** of Previous Day or Current Day for which the attendance details is to be exported.

- **Run time:** Specify the Run time in HH:MM format when the export process is to be run.

- **Retry Count:** Set the Retry Count from the drop down list to retry the export if it gets failed.

- **Retry Interval:** Select the Retry Interval in hours from the drop down list. This parameter specifies the time period between successive retries.

- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

  Select the checkboxes as per your requirement:

  Select **Success** checkbox to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

  Select **Failure** checkbox to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

  If you require Alerts for both the above events, select both the check boxes.

  In case of partial data transfer i.e. if both the above checkboxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

  Example: There are in total 100 records which are to be transferred.

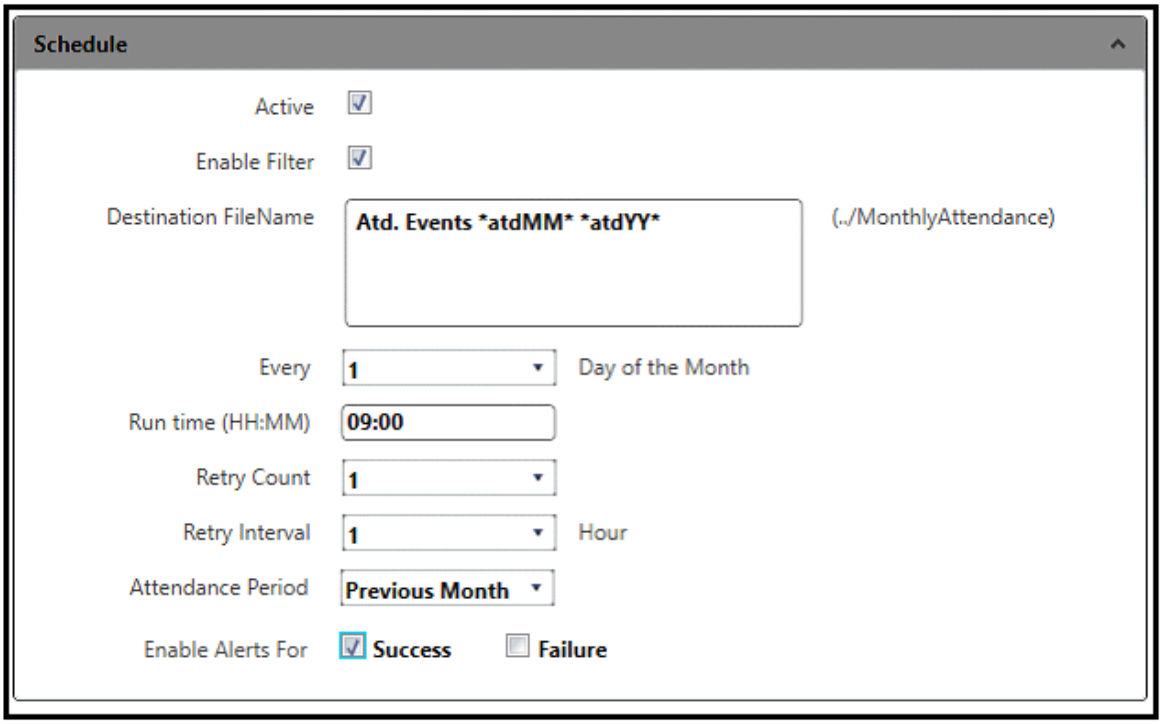
  Now, out of 100 records, only 60 records are transferred Successfully and the remaining 40 records have Failed. Such data transfers are known as partial data transfers.

  So here the connection status will be Failure and an alert will be sent to the configured COSEC Server along with the reason for failed data transfer.

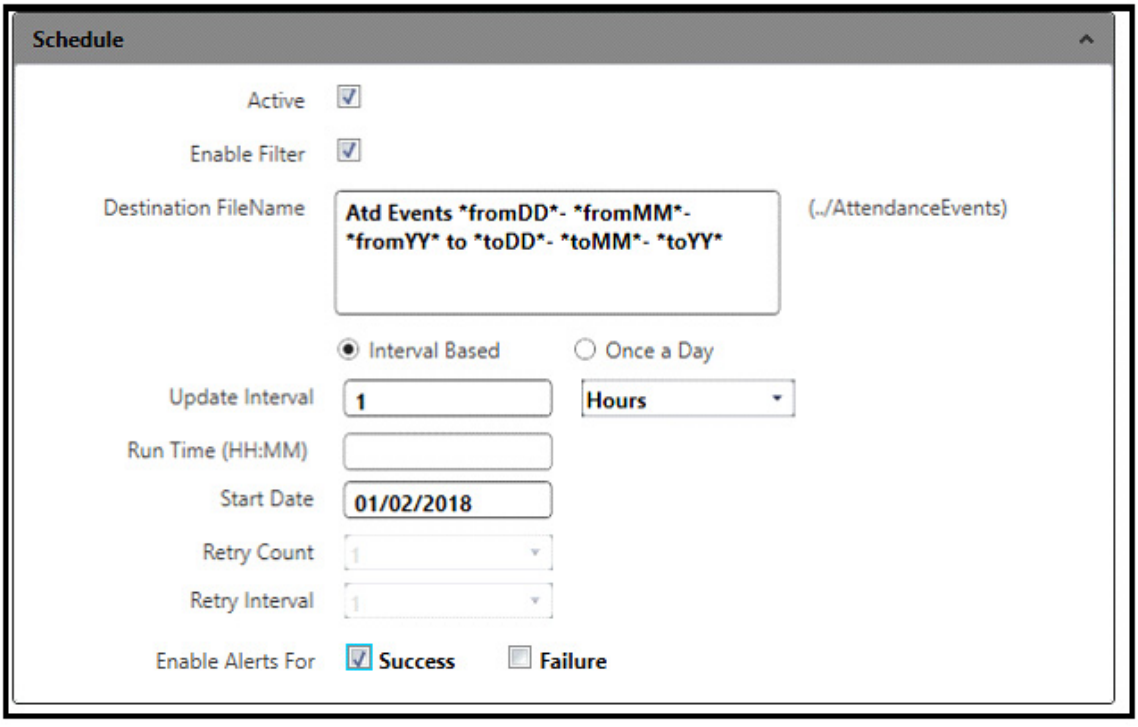
It is to be supported for all integrate modes defined in COSEC Integrate where enable alerts provision is present i.e. for all the integration modes except for Custom Export-FP Template & Export FP Template to File.

Then click on **Save** button to save the schedule. Now you can start service for running the export schedule. See "Exporting Data" on page 36.

The **Monthly Template** will have the same options as mentioned above except the **Attendance Period** option.



The **ATD Events** and **ACS Events** templates' schedule is shown below.



- Specify the **Update Interval** in seconds, minutes or hours to define the frequency at which the application will export the data to the csv file.
- Specify the **Start Date** from which the export process is to be initiated.

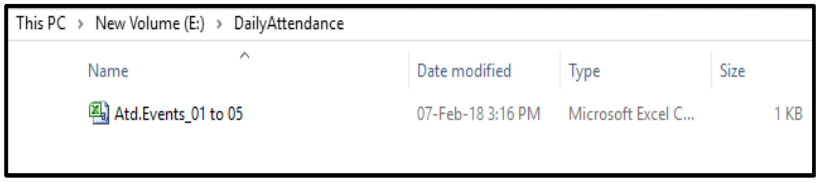
In the csv format for exporting data, the records in the csv file would be sorted in the same order as they were added.

Exporting Data

Schedule Export

For starting the export of file, after saving the schedule; click on **Start Service** button. The exported file will be exported at the path specified in Server configuration.

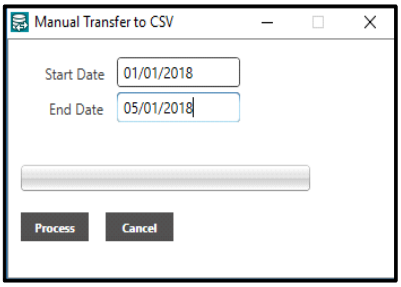
The Daily Attendance exported file is shown below.

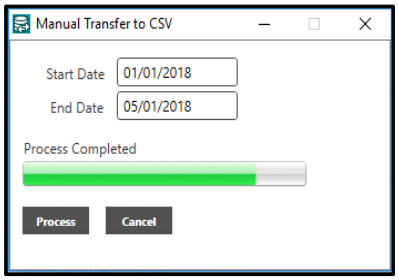


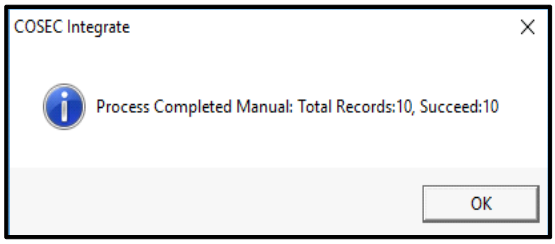
	A	B	C	D	E	F
1	Chirag		1-1-18 12:00 AM	9:00:00	19:00:00	
2	Khushbu		1-1-18 12:00 AM			
3	Chirag		2-1-18 12:00 AM	9:15:00	19:30:00	
4	Khushbu		2-1-18 12:00 AM			
5	Chirag		3-1-18 12:00 AM	9:00:54	19:00:53	
6	Khushbu		3-1-18 12:00 AM			
7	Chirag		4-1-18 12:00 AM	9:16:29	19:16:27	
8	Khushbu		4-1-18 12:00 AM			
9	Chirag		5-1-18 12:00 AM			
10	Khushbu		5-1-18 12:00 AM			
11						

Manual Export

You can also do the Manual transfer of data by clicking **Manual Transfer** button.





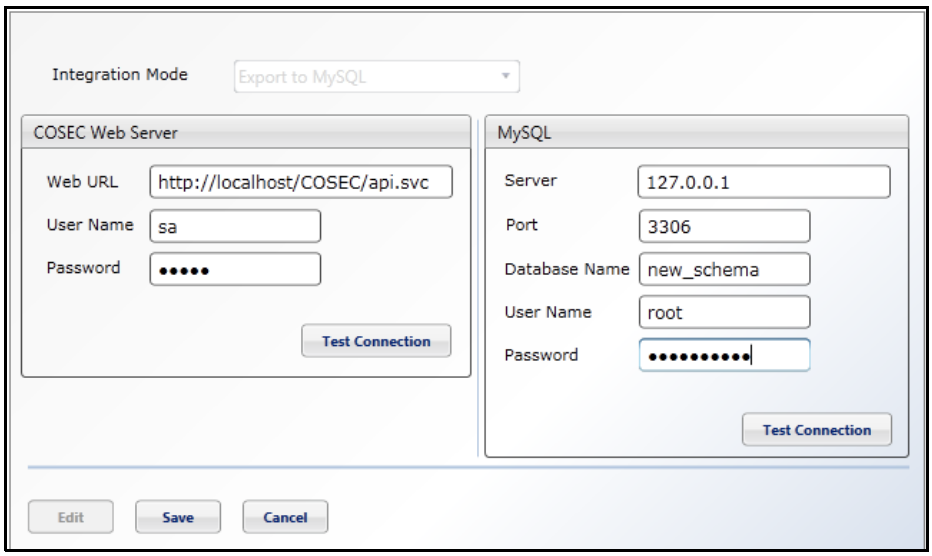


The name of the exported text file will be as per the Destination File name and data will be as per the Table field Mapping. The exported file will be as shown in Schedule export.

Export to MySQL

Select the **Export to MySQL Server** option in the **Integration Mode** field. Click on the **Edit** button.

Integrate supports Export to MySQL from version MySQL 8.0.27 to MySQL 8.3.0



In the **COSEC Web Server** section:

- Specify the web url of the api service of the COSEC WEB application as shown.
- Enter the User Name and Password of the sa user as set in the COSEC WEB application.

In the **Destination Database** Server section:

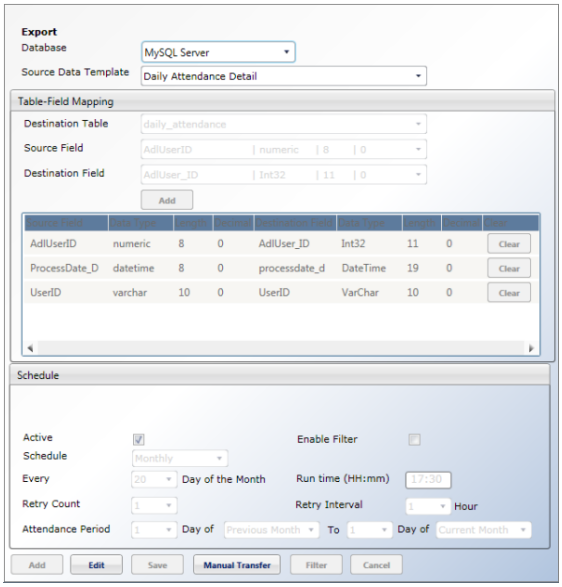
- The **Database Type** will be SQL SERVER.
- **Server**: Enter the database server name in the following format - **Database server name\Instance Name** e.g. dbserver\sqlexpress.
- **Database Name**: Specify the database name of the destination database as per the site settings.
- **User Name**: Specify the database administrator ID in this field.
- **Password**: Enter the password of the Database administrator as per the site settings.

The **Test Connection** button is provided to test the connections with the web server as well as the SQL Server database.

Click on **Save** once done.

Export Data Configuration

This option enables the Admin user to map the fields from the COSEC database tables to fields in a third party database. Click on the **Export Data** button. The following page appears.

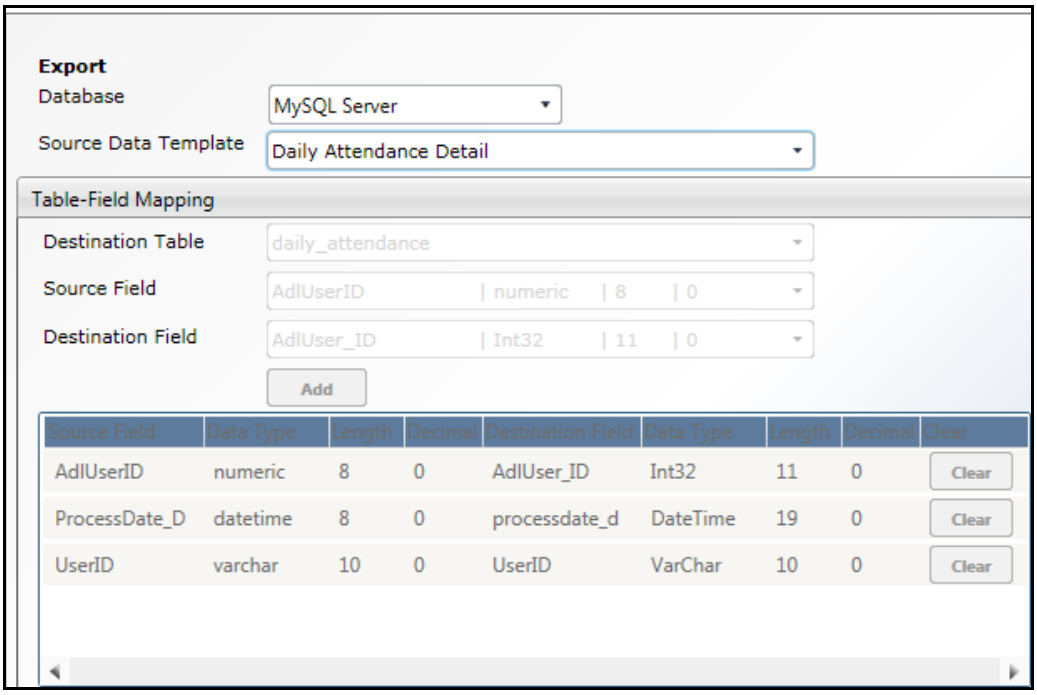


The COSEC INTEGRATE application provides four data templates in line with the default **Database Views** as shown. The COSEC System provides the following four Database views which would provide the relevant field options to be mapped with the fields of a destination database.

- Monthly Attendance Summary
- Daily Attendance Detail
- Attendance Events
- Access Control Events

Each of the above database views would provide the relevant fields whose values can be exported from the COSEC database. Select the required data template and click on the **Edit** button.

Now the Admin user can start the **mapping of the fields** from the source database to that of the destination database as shown.



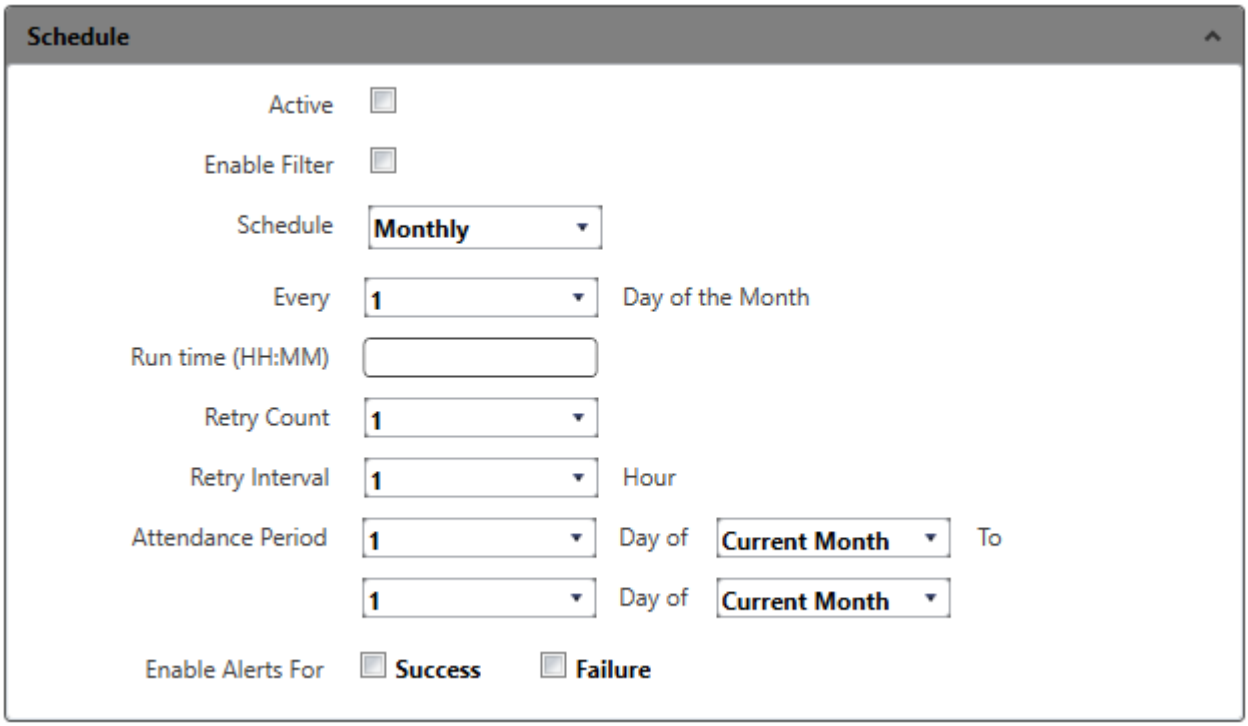
- Select the **Destination Table** from the pull down list.
- Select the **Source field** from the COSEC database.
- Select the **Destination field** from the selected destination table.
- Click on the **Add** button. The mapped fields will be visible in the bottom grid as shown.

In the case of Attendance Events and Access Control Events the user needs to map the UserID and the EventDateTime_D source fields to fields in the destination table.

Map the UserID, PMonth and Pyear source fields to appropriate fields in the destination table in the case of the Monthly Attendance Summary.

Map the UserID and ProcessDate_D source fields to appropriate fields in the destination table in the case of the Daily Attendance Detail.

The **Schedule section** enables the Admin user to schedule the data export process. The schedule option vary based on the selected Source Data Template. The **Daily Attendance detail** will have the following options as shown.



- Check the **Active** box to enable the schedule.
- The **Enable Filter** option is provided to enable the administrator to filter the users whose data is to be exported. Check this box and click on the **Filter** button. The Multiple selection window appears. Select the users whose data is to be exported.
- Specify the day of the month on which the export process is to be run.
- Specify the **Run time** in HH:MM format when the export process is to be run.
- Set the **Retry Count** from the pull down list.
- Set the **Retry Interval** in hours from the pull down list. This parameter specifies the time period between successive retries.
- Specify the **Attendance Period** by specifying the starting and the ending day of the attendance period for which the data is to be exported.
- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

  Select the checkboxes as per your requirement:

  Select **Success** checkbox to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

  Select **Failure** checkbox to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

  If you require Alerts for both the above events, select both the check boxes.

In case of partial data transfer i.e. if both the above checkboxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

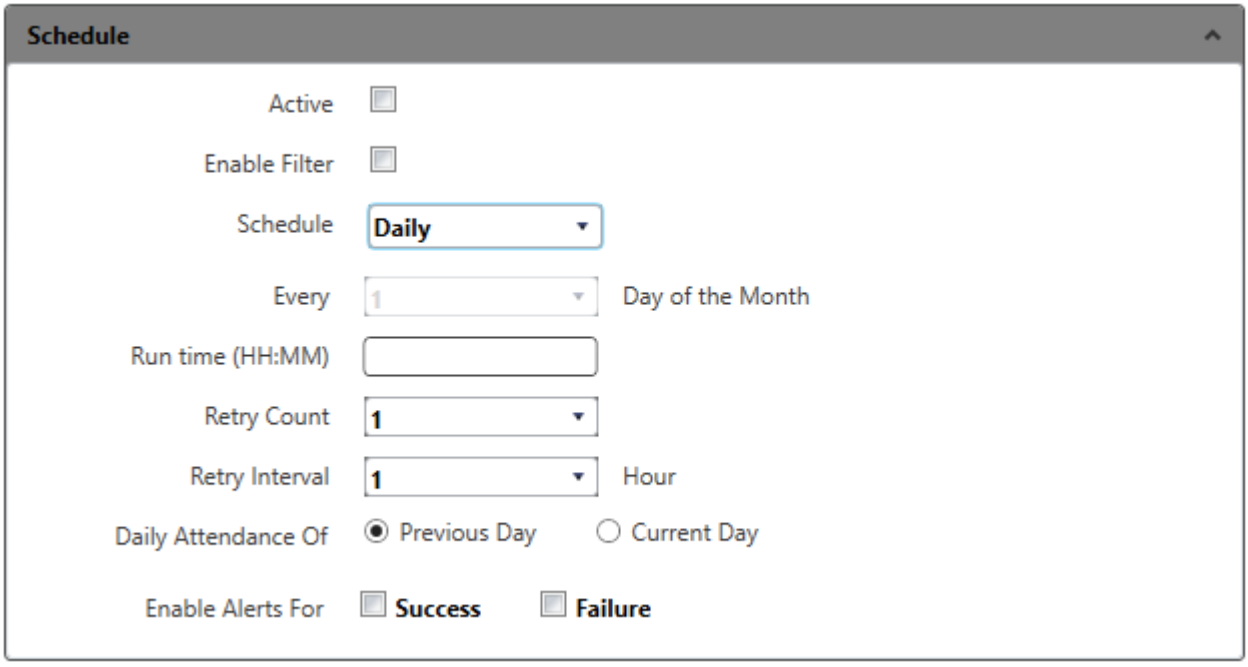
Example: There are in total 100 records which are to be transferred.

Now, out of 100 records, only 60 records are transferred Successfully and the remaining 40 records have Failed. Such data transfers are known as partial data transfers.

So here the connection status will be Failure and an alert will be sent to the configured COSEC Server along with the reason for failed data transfer.

It is to be supported for all integrate modes defined in COSEC Integrate where enable alerts provision is present i.e. for all the integration modes except for Custom Export-FP Template & Export FP Template to File.

Select any one option for data transfer i.e, Daily or Monthly in the field **Schedule**.On selection of Monthly option, user can set data transfer process to run only once in a month.By default, **Monthly** option would be selected.When selecting **Daily** option from the drop down list, the options appears as shown.

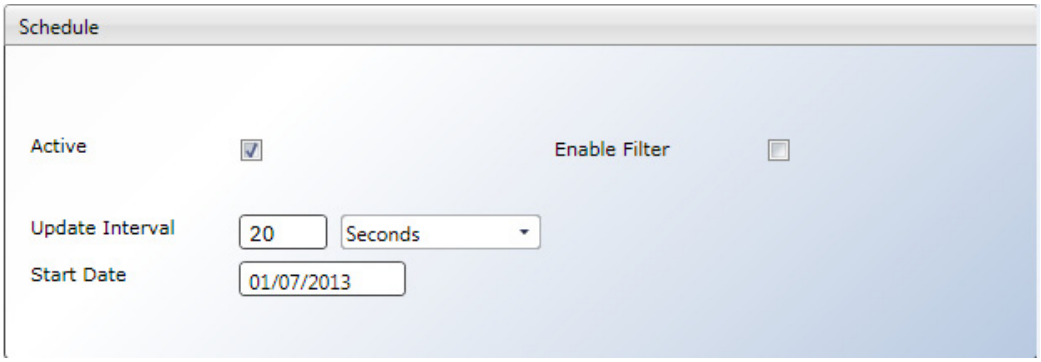


User can configure to transfer data for either previous day's attendance data or current day's attendance data with respect to schedule run day.

The **Monthly Attendance Summary** will have the following unique options:

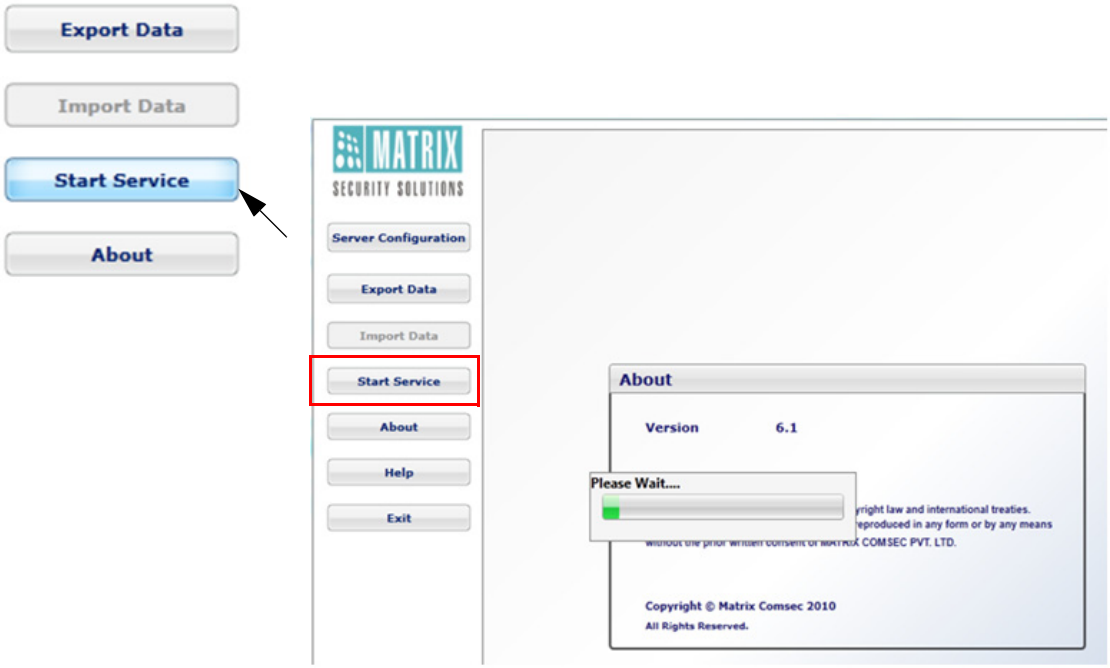
- Select the **Attendance Period** for which the monthly Attendance summary data is to be exported.The Admin user can select either the **previous month** or **current month** option.

On selecting the **Attendance Events** or the **Access Control Events** the following schedule options will be available.



- Check the **Active** box to enable the schedule.
- Set the filter parameters as described earlier.
- Specify the **Update Interval** in seconds, minutes or hours to define the frequency at which the application will update the destination database.
- Specify the **Start Date** from which the export process is to be initiated.

After defining the above parameters, the Admin user has to click on the **Start Service** button.



The application will start the **COSEC INTEGRATE** service as shown.

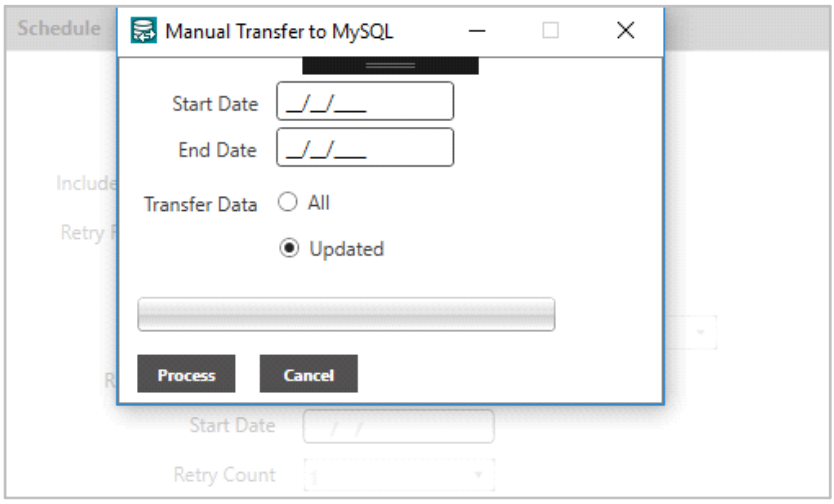
Manual Transfer

The Manual Transfer option provides the Admin user the flexibility to export data of a specific time period as and when required. In order to access this functionality click on the **Stop Service** button to stop the COSEC INTEGRATE service.

Click the **Export Data** button.

On the **Export Data** page, edit and save the export settings as per your requirement.

Click the **Manual Transfer** button. The following window appears for *Manual Transfer to MySQL*.



Enter the **Start Date** and **End Date**.

Select the **Transfer Data** mode— **All** or **Updated**.

All: All the past data falling within the selected date range will be transferred.
Updated: All the updated data falling within the selected date range will be transferred.

Click the **Process** button. The data of the specified time period will be exported to the destination table.

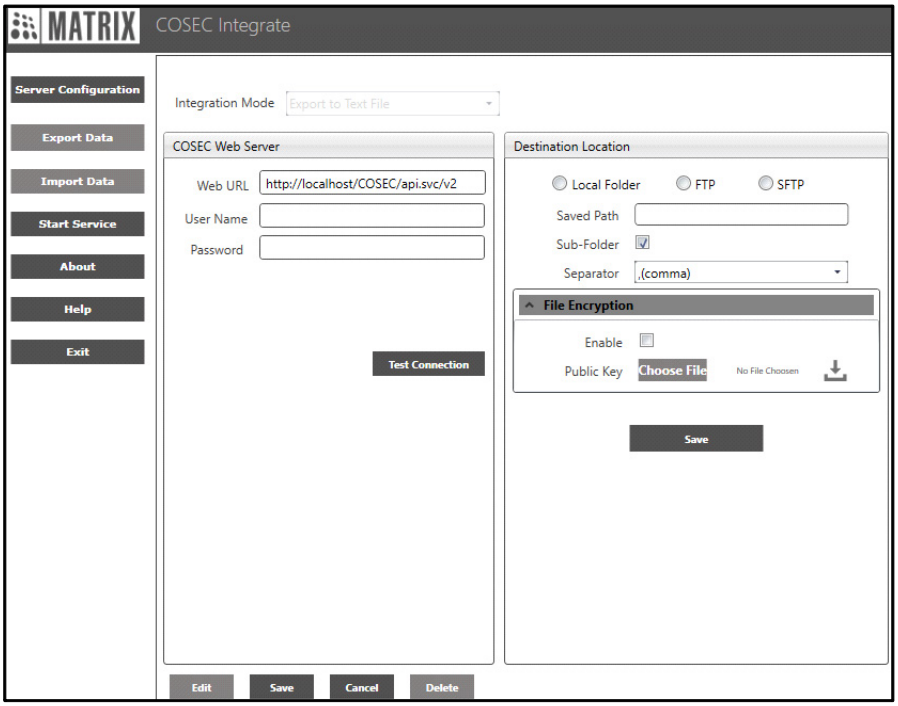
Export to Text

The application allows the administrator to export data related to various user events as mentioned earlier to a text file which can be stored at a specific location on FTP/SFTP server or in a local folder on the hard disk.

Click **Server Configuration.**

In **Integration Mode** select **Export to Text File**.

Click **Edit** to configure the parameters.



Under **COSEC Web Server** configure the following:

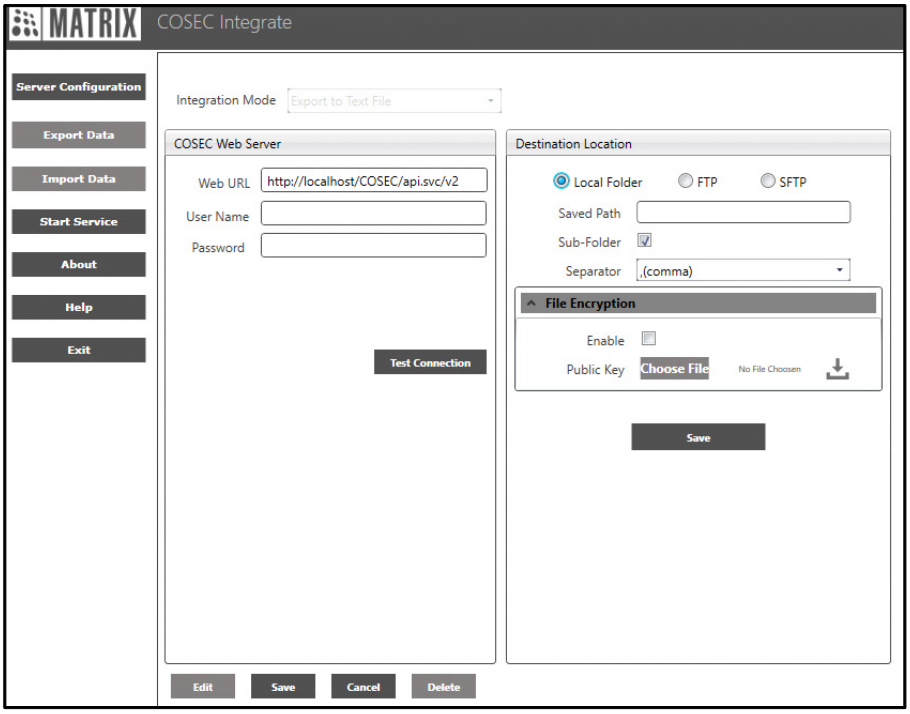
- **Web URL:** Specify the Web URL of the API service of the COSEC WEB Server application.
- **User Name:** Enter the User Name as **sa** as set for the COSEC WEB Server application.
- **Password:** Enter the Password as set for the COSEC WEB Server application.
- Click **Save**.
- Click **Test Connection** to confirm that the connectivity is established with the COSEC WEB Server application.

Under **Destination Location**, configure the following:

- Select the desired option — Local Folder, FTP or SFTP.

Local Folder

- If you select **Local Folder**, configure the following:



- **Saved Path:** Specify the Path at which the exported files are to be stored.
- **Sub-Folders:** Select the Sub-Folders check box to enable a folder hierarchy to be created at the export destination for the exported file.
- **Separator:** Select the separator which will be used to separate the fields in the exported file.

Click **File Encryption** collapsible panel and configure the following:

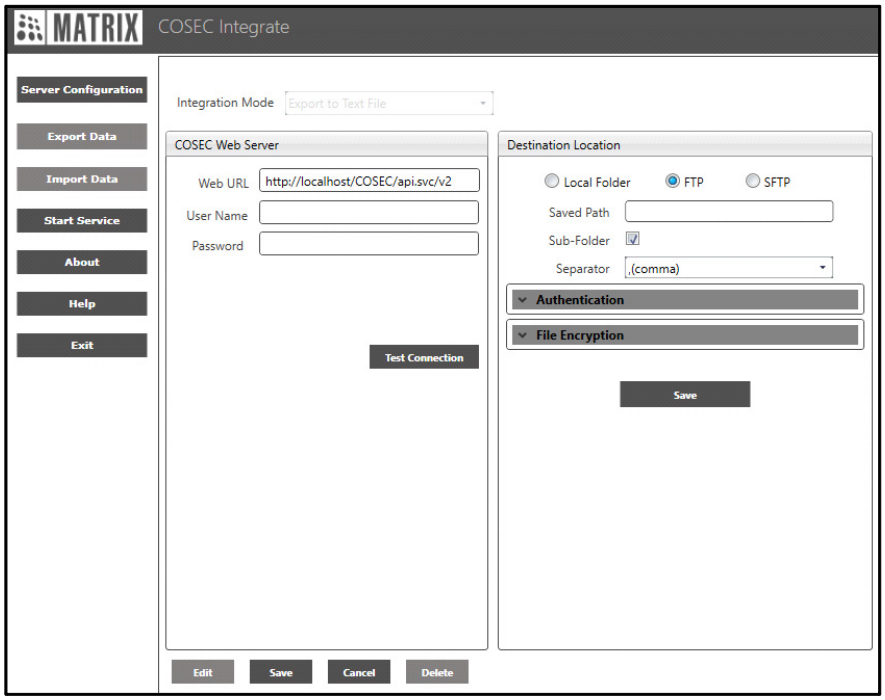
The file will be encrypted using PGP (Pretty Good Privacy) encryption method using AES algorithm.

- **Enable:** Select this check box to enable encryption. If enabled the file will be encrypted using the Public Key provided by the Third Party and then will be saved on the Path.
- **Public Key:** Click **Choose** and select the key file which is to be used for encryption. This will be provided by the Third Party. The maximum file size supported is 5MB.

- *If File Encryption check box is enabled, then Third Party must take the last updated file based on time stamping from the Saved Path.*
- Click **Save**.

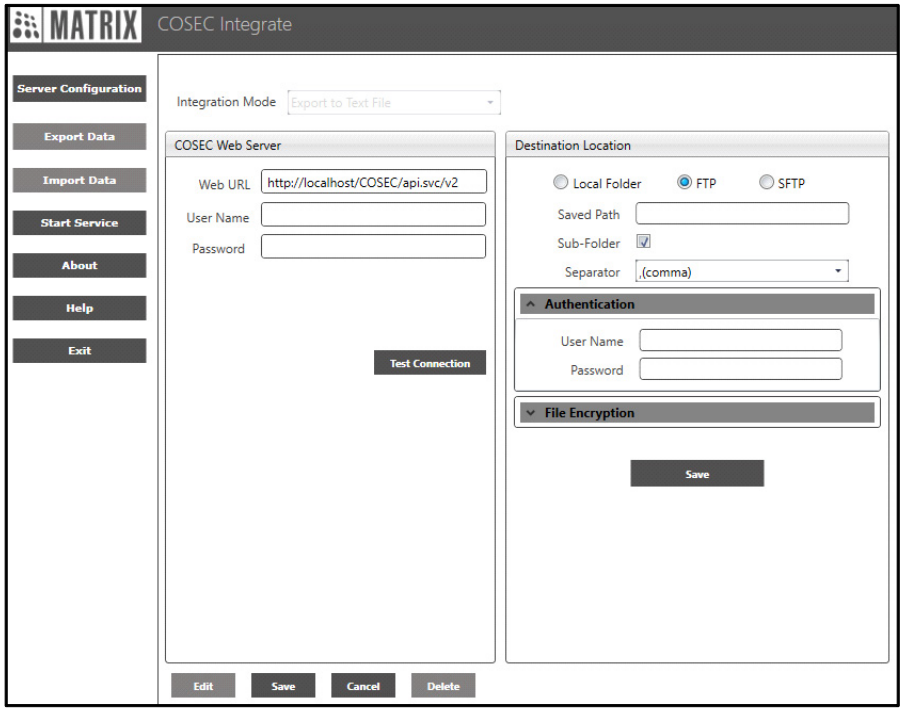
FTP

- If you select **FTP**, configure the following:



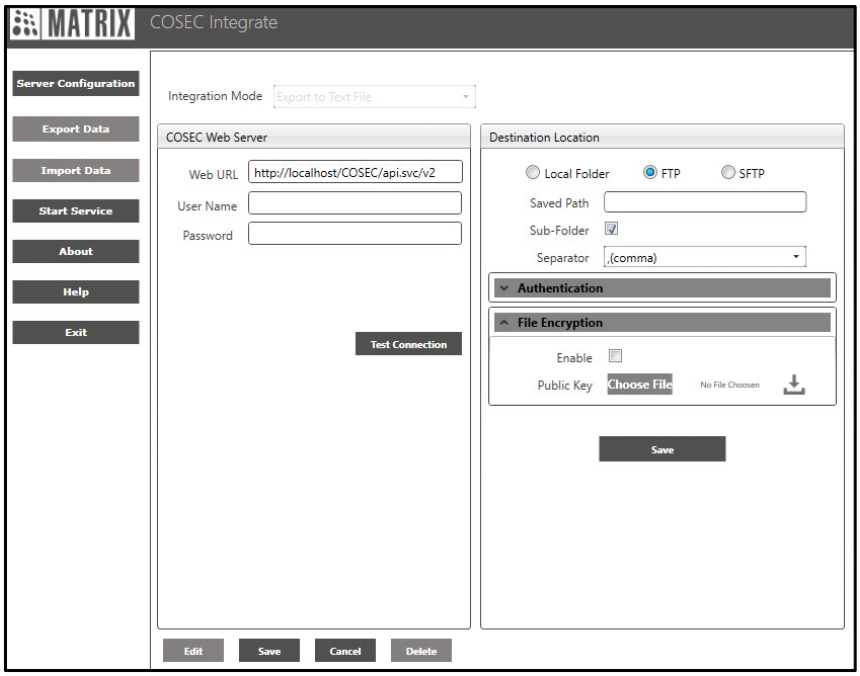
- **Saved Path:** Specify the Path at which the exported files are to be stored.
- **Sub-Folders:** Select the Sub-Folders check box to enable a folder hierarchy to be created at the export destination for the exported file.
- **Separator:** Select the separator which will be used to separate the fields in the exported file.

Click **Authentication** collapsible panel and configure the following:



- **User Name:** Enter the User Name to be used for authentication while accessing the Path.
- **Password:** Enter the Password to be used for authentication while accessing the Path.

Click **File Encryption** collapsible panel and configure the following:



The file will be encrypted using PGP (Pretty Good Privacy) encryption method using AES algorithm.

- **Enable:** Select this check box to enable encryption. If enabled the file will be encrypted using the Public Key provided by the Third Party and then will be saved on the Path.

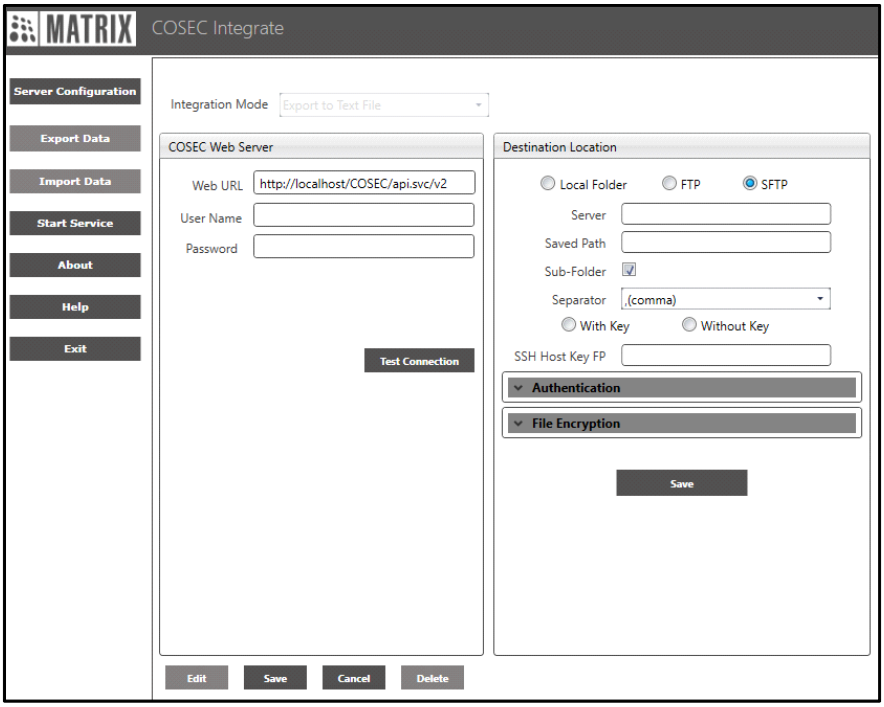
- **Public Key:** Click **Choose** and select the key file which is to be used for encryption. This will be provided by the Third Party. Maximum file size supported is 5 MB.

If File Encryption check box is enabled, then Third Party must take the last updated file based on time stamping from the Saved Path.

- Click **Save**.

SFTP

- If you select **SFTP**, configure the following:



- **Server:** Specify the SFTP Server IP Address where the exported files are to be stored.

  COSEC Integrate communicates with the SFTP Server using the default port number 22. If you wish to use any other port, then you need to configure the same in the format Server IP Address:Port. For example if Port 33 is to be used then configure the Server as 192.168.104.20:33.

- **Saved Path:** Specify the Path at which the exported files are to be stored.

- **Sub-Folders:** Select the Sub-Folders check box to enable a folder hierarchy to be created at the export destination for the exported file.

- **Separator:** Select the separator which will be used to separate the fields in the exported file.

- For additional authentication and security, you can select the desired option — **With Key** or **Without Key**.

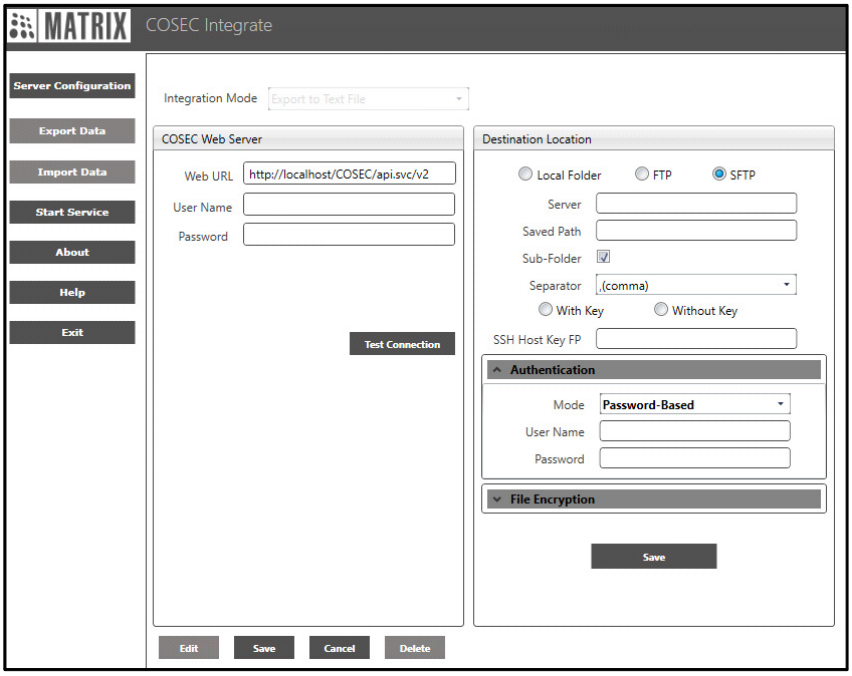
  If you select **With Key**, then configure the **SSH Host Key FP**.

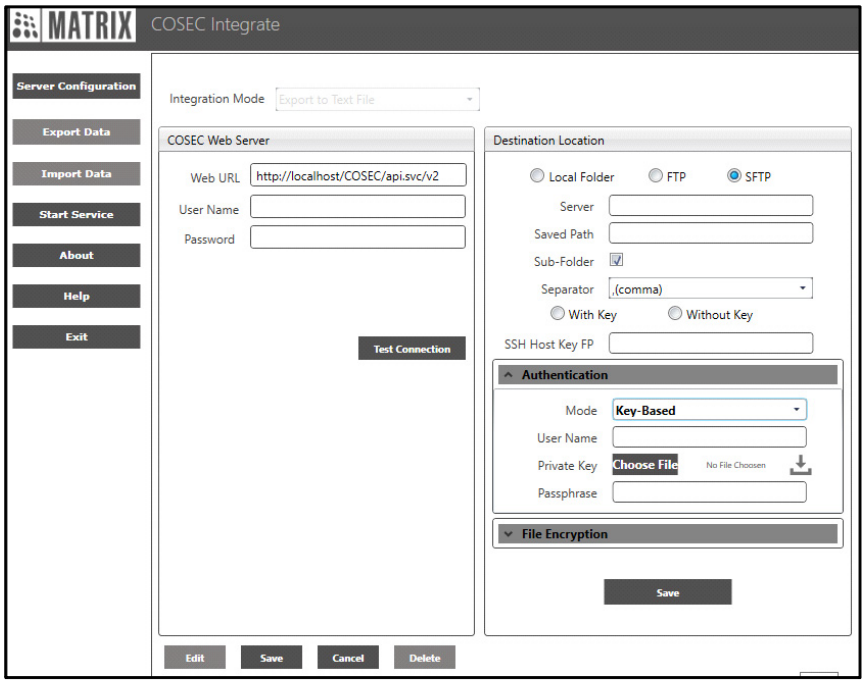
The **SSH Host Key FP** servers as a unique identifier for the Server. This is a cryptographic representation of the Servers Public Key. It is used to verify the authenticity of the Server during the connection process. It is used to ensure that the Server the client is connecting to is the same Server that it connected with previously.

This key is provided by the Administrator of the SFTP Server to the clients.

If you select **Without Key**, then no key is required.

Click **Authentication** collapsible panel and configure the following:





- **Mode:** Select the desired mode for authentication — **Password-Based**, **Key-Based**.

If you select **Password-Based,** configure the following:

In Password-Based, when a client signs in, the Server checks the User Name and Password combination and then approves/denies the request.

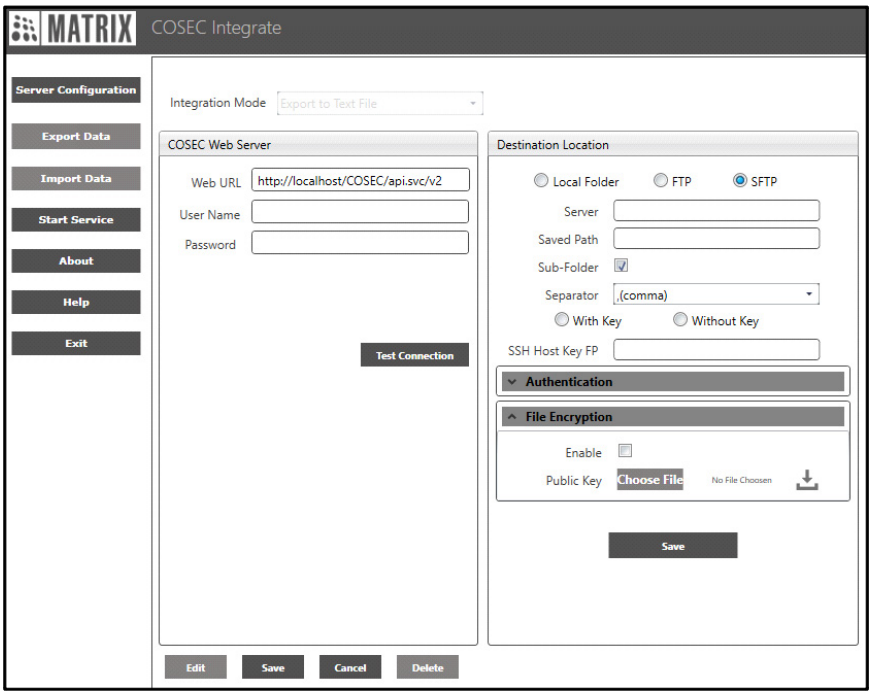
- **User Name:** Enter the User Name to be used for authentication while accessing the Path.
- **Password:** Enter the Password to be used for authentication while accessing the Path.

If you select **Key-Based,** configure the User Name, Private Key and Passphrase.

In Key-Based, when a client signs in, a pair of keys — Private and Public — are used for authentication. The Public Key is uploaded in the SFTP Server while the Private Key is provided to the client.

- **User Name:** Enter the User Name to be used for authentication while accessing the Path.
- **Private Key:** Click **Choose** and select the key file which is to be used for authentication.
- **Passphrase:** Enter the Passphrase. This is used in combination with the Private Key to acquire the SFTP Server access.

Click **File Encryption** collapsible panel and configure the following:



The file will be encrypted using PGP (Pretty Good Privacy) encryption method using AES algorithm.

- **Enable:** Select this check box to enable encryption. If enabled the file will be encrypted using the Public Key provided by the Third Party and then will be saved on the Path.
- **Public Key:** Click **Choose** and select the key file which is to be used for encryption. This will be provided by the Third Party. Maximum file size supported is 5 MB.

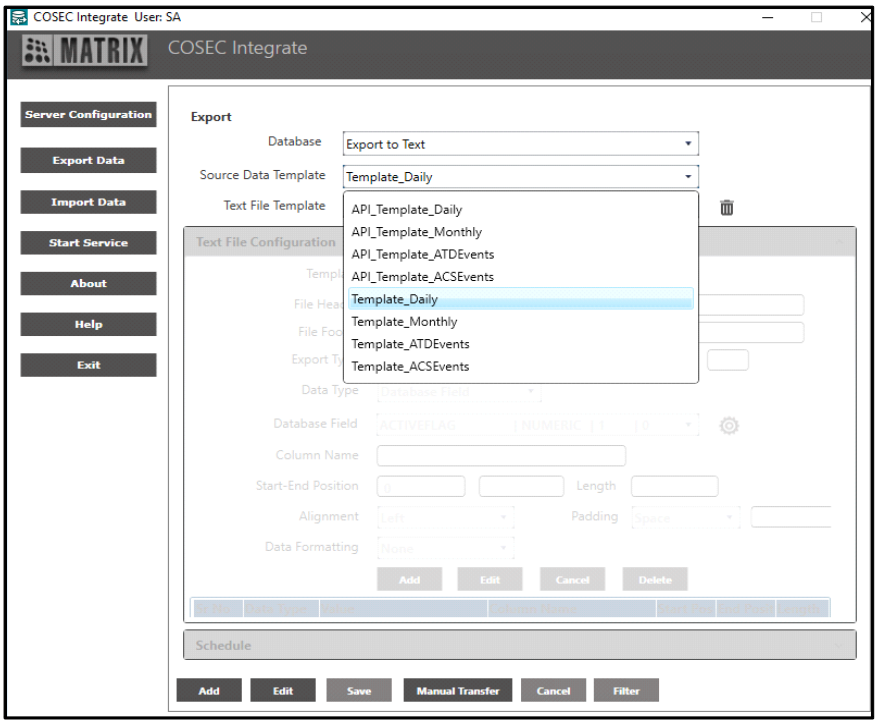
If File Encryption check box is enabled, then Third Party must take the last updated file based on time stamping from the Saved Path.

- Click **Save**.

Export Data Configuration

This option enables the admin user to specify the fields whose values are to be exported to the text file.
Each database views would provide the relevant fields whose values can be exported from the COSEC database.

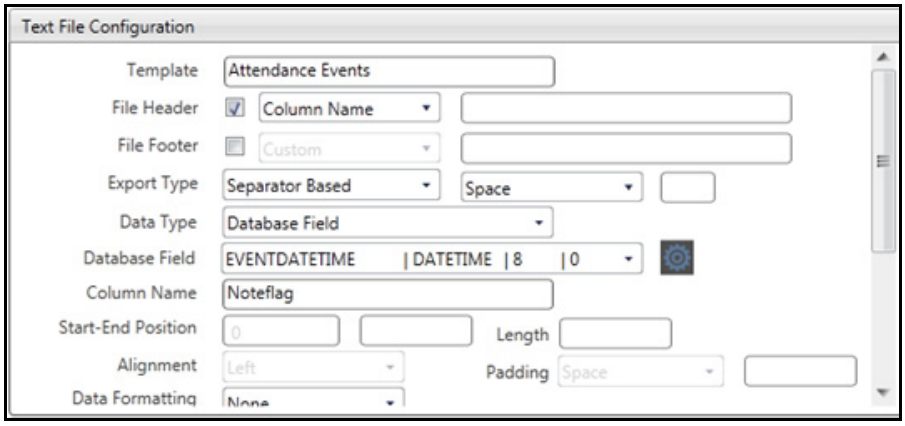
Source Data Template: Select the required data template



Text File Template: The templates will be generated once the Text file configuration is done. For configuring Text file template, click on **Add** button by scrolling the Text file Configuration section.

If the Text file template is available then you can select it and click on the **Edit** button for selecting the fields from the source database.

Text File Configuration



Template: Specify the name of the Template to which the source file is to be mapped.

File Header: Click on the check box to enable this option. Click on the drop down arrow to select the options as mentioned below

- **Column Name**: Enable the checkbox. You can specify the name of the columns while selecting Data type and the related fields which is described later. The Column Name will then be exported as the header.
- **Custom**: For a common header of the page, you can select the custom option and specify a file header name in adjacent box.

The allowed functions are mentioned below:

AVG: Returns the average. Syntax: AVG(arg1)

CONVERT: Converts particular expression to a specified .NET framework type. Syntax: Convert(expression, type)

COUNT: Counts how many numbers are in the list of arguments. Syntax: COUNT(arg1,)

IIF: Specifies a logical test to perform. Syntax:IIF(expression, [value_if_true],[value_if_false])

ISNULL: Checks an expression and either returns the checked expression or a replacement value.
Syntax: ISNULL(expression,replacement value)

MAX: Returns the maximum value in a list of arguments. Syntax: MAX(arg1)

MIN: Returns the minimum value in a list of arguments. Syntax: MIN(arg1)

LEN: Gets the length of a String. Syntax: CONVERT(expression)

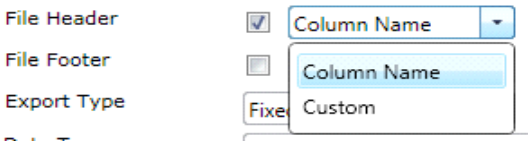
SUBSTRING: Gets a sub-string of a specified length,starting at a specified point in the string.
Syntax:SUBSTRING(expression, start, length)

SUM: Adds its arguments.Syntax: SUM(arg1)

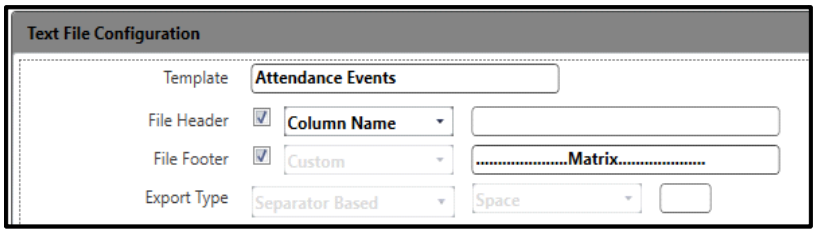
STDEV: Estimates standard deviation based on a sample. Syntax: STDDEV(arg1)

VAR: Estimates variance based on a sample. Syntax: VAR(arg1)

TRIM: Removes all leading and trailing blank charaters like \r, \n, \t. Synatx: TRIM(arg1)



File Footer: Click on the check box to enable this option. Specify the desired footer in the adjacent box as shown below.

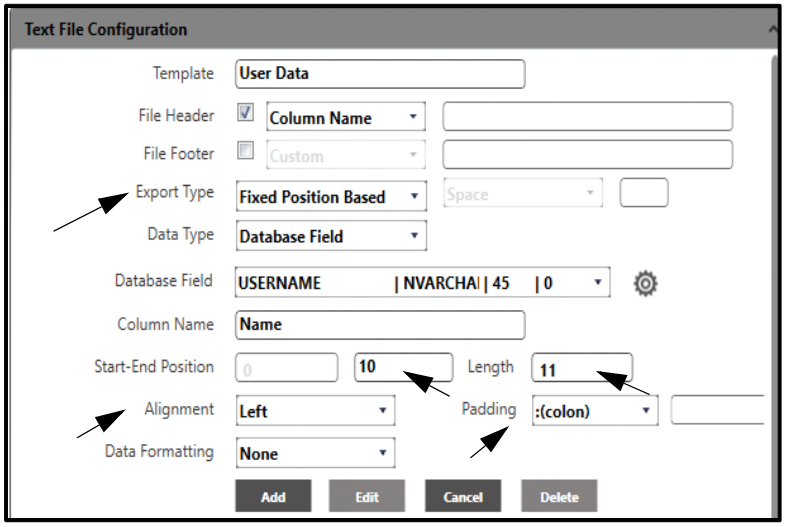


Export Type: Click on the drop down arrow to select the export type as Fixed Position based or Separator based.

The Export type option can be selected when the template is created for the first time. When the template is edited then Export type will be disabled.

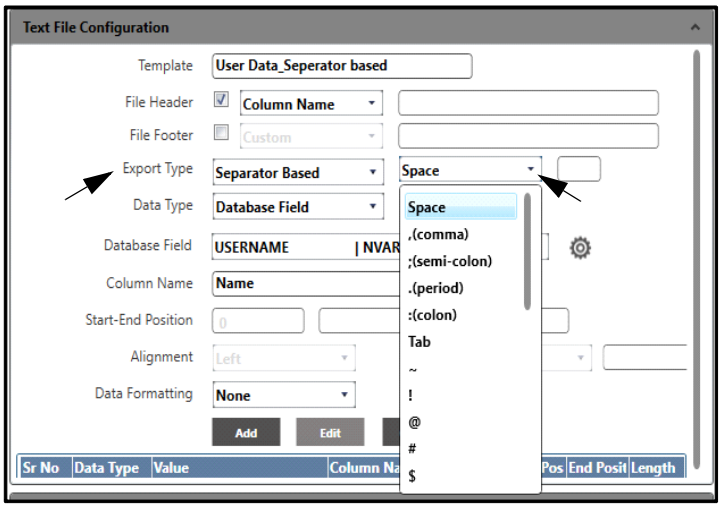
1. **Fixed Position Based**: Select this option if you want the columns to be fixed position based.

   - **Start-End Position:** Enter the position value. Eg: 0 to 10 position is set by entering end position as 10
   - **Length** will be updated automatically according to the fixed position value. You can manually enter the Length value less than the position value.
   - **Alignment** can be selected as Left or Right.
   - **Padding**: Select the Padding value from the drop down options for appending it after the data end point upto the position end point.
   - **Data formatting:** Select the Data formatting if required.

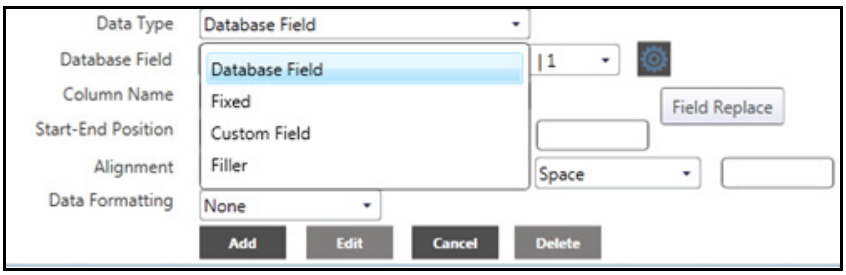


2. **Separator Based**: Select this option if you want the columns to be Separator based.

   - Select the separator options from the drop down list as shown below. You can also select the custom separator option and specify the separator in the adjacent box.



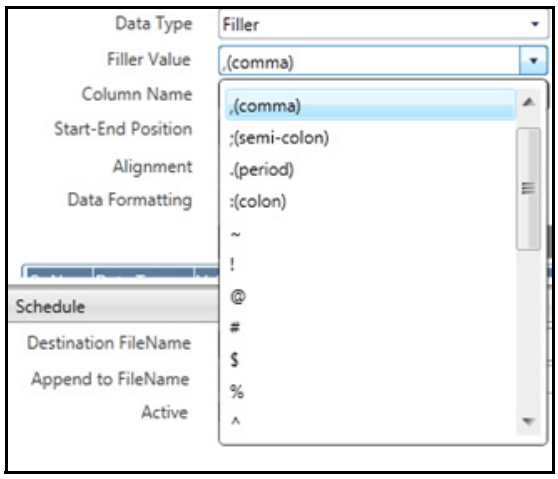
Data Type: Click on the drop down arrow to select the type of data to be exported.



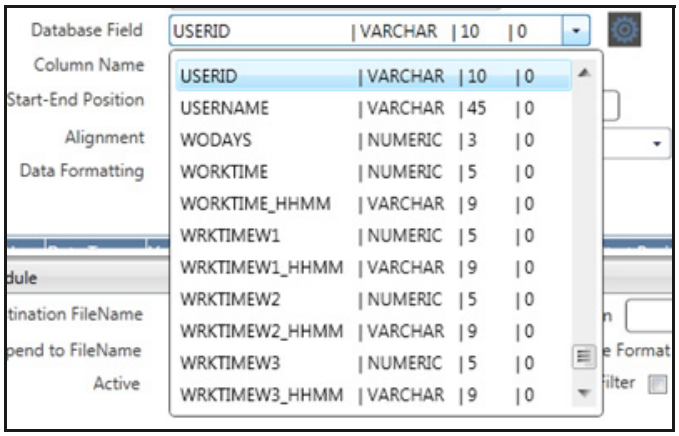
- **Fixed**: Select this option and enter the value in the Fixed value field as shown below. For eg: the organization name remains common to all the employees, so it is considered as fixed value.

- **Custom Field**: Select this option and enter the value in the Custom value field as shown below.

- **Filler**: If Export type is selected as Fixed position based, then the data type can be selected as Filler. This is used as the gap between the columns. Filler itself acts as a column, which has value other than data for eg: space, comma etc. Specify the filler value from the drop down list.



- **Database Field**: Click the drop down arrow and select the database field options.



When **Data Type** is selected as **Database Field,** then you have the option to Replace value. “Example: Replace Value”
When **Data Type** is selected as **Custom field**, the user can create an expression with the fields available in the selected export view template. The expression should be validated same as in the Text File Configuration section of Export to Text.

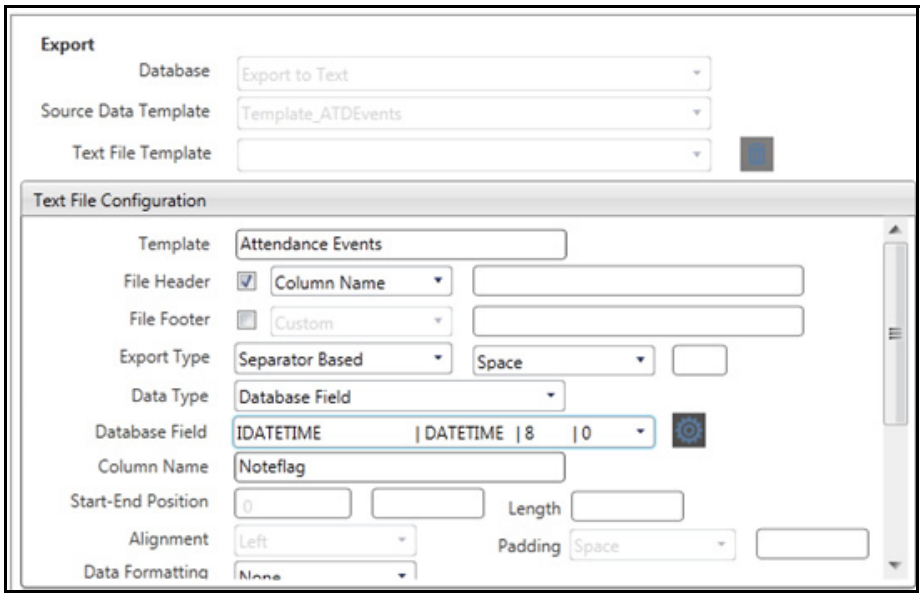
"Field Conditions support replacing value after performing comparison of field value with some fixed value / database field.

Example: Replace Value

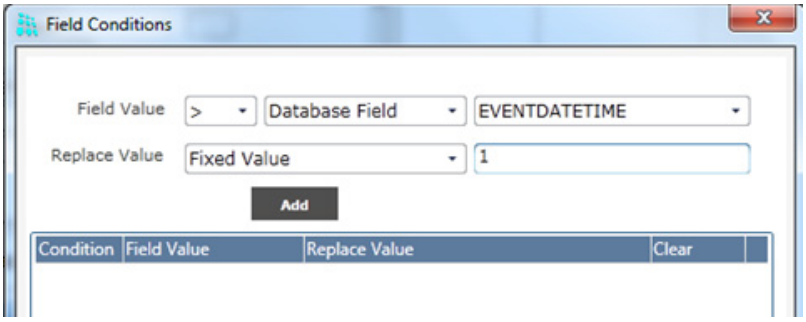
To compare punch event date-time (EDateTime) and insertion date-time (IDateTime).

During door offline condition suppose only first punch(9:00 hrs) is recorded and after that punch was not recorded for that day. So punch can be inserted after the first punch.

The system will compare the inserted punch> event punch, then the Noteflag column will be replaced with the value 1. You can give any name to the column for the fields.

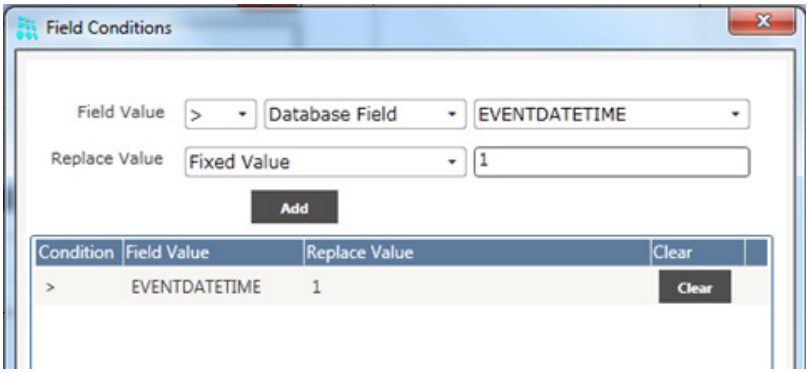


Click the Field Replace button to replace the desired field value.



Field Value can be Database Field value or fixed value with which the database field value (selected from the Text file configuration) will be compared.

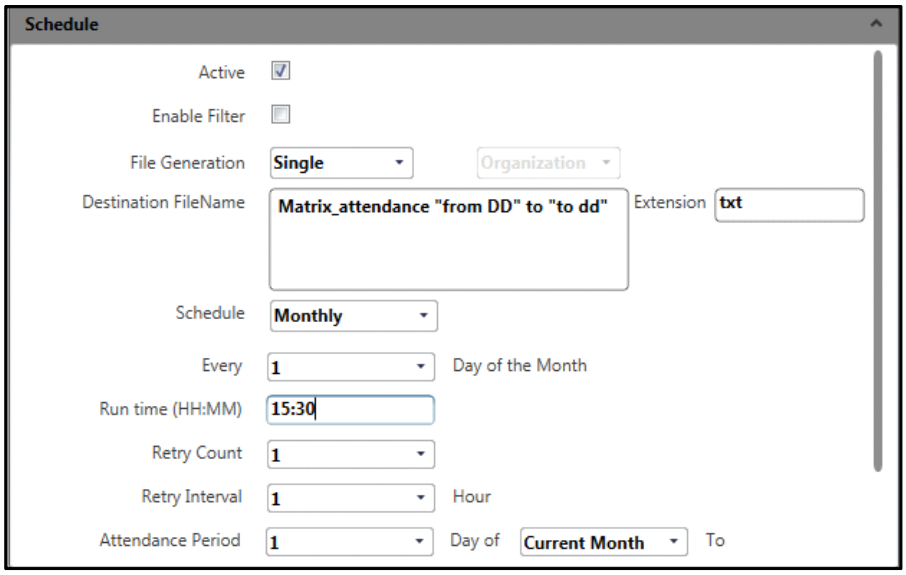
Replace Value can be a fixed value or any custom value. (Here If IDATETIME > EDATETIME, then column will be replace with value 1)



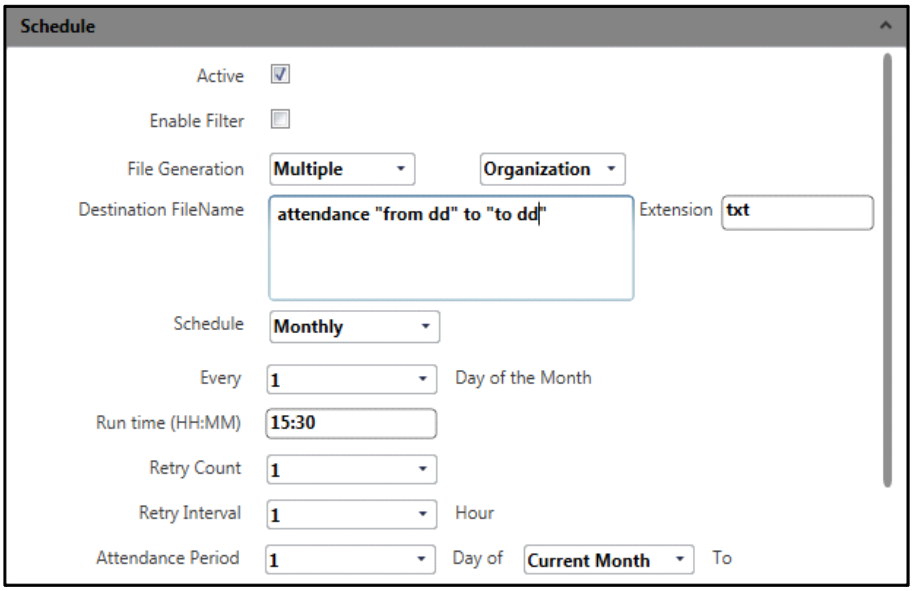
Schedule Section

The **Schedule section** enables the Admin user to schedule the data export process. The schedule option vary based on the selected Source Data Template.

The **Daily Template** will have the following options as shown. (Attendance Period for monthly schedule and Daily Attendance for Daily schedule.)



- Check the **Active** box to enable the schedule.
- The **Enable Filter** option is provided to enable the administrator to filter the users whose data is to be exported. Check this box and click on the **Filter** button. The Multiple selection window appears. Select the users whose data is to be exported.
- **File Generation:** Select **Single** or **Multiple** configuration for the file generation based on Enterprise groups. On Selecting Multiple option, second drop-down of File Generation will be activated. It enables to generate different files based on enterprise groups as shown below.



- **Destination FileName:** Enter a filename in this field. The max characters can be 200. The file name can include Alphanumeric characters, Special characters like **!@#$%^&()_-+=[]{};',.<space> A-Z a-z 0-9 and pair of asterisks(**).**

You can type '*' in the text-area. This will show the list of variables as per the template type. Select the desired variable. It will be added by appending '*' at the end. During the deployment of file, the current date-time values will be fetched and replaced instead of these variables.

1. When '' is typed in text area, another '*' will be added automatically as it is allowed only in pair.*
*2. When you are entering filename and the appearing variable list is disturbing then you can enter **ESC** key to hide the variables for the instance.*

Example of Variables:
***gdateDD*-** This variable will fetch and show the date on which the data is exported and file is generated. Similarly variables are available for month, year, hours. minute and seconds.

***fromDD*-** This variable will fetch and show the date value of the Start Date. Similarly variables are available for month and year. Suppose Start date is 1st date of current month. If current month is Feb so the value of variable will be “1”.

***toDD*-** This variable will fetch and show the date value of the End Date. Similarly variables are available for month and year. Suppose End date is Last date of current month. If current month is Feb so the value of variable will be “28”.

atdMM*- This variable will fetch and show the month value of attendance period. Similarly variables is available for year.

Example : A new template has been configured with Destination FileName = 'Atd. Events_*fromDD*-*fromMM*-*fromYY*_to_*toDD*-*toMM*-*toYY*

Now, this template is manually exported with date-range, 01-01-2016 to 02-01-2016. Thus, the exported file name will be Atd. Events_01-01-16_to_02-01-16.txt

- **Schedule**: Select the option as **Daily** or **Monthly** to run the schedule.
    - For **monthly schedule** specify the **day** of the month on which the export process is to be run. And select the **Attendance period** i.e. starting and the ending day of the attendance period for which the data is to be exported.
    - For **daily schedule** select the **Daily Attendance** of Previous Day or Current Day for which the attendance details is to be exported.
- **Run time:** Specify the Run time in HH:MM format when the export process is to be run.
- **Retry Count:** Set the Retry Count from the drop down list to retry the export if it gets failed.
- **Retry Interval:** Select the Retry Interval in hours from the drop down list. This parameter specifies the time period between successive retries.
- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

Select the checkboxes as per your requirement:

Select **Success** checkbox to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

Select **Failure** checkbox to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

If you require Alerts for both the above events, select both the check boxes.

In case of partial data transfer i.e. if both the above checkboxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

Example: There are in total 100 records which are to be transferred.

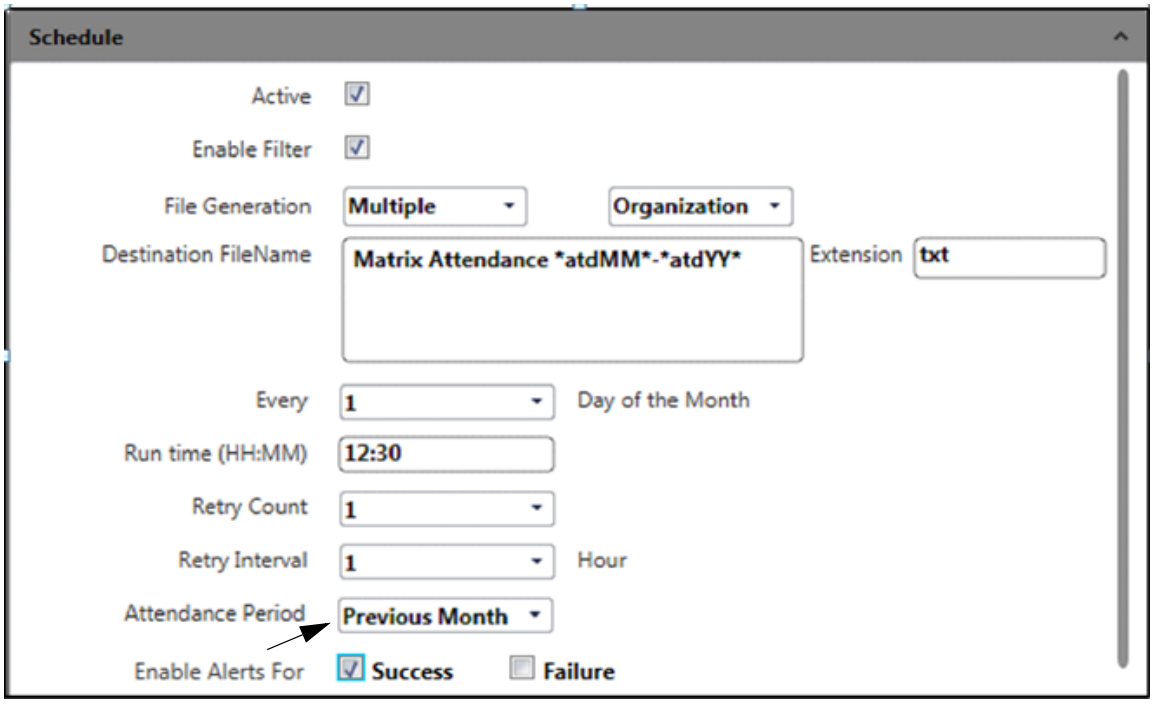
Now, out of 100 records, only 60 records are transferred Successfully and the remaining 40 records have Failed. Such data transfers are known as partial data transfers.

So here the connection status will be Failure and an alert will be sent to the configured COSEC Server along with the reason for failed data transfer.

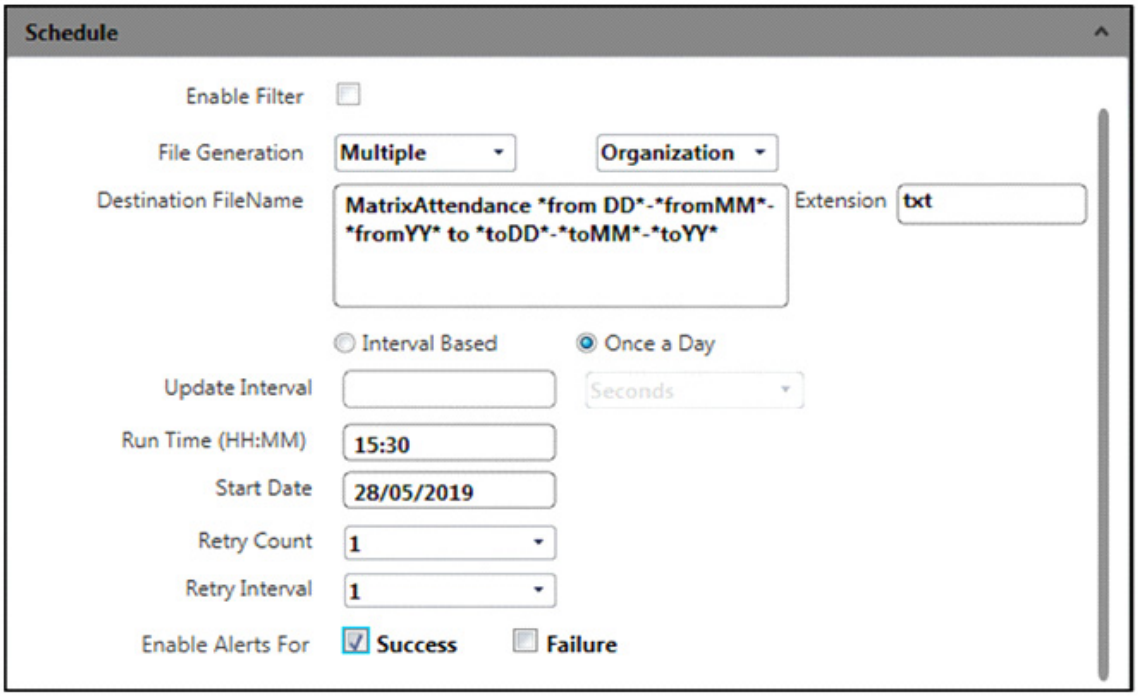
It is to be supported for all integrate modes defined in COSEC Integrate where enable alerts provision is present i.e. for all the integration modes except for Custom Export-FP Template & Export FP Template to File.

Then click on **Save** button to save the schedule. Now you can start service for running the export schedule. *See "Exporting Data" on page 61.*

The **Monthly Template** will have the same options as mentioned above except the **Attendance Period** option.



The **ATD Events** and **ACS Events** templates' schedule is shown below.

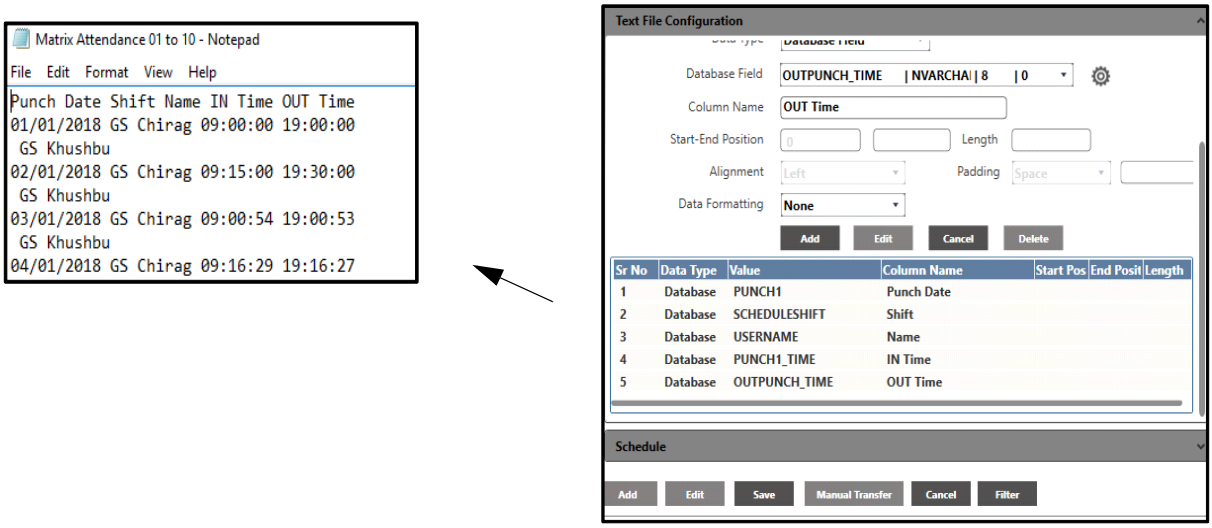


Exporting Data

Schedule Export

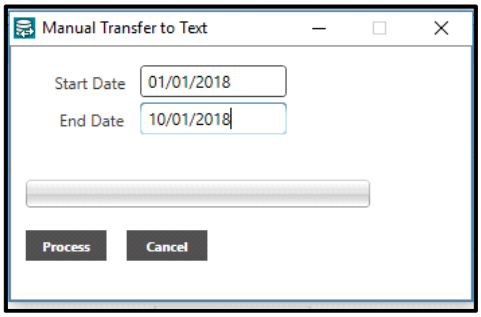
For starting the export of file, after saving the schedule; click on **Start Service** button. The exported file will be exported at the path specified in Server configuration.

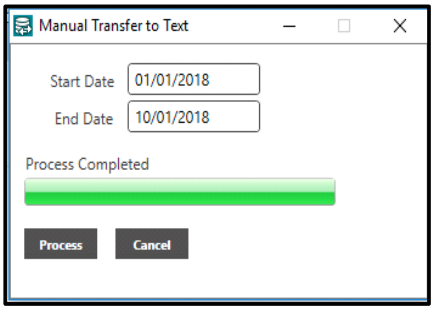
The data in the exported file is as per the Text file configuration shown below.



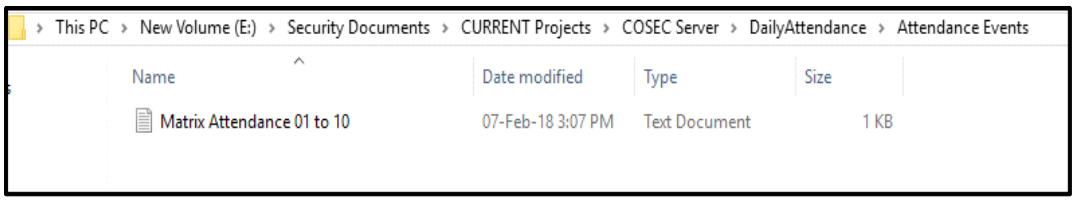
Manual Export

You can also do the Manual transfer of data by clicking **Manual Transfer** button.

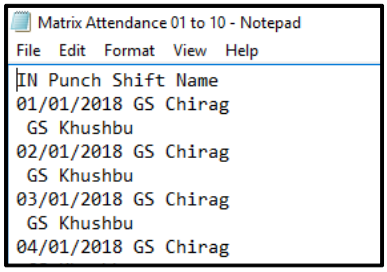


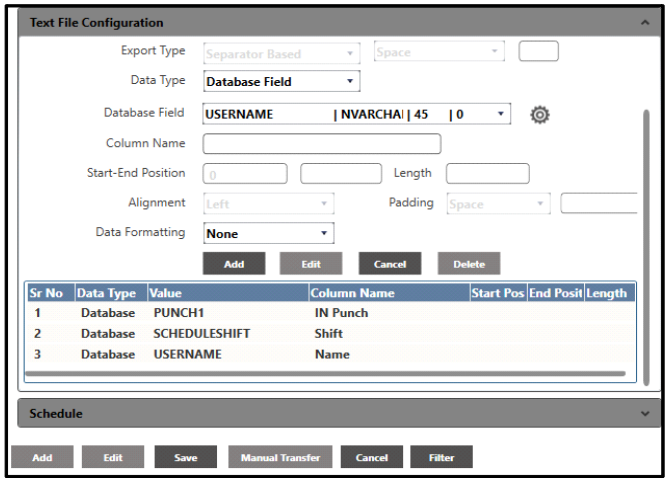


The name of the exported text file is as per the Destination File name.



The data in the exported file is as per the Text file configuration shown below.





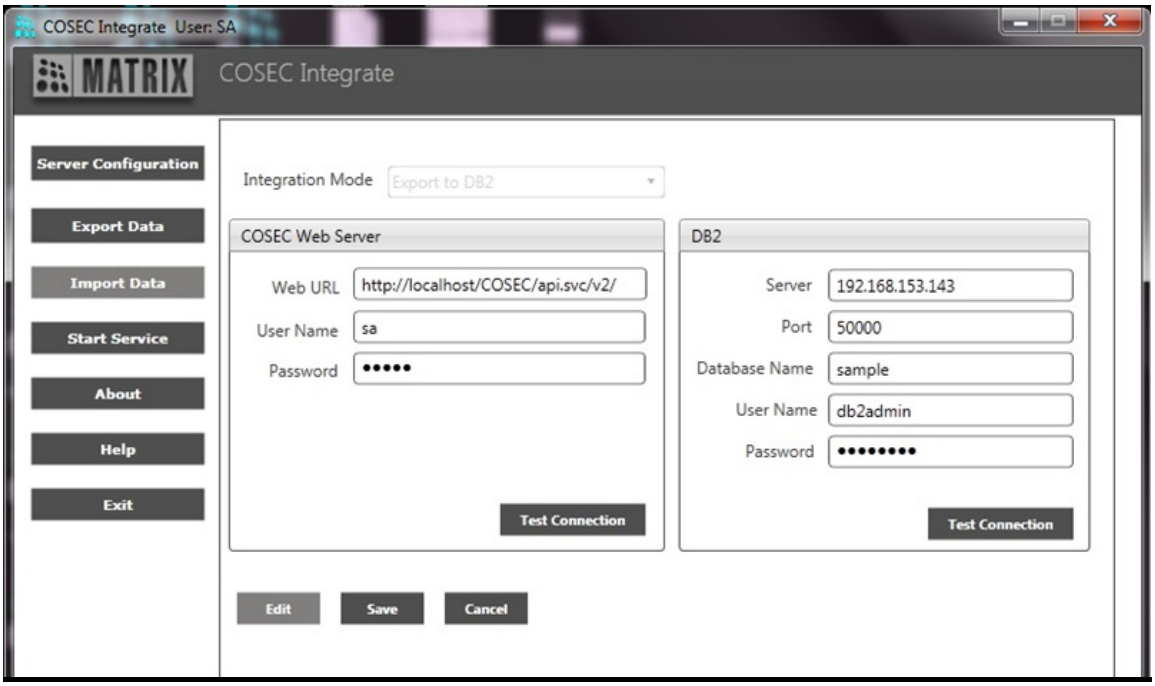
Export to DB2

The application allows the administrator to export access events from the COSEC application database to a destination **DB2 database server**.

Click on the **Server Configuration** button to start the configuring process.

The following page appears. Select the **Export to DB2** option in the **Integration Mode** field.

Integrate supports Export to DB2 version DB2 11.5.9 Z/OS



Click on the **Edit** button.

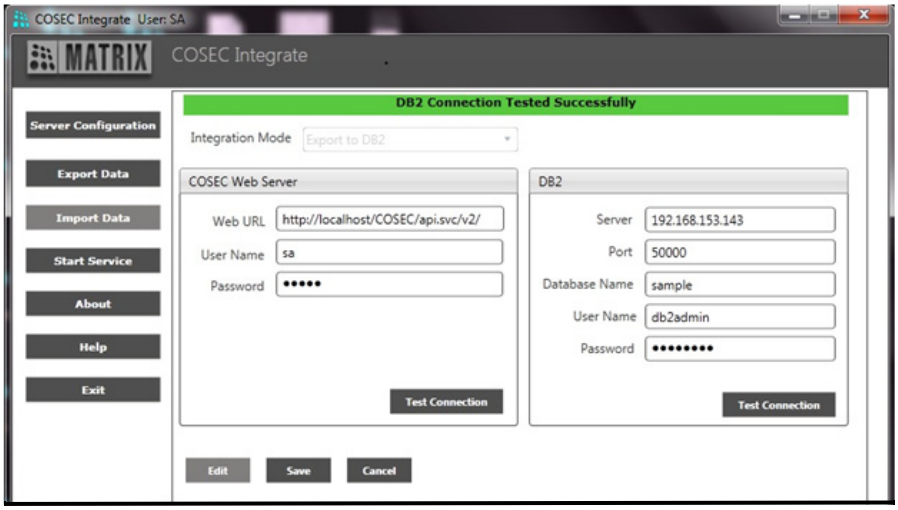
In the **COSEC Web Server** section:

- Specify the web url of the API service of the COSEC WEB application as shown.
- Enter the User Name and Password of the system administrator (sa) as set in the COSEC WEB application.

In the **DB2** destination database server section:

- Enter the database server name and port.
- Specify the database name of the destination database as per the site settings.
- Specify the database administrator ID as user name.
- Enter the password of the database administrator as per the site settings.

The **Test Connection** button is provided to test the connections with the web server as well as the DB2 database.

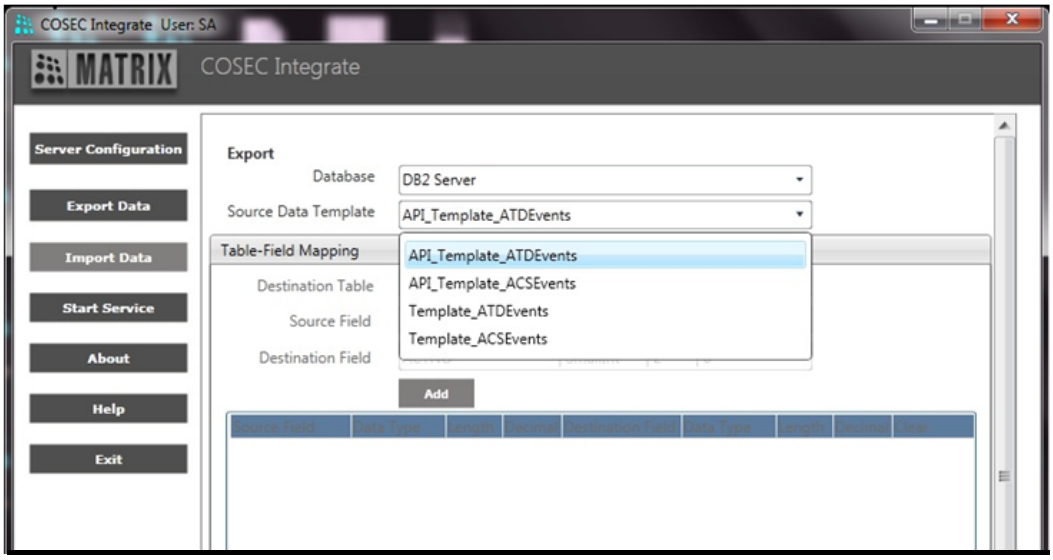


Click on **Save** once done.

Export Data Configuration

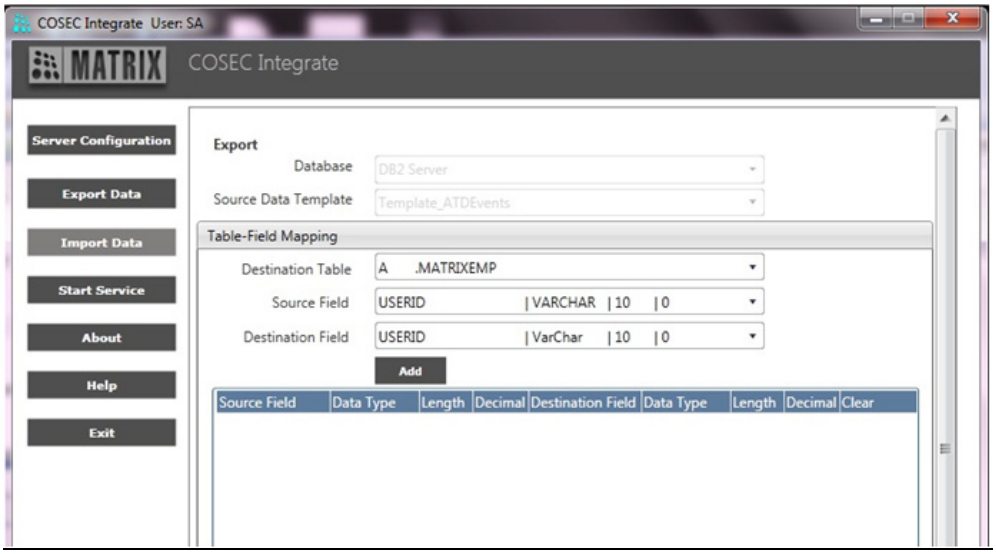
Click the **Export Data** button to map fields between source and destination tables.

For the DB2 Server Database, select a source template from the system-defined data templates or other custom export templates defined on COSEC that appear for selection.

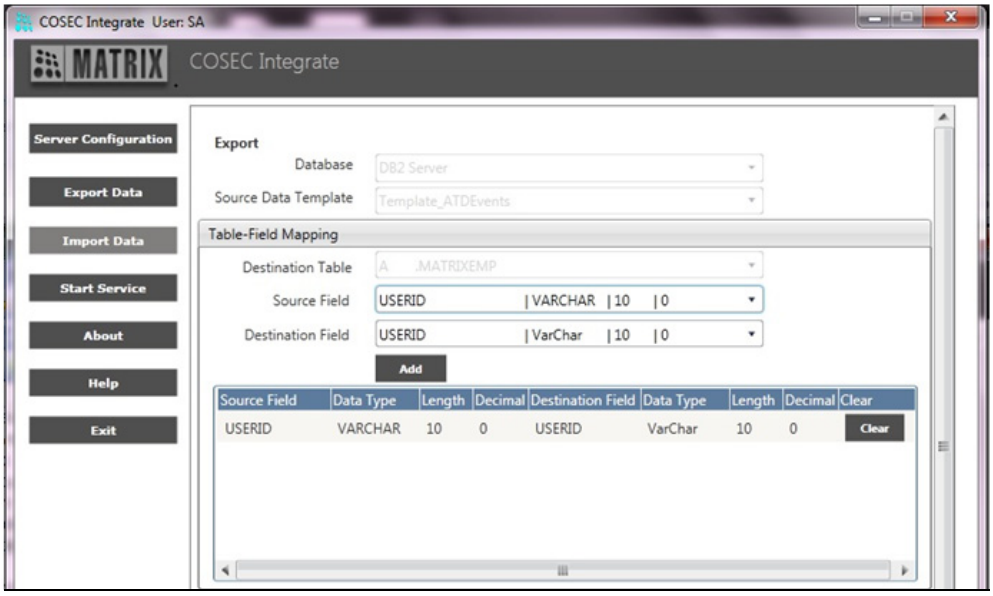


Each of the above database views would provide the relevant fields whose values can be exported from the COSEC database. Select the required data template and click on the **Edit** button.

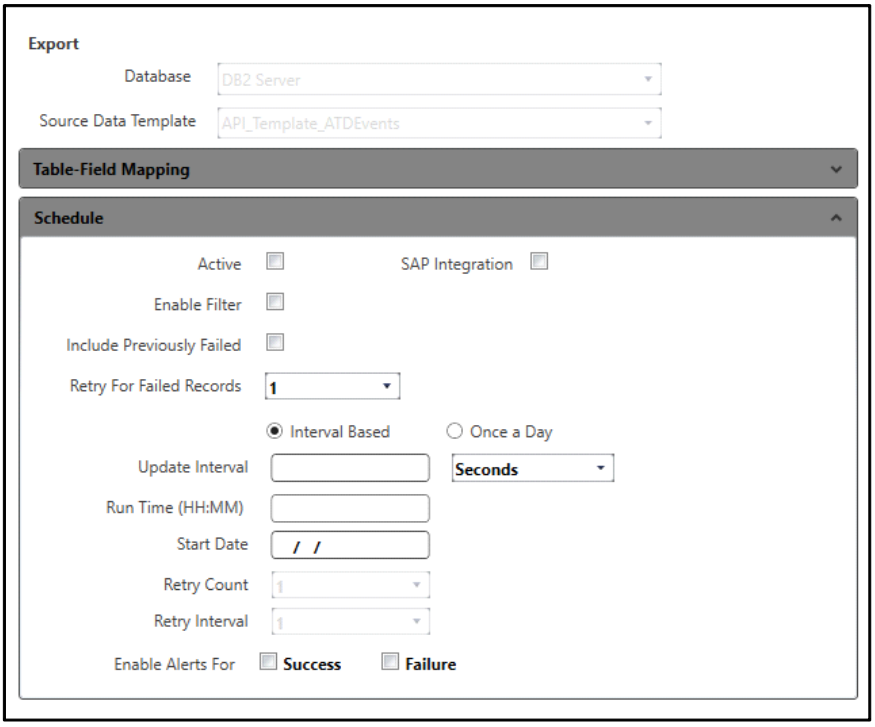
Now the admin user can start the mapping of the fields from the source database to that of the destination database as shown.



- Select the **Destination Table** from the pull down list.
- Select the **Source field** from the COSEC database.
- Select the **Destination field** from the selected destination table.
- Click on the **Add** button. The mapped fields will be visible in the bottom grid as shown.



In the **Schedule** panel, user can set up a schedule for data update between source and destination databases or update data manually using the **Manual Transfer** option.



- Check the **Active** box to enable the schedule.
- The **Enable Filter** option is provided to enable the administrator to filter the users whose data is to be exported. Check this box and click on the **Filter** button. The Multiple selection window appears. Select the users whose data is to be exported.
- To use the exported data for SAP Integration, enable the **SAP Integration** checkbox.
- To set **Interval Based** data update, specify the **Update Interval**.
- To schedule data update **Once a Day**, specify the **Run time** in HH:MM format, **Start Date** (i.e. date since when export data is to be fetched from COSEC database), **Retry Count** and **Retry Interval**.
- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

  Select the checkboxes as per your requirement:

  Select **Success** checkbox to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

  Select **Failure** checkbox to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

  If you require Alerts for both the above events, select both the check boxes.

  In case of partial data transfer i.e. if both the above checkboxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

Example: There are in total 100 records which are to be transferred.

Now, out of 100 records, only 60 records are transferred Successfully and the remaining 40 records have Failed. Such data transfers are known as partial data transfers.

So here the connection status will be Failure and an alert will be sent to the configured COSEC Server along with the reason for failed data transfer.

It is to be supported for all integrate modes defined in COSEC Integrate where enable alerts provision is present i.e. for all the integration modes except for Custom Export-FP Template & Export FP Template to File.

- Click **Save** and start service.

Export to People Works

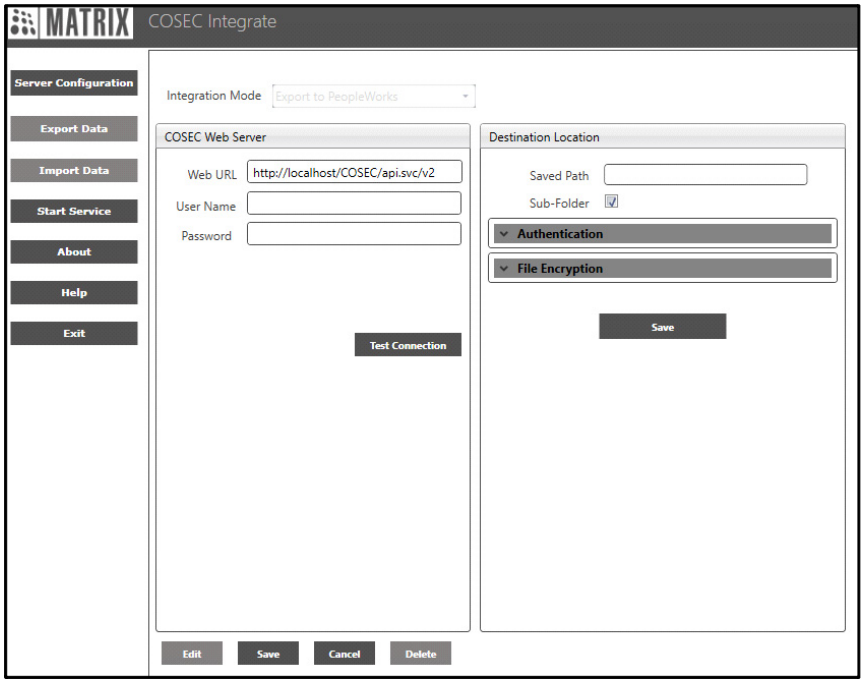
This feature allows the user to export data from the COSEC application database to a user-defined FTP location in the *.XLSX* format. The export filename will follow the below format:

“PeopleWorks<ddmmyyyy><hhmm>.xlsx”

Click **Server Configuration.**

In **Integration Mode** select **Export to PeopleWorks**.

Click **Edit** to configure the parameters.



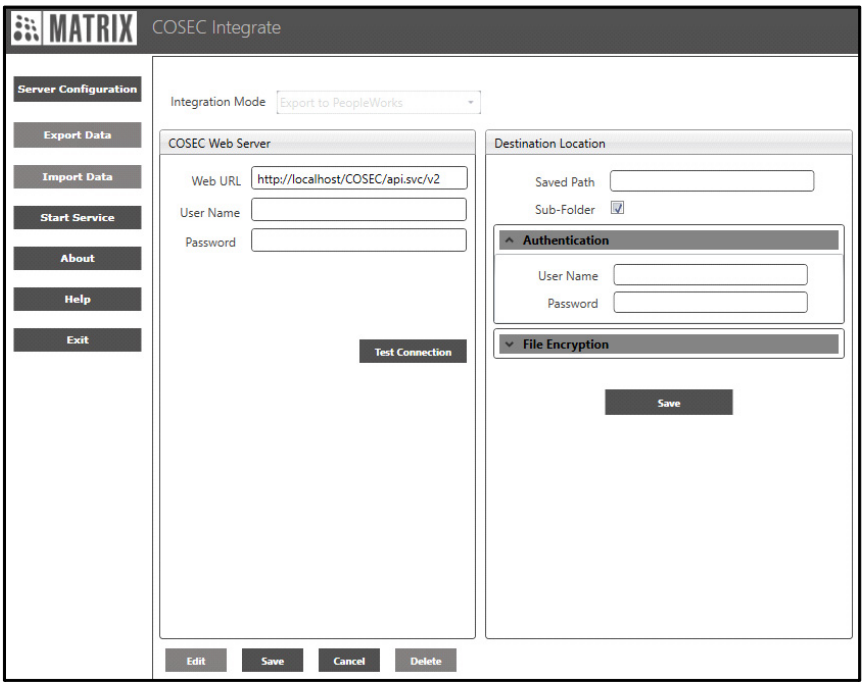
Under **COSEC Web Server** configure the following:

- **Web URL:** Specify the Web URL of the API service of the COSEC WEB Server application.
- **User Name:** Enter the User Name as **sa** as set for the COSEC WEB Server application.
- **Password:** Enter the Password as set for the COSEC WEB Server application.
- Click **Save**.
- Click **Test Connection** to confirm that the connectivity is established with the COSEC WEB Server application.

Under **Destination Location**, configure the following:

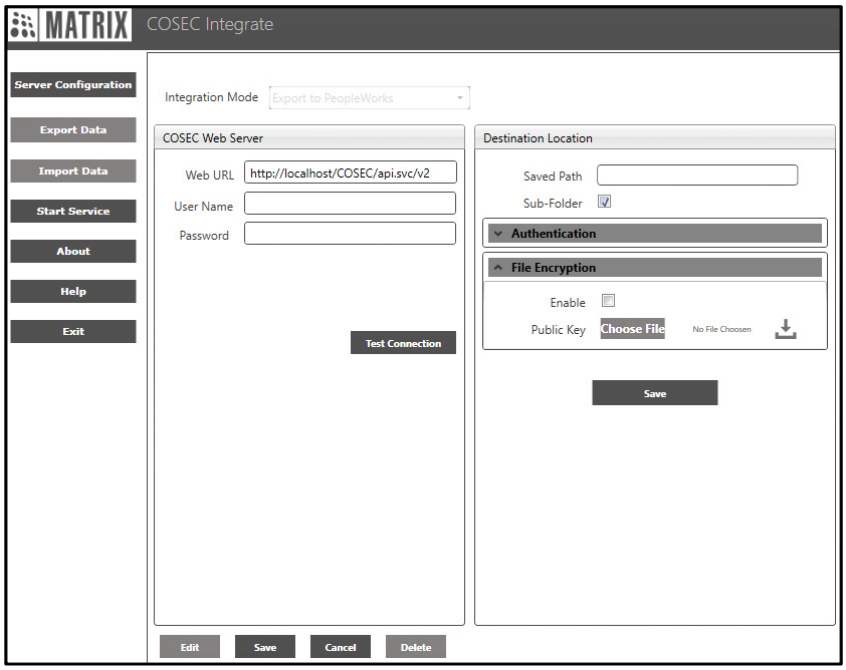
- **Saved Path:** Specify the Path at which the exported files are to be stored.
- **Sub-Folders:** Select the Sub-Folders check box to enable a folder hierarchy to be created at the export destination for the exported file.

Click **Authentication** collapsible panel and configure the following:



- **User Name:** Enter the User Name to be used for authentication while accessing the Path.
- **Password:** Enter the Password to be used for authentication while accessing the Path.

Click **File Encryption** collapsible panel and configure the following:



The file will be encrypted using PGP (Pretty Good Privacy) encryption method using AES algorithm.

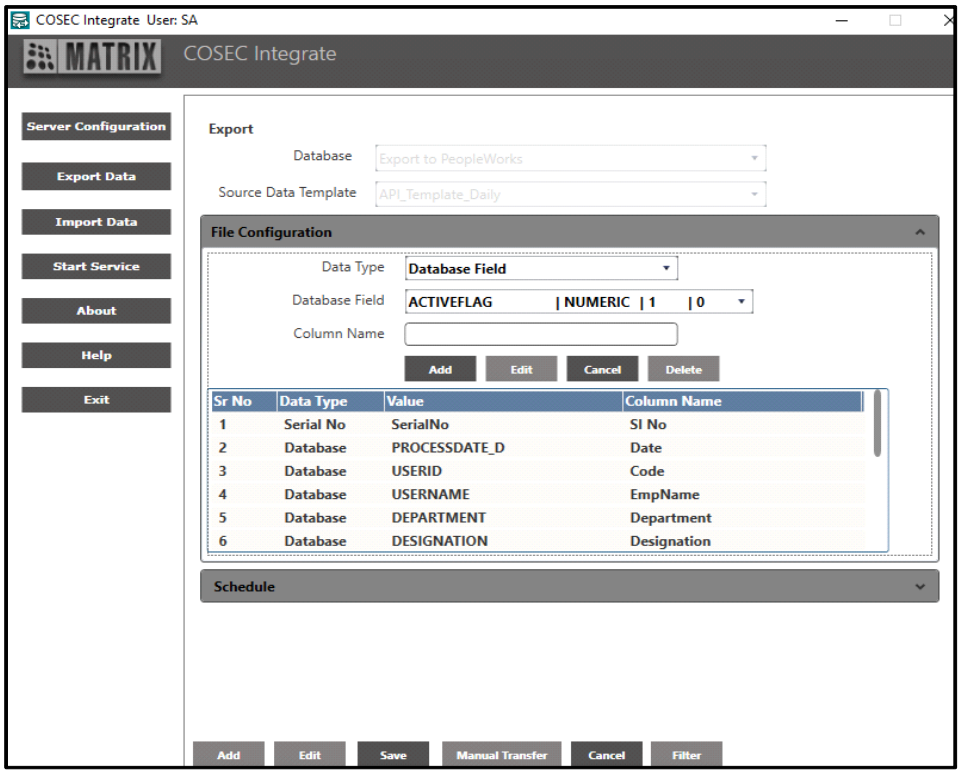
- **Enable:** Select this check box to enable encryption. If enabled the file will be encrypted using the Public Key provided by the Third Party and then will be saved on the Path.
- **Public Key:** Click **Choose** and select the key file which is to be used for encryption. This will be provided by the Third Party. Maximum file size supported is 5 MB.

If File Encryption check box is enabled, then Third Party must take the last updated file based on time stamping from the Saved Path.

- Click **Save**.

PeopleWorks Export Configuration

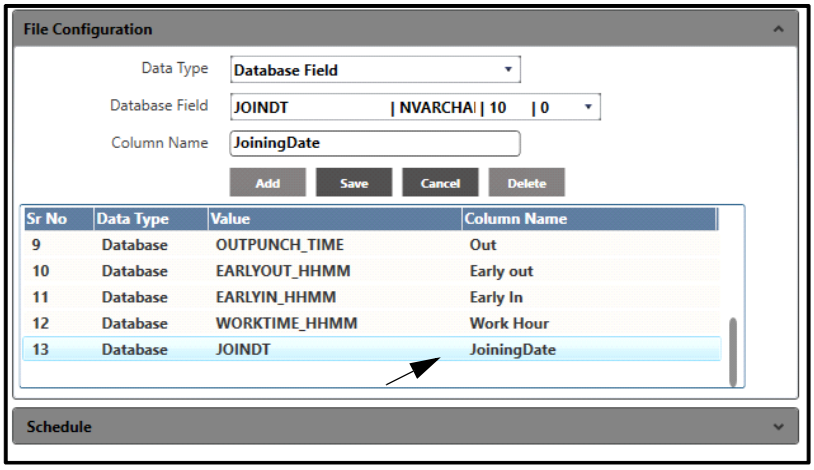
Click the **Export Data** button to map fields between source and destination tables. Select the Database type as **Export to PeopleWorks**.



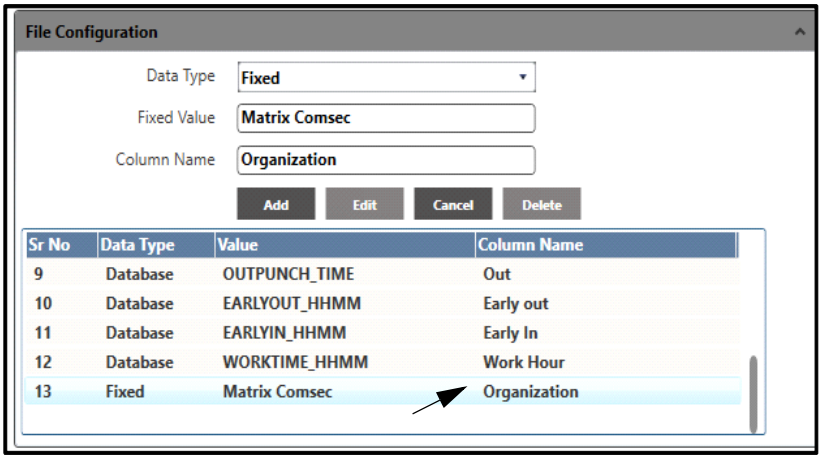
Click on the **Edit** button.

Select a **Data Type** to configure fields. There are four data types to choose from:

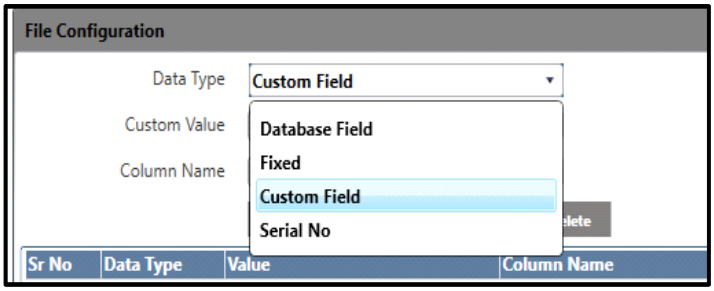
- **Database Field**: Select a Database Field from the drop-down list to be added to the export file and define a new column name against it. Click **Add**.



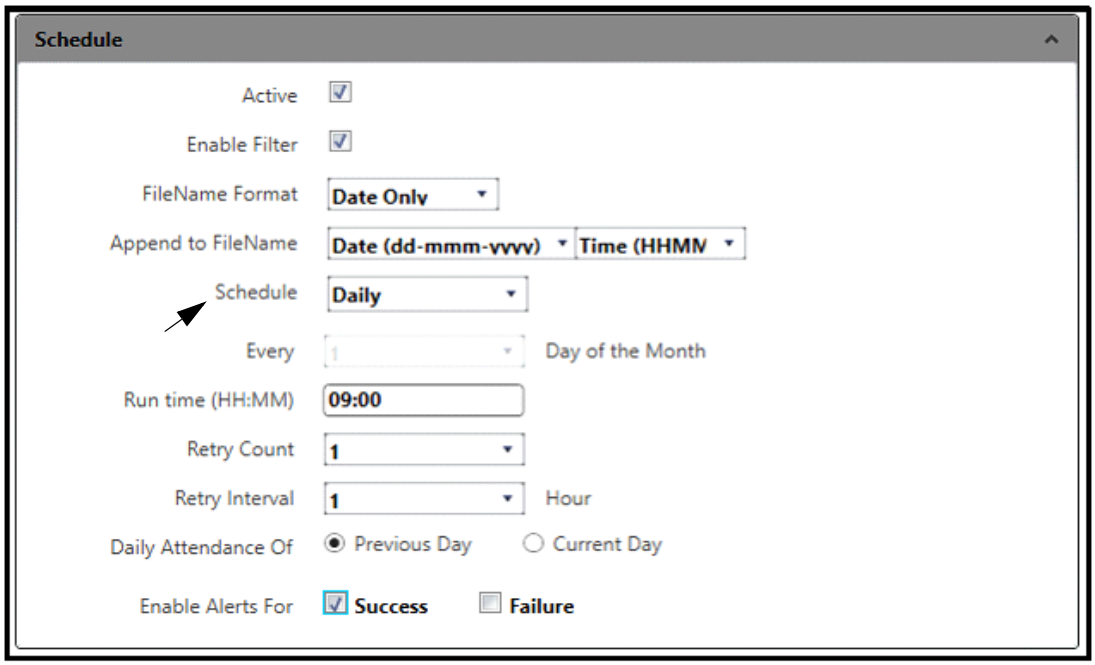
- **Fixed**: Select this option to set a fixed value for a field as shown below. For eg: the organization name remains common to all the employees, so it is considered as fixed value. Click **Add**.

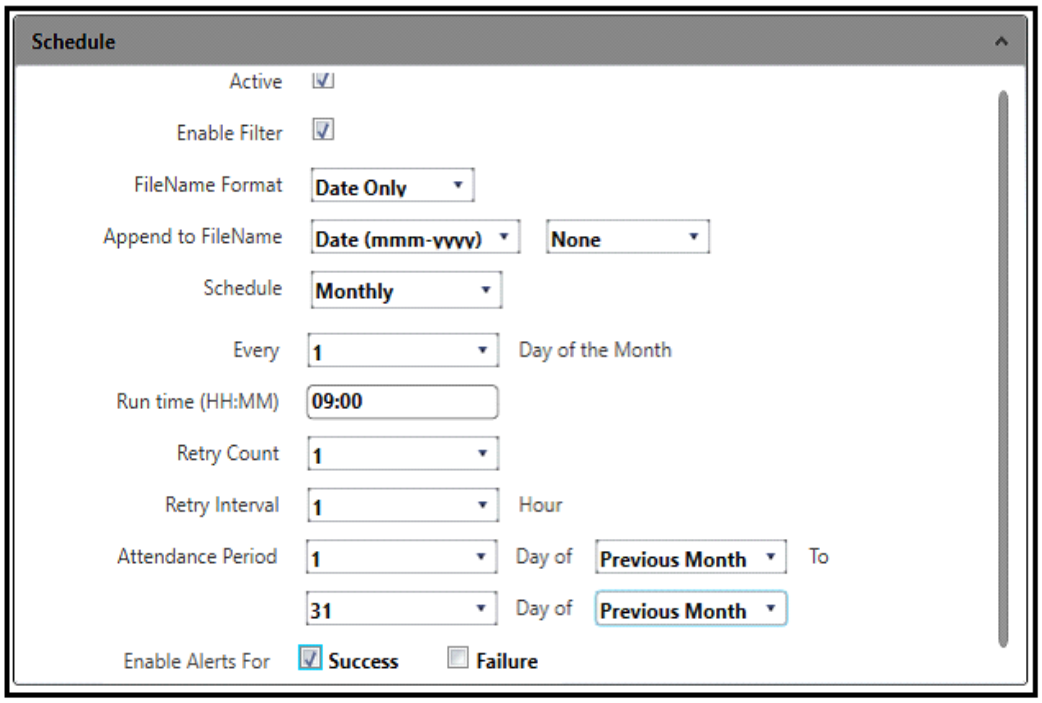


- **Custom Field**: Select this option to assign a custom value to a field. Click **Add**.
- **Serial No**: Select this option to set serial number as value for a column. Click **Add**.



In the **Schedule** section, user can set up a daily or monthly schedule for data export or export data manually using the **Manual Transfer** option.





The description of above fields is given in Export to MSSQL.

- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

  Select the checkboxes as per your requirement:

Select **Success** checkbox to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

Select **Failure** checkbox to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

If you require Alerts for both the above events, select both the check boxes.

In case of partial data transfer i.e. if both the above checkboxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

Example: There are in total 100 records which are to be transferred.

Now, out of 100 records, only 60 records are transferred Successfully and the remaining 40 records have Failed. Such data transfers are known as partial data transfers.

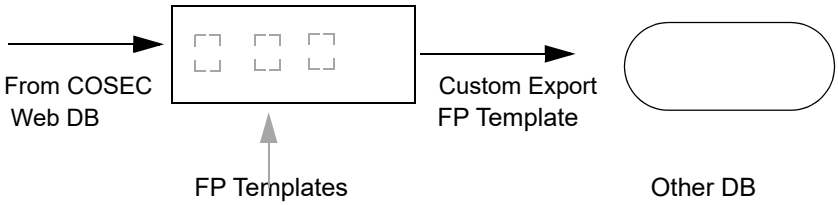
So here the connection status will be Failure and an alert will be sent to the configured COSEC Server along with the reason for failed data transfer.

It is to be supported for all integrate modes defined in COSEC Integrate where enable alerts provision is present i.e. for all the integration modes except for Custom Export-FP Template & Export FP Template to File.

Click **Save** and start service.

Export FP Template to File

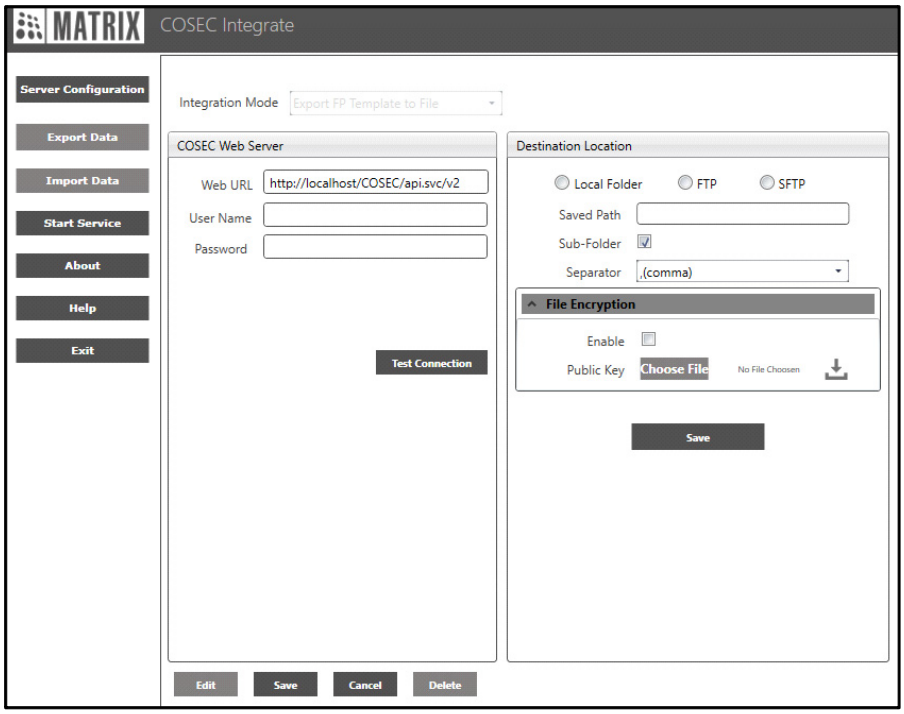
It is required to export FP Template of selected user to some directory path in physical file.



Click **Server Configuration.**

In **Integration Mode** select **Export FP Template to File**.

Click **Edit** to configure the parameters.



Under **COSEC Web Server** configure the following:

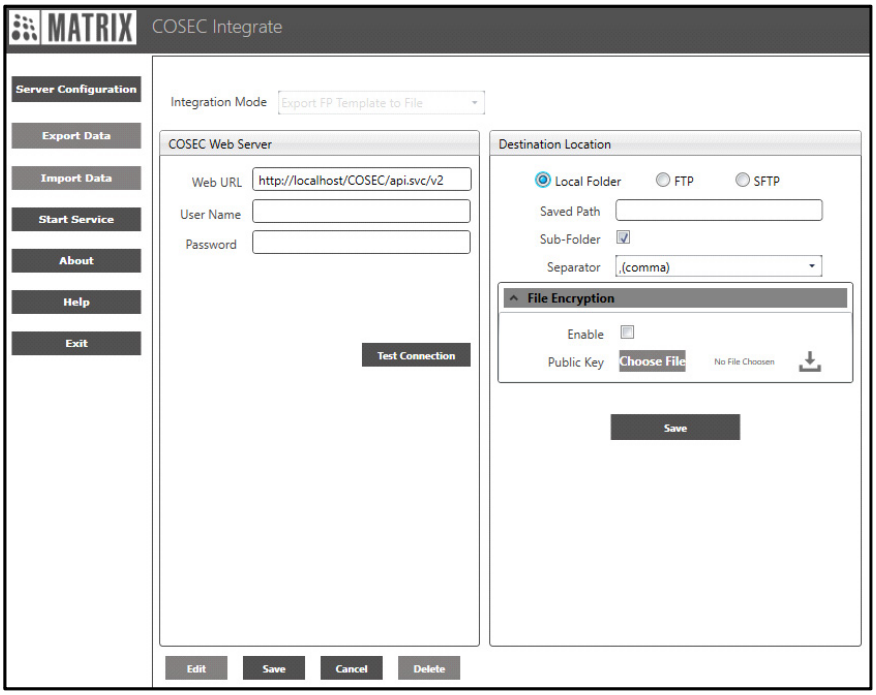
- **Web URL:** Specify the Web URL of the API service of the COSEC WEB Server application.
- **User Name:** Enter the User Name as **sa** as set for the COSEC WEB Server application.
- **Password:** Enter the Password as set for the COSEC WEB Server application.
- Click **Save**.
- Click **Test Connection** to confirm that the connectivity is established with the COSEC WEB Server application.

Under **Destination Location**, configure the following:

- Select the desired option — Local Folder, FTP or SFTP.

Local Folder

- If you select **Local Folder**, configure the following:



- **Saved Path:** Specify the Path at which the exported files are to be stored.
- **Sub-Folders:** Select the Sub-Folders check box to enable a folder hierarchy to be created at the export destination for the exported file.
- **Separator:** Select the separator which will be used to separate the fields in the exported file.

Click **File Encryption** collapsible panel and configure the following:

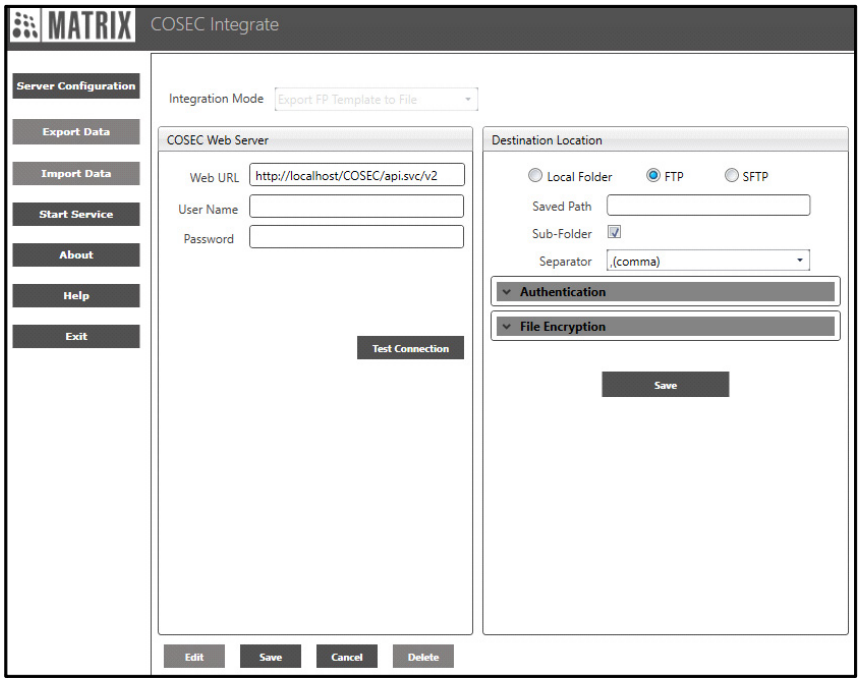
The file will be encrypted using PGP (Pretty Good Privacy) encryption method using AES algorithm.

- **Enable:** Select this check box to enable encryption. If enabled the file will be encrypted using the Public Key provided by the Third Party and then will be saved on the Path.
- **Public Key:** Click **Choose** and select the key file which is to be used for encryption. This will be provided by the Third Party. The maximum file size supported is 5MB.

- *If File Encryption check box is enabled, then Third Party must take the last updated file based on time stamping from the Saved Path.*
- Click **Save**.

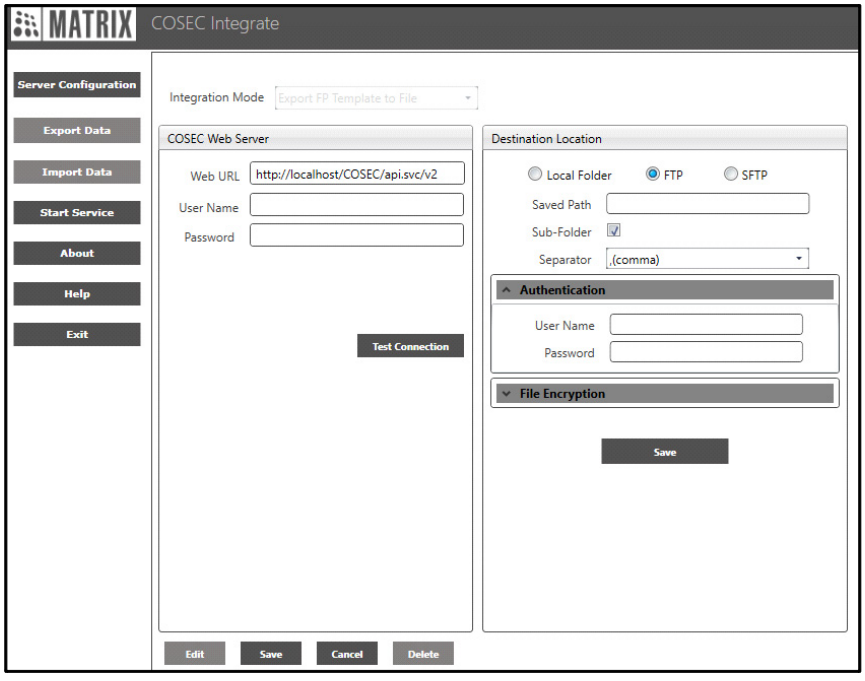
FTP

- If you select **FTP**, configure the following:



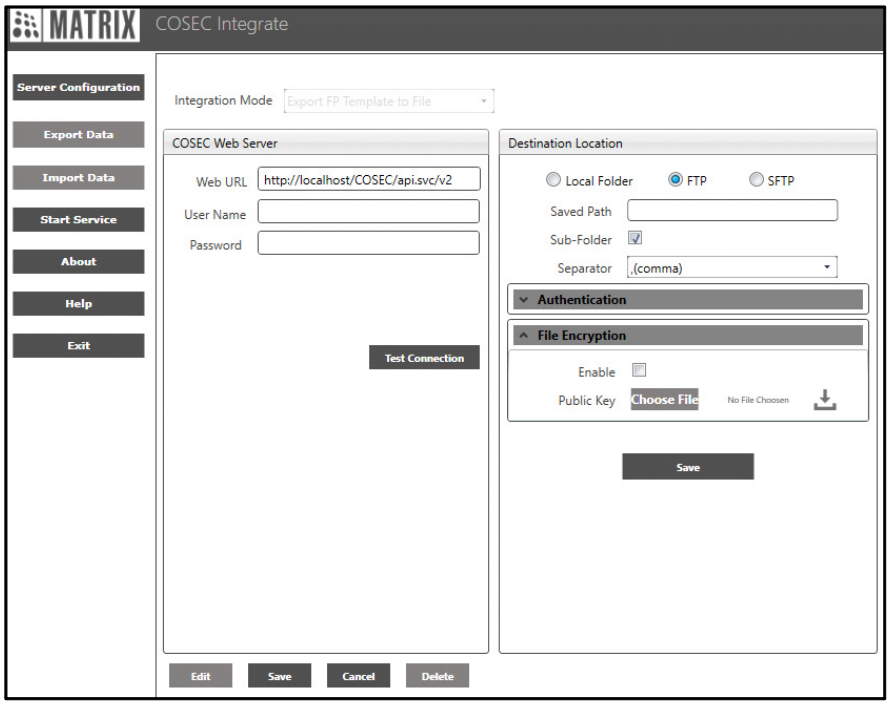
- **Saved Path:** Specify the Path at which the exported files are to be stored.
- **Sub-Folders:** Select the Sub-Folders check box to enable a folder hierarchy to be created at the export destination for the exported file.
- **Separator:** Select the separator which will be used to separate the fields in the exported file.

Click **Authentication** collapsible panel and configure the following:



- **User Name:** Enter the User Name to be used for authentication while accessing the Path.
- **Password:** Enter the Password to be used for authentication while accessing the Path.

Click **File Encryption** collapsible panel and configure the following:



The file will be encrypted using PGP (Pretty Good Privacy) encryption method using AES algorithm.

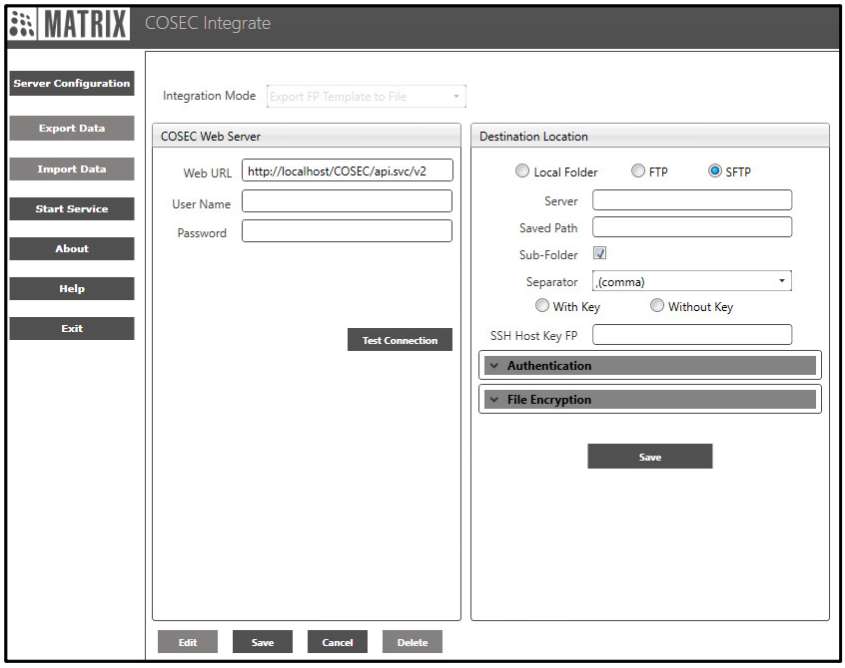
- **Enable:** Select this check box to enable encryption. If enabled the file will be encrypted using the Public Key provided by the Third Party and then will be saved on the Path.
- **Public Key:** Click **Choose** and select the key file which is to be used for encryption. This will be provided by the Third Party. Maximum file size supported is 5 MB.

If File Encryption check box is enabled, then Third Party must take the last updated file based on time stamping from the Saved Path.

- Click **Save**.

SFTP

- If you select **SFTP**, configure the following:



- **Server:** Specify the SFTP Server IP Address where the exported files are to be stored.

  COSEC Integrate communicates with the SFTP Server using the default port number 22. If you wish to use any other port, then you need to configure the same in the format Server IP Address:Port. For example if Port 33 is to be used then configure the Server as 192.168.104.20:33.

- **Saved Path:** Specify the Path at which the exported files are to be stored.

- **Sub-Folders:** Select the Sub-Folders check box to enable a folder hierarchy to be created at the export destination for the exported file.

- **Separator:** Select the separator which will be used to separate the fields in the exported file.

- For additional authentication and security, you can select the desired option — **With Key** or **Without Key**.

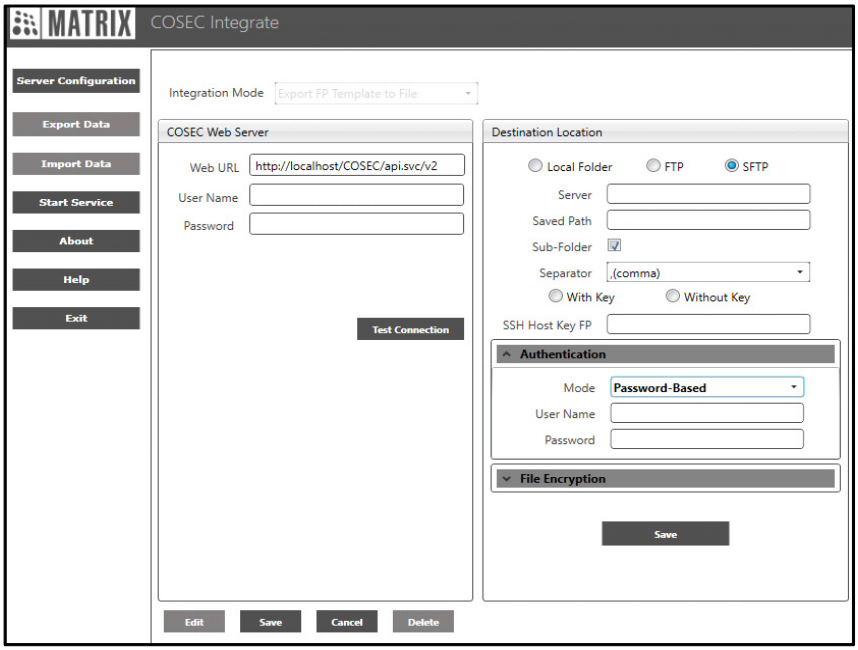
  If you select **With Key**, then configure the **SSH Host Key FP**.

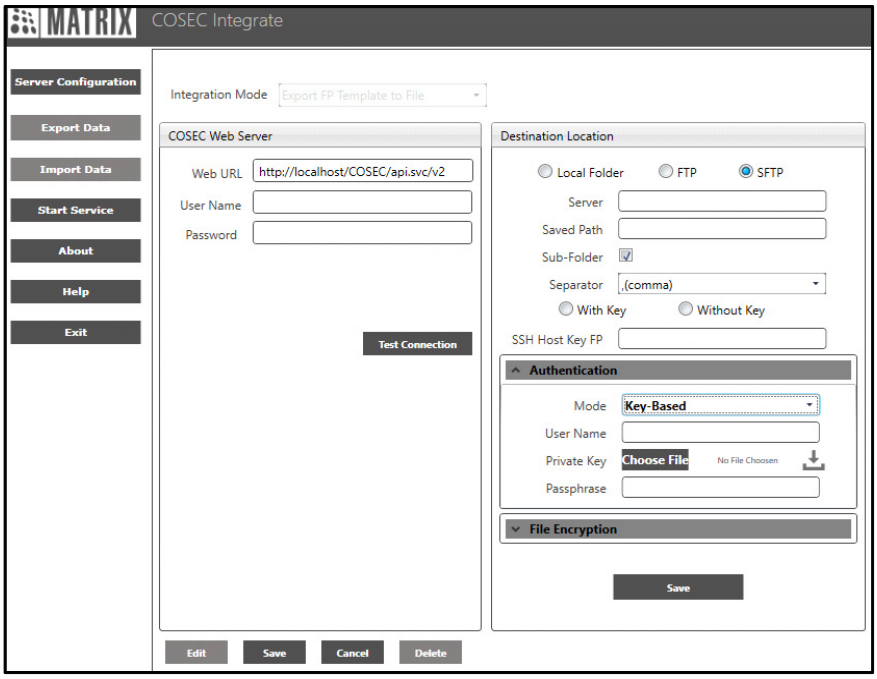
  The **SSH Host Key FP** servers as a unique identifier for the Server. This is a cryptographic representation of the Servers Public Key. It is used to verify the authenticity of the Server during the connection process. It is used to ensure that the Server the client is connecting to is the same Server that it connected with previously.

  This key is provided by the Administrator of the SFTP Server to the clients.

  If you select **Without Key**, then no key is required.

Click **Authentication** collapsible panel and configure the following:





- **Mode:** Select the desired mode for authentication — **Password-Based**, **Key-Based**.

If you select **Password-Based,** configure the following:

In Password-Based, when a client signs in, the Server checks the User Name and Password combination and then approves/denies the request.

- **User Name:** Enter the User Name to be used for authentication while accessing the Path.

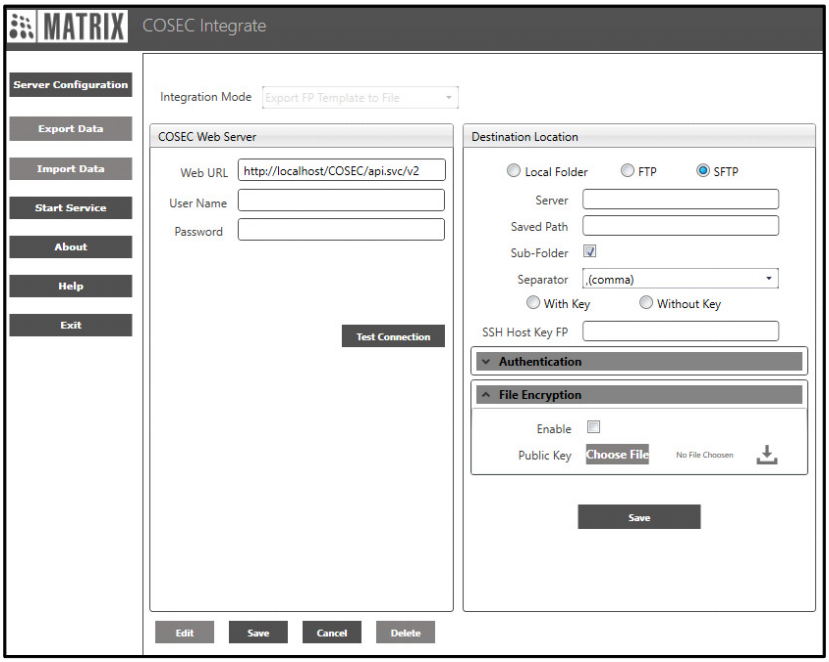
- **Password:** Enter the Password to be used for authentication while accessing the Path.

If you select **Key-Based,** configure the User Name, Private Key and Passphrase.

In Key-Based, when a client signs in, a pair of keys — Private and Public — are used for authentication. The Public Key is uploaded in the SFTP Server while the Private Key is provided to the client.

- **User Name:** Enter the User Name to be used for authentication while accessing the Path.
- **Private Key:** Click **Choose** and select the key file which is to be used for authentication.
- **Passphrase:** Enter the Passphrase. This is used in combination with the Private Key to acquire the SFTP Server access.

Click **File Encryption** collapsible panel and configure the following:



The file will be encrypted using PGP (Pretty Good Privacy) encryption method using AES algorithm.

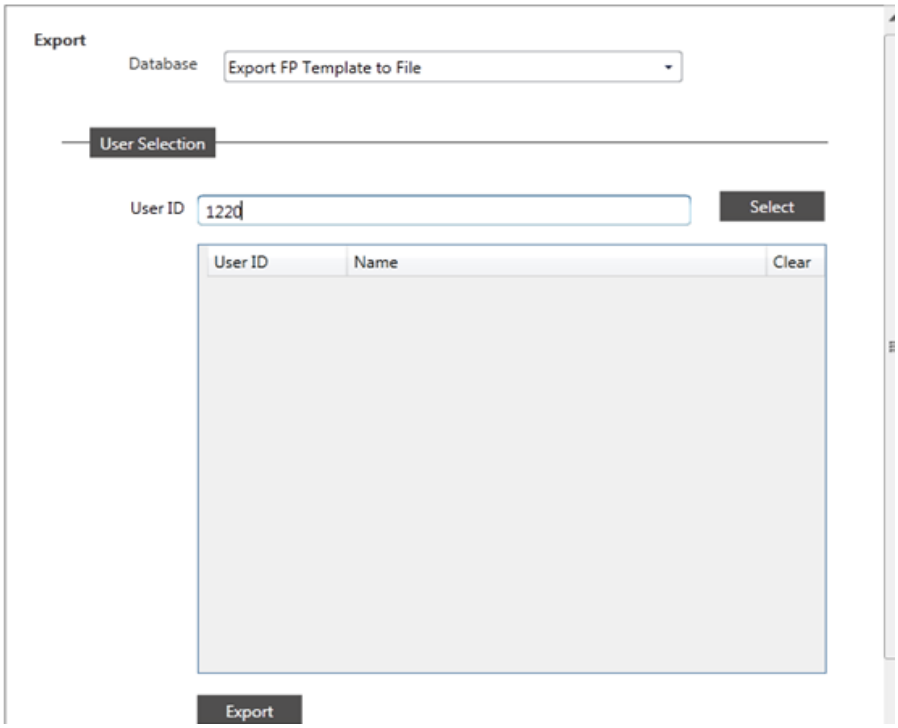
- **Enable:** Select this check box to enable encryption. If enabled the file will be encrypted using the Public Key provided by the Third Party and then will be saved on the Path.
- **Public Key:** Click **Choose** and select the key file which is to be used for encryption. This will be provided by the Third Party. Maximum file size supported is 5 MB.

If File Encryption check box is enabled, then Third Party must take the last updated file based on time stamping from the Saved Path.

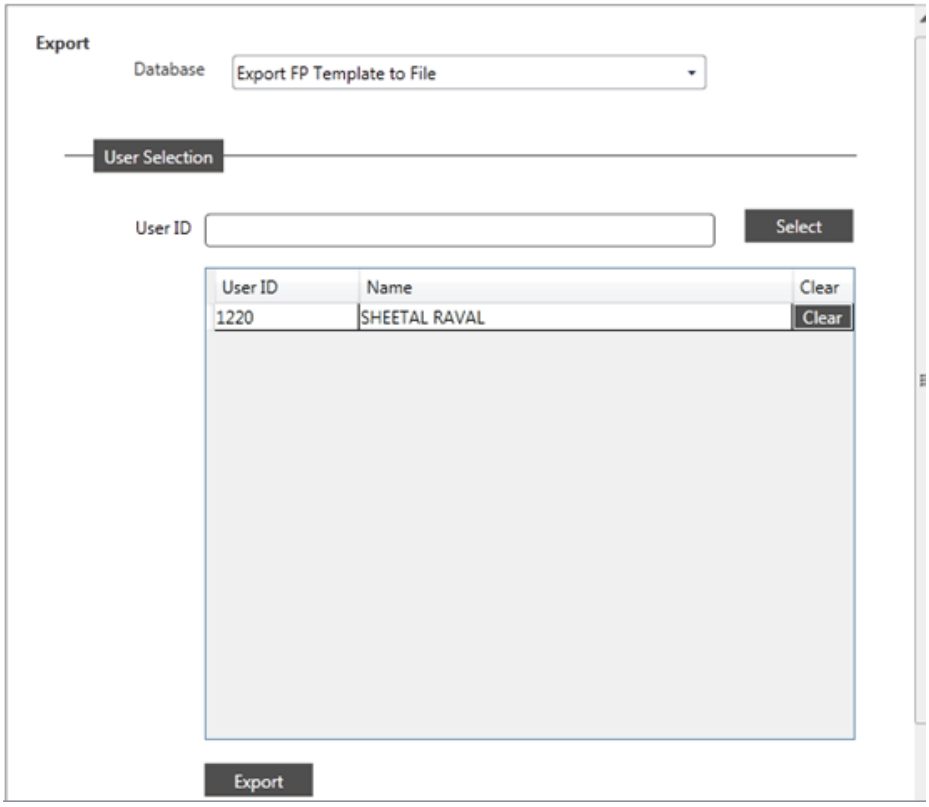
- Click **Save**.

Export Data Configuration

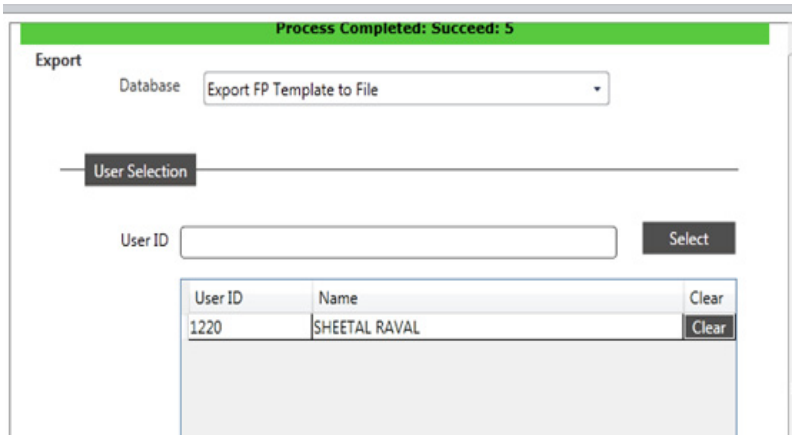
This option enables the admin user to specify the fields whose values are to be exported to the FP template file.



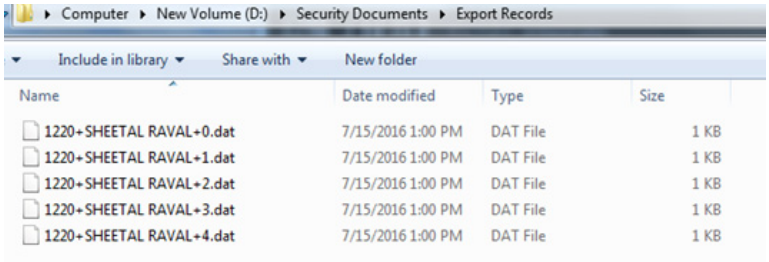
Enter the **User ID** of the user whose FP templates are to be backed up. And click on **Select** button.
The user ID and name will be displayed in the grid.



Now click on **Export** button. The export completion will be shown as below:

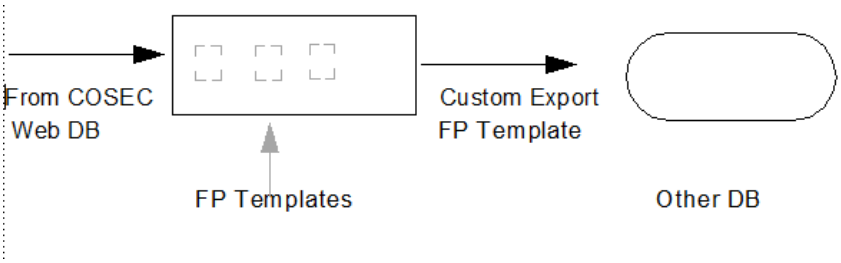


Here you can find 5 FP templates of selected user which are exported as individual files at the Destination location.



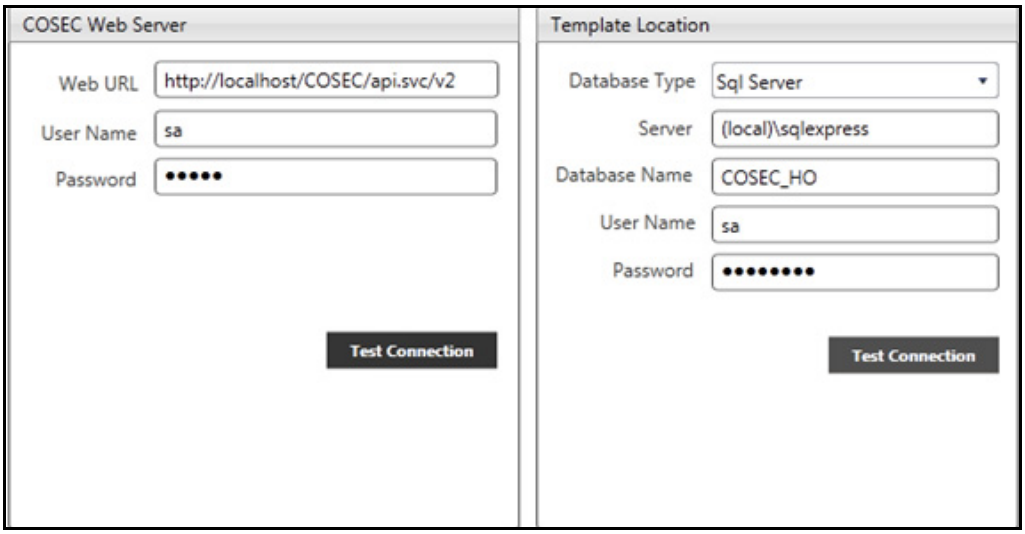
Custom Export- FP Template

Provision is required in Integrate from where user can select physical file of FP templates and insert them to configured database's table with various user details like user id, name, user photo and finger print location. This purpose is served through “Custom Export of FP Template”.



Click on the **Server Configuration** option and select the **Custom Export- FP Template** option as the **Integration Mode**.

Click on the **Edit** button.



In the **COSEC Web Server** section:

- Specify the web url of the API service of the COSEC WEB application as shown.
- Enter the User Name and Password of the sa user as set in the COSEC WEB application.

The **Test Connection** button is provided to test the connections with the web server

IIn the **Template Location** section:

- The **Database Type** can be selected as SQL SERVER or ORACLE server.
- **Server**: Enter the database server name in the following format - **Database server name\Instance Name** e.g. dbserver\sqlexpress.
- **Database Name**: Specify the database name of the destination database as per the site settings. Eg: COSEC_HO is the destination database to which you can export the data.

For newly created database, ensure that you have set the password in COSEC Web application. Then only Test connection from COSEC Integrate with Web server will be successful.

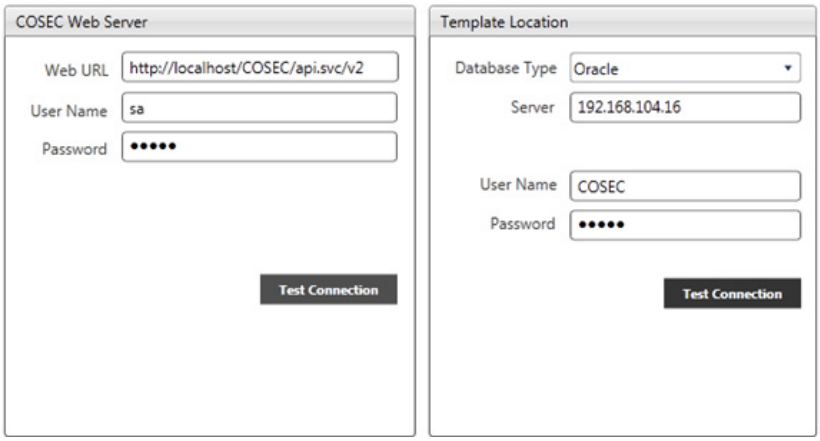
- **User Name**: Specify the database administrator ID in this field. This is the username which you have set while installing SQL Server Management Studio in your computer.

- **Password**: Enter the password of the Database administrator as per the site settings. This is the password which you have set while installing SQL Server Management Studio in your computer.

The **Test Connection** button is provided to test the connections with the web server as well as the SQL Server database.

Click on **Save** once done.

In the event of selecting the **Export to Oracle Server** option in the **Integration Mode** field, specify the Oracle server destination address as well as the username and the password (case-sensitive for Oracle Server) in the respective fields as shown below:

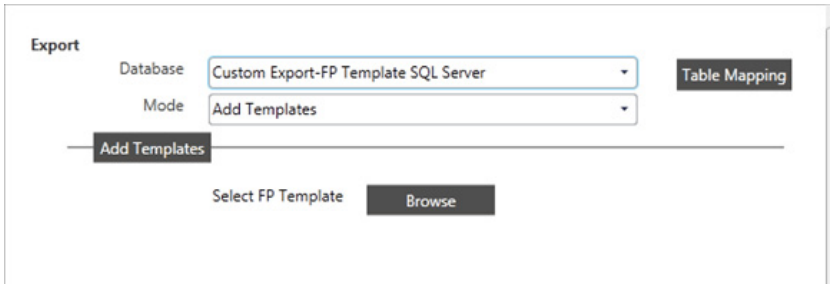


Test the connection and Save the configuration.

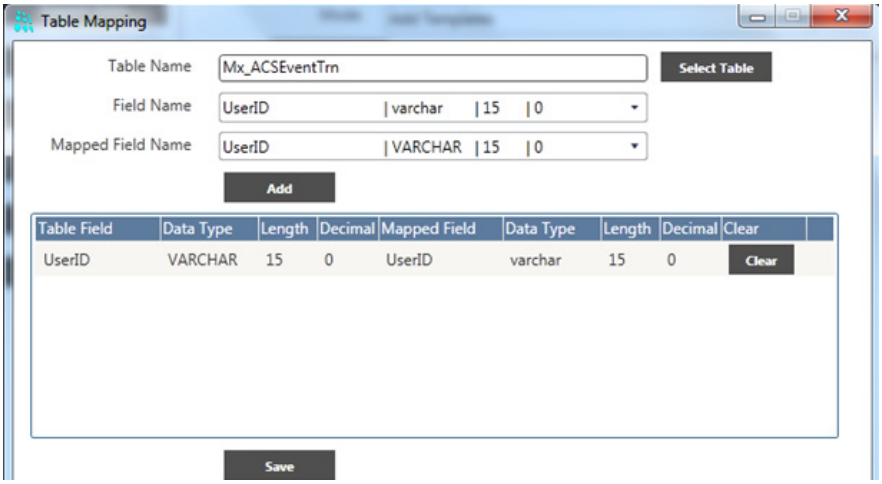
Export Data Configuration

This option enables the admin user to specify the fields whose values are to be exported.

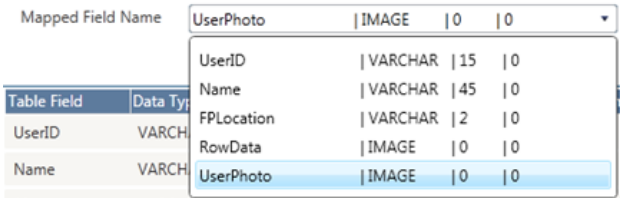
Select the Database "**Custom Export-FP Tempate SQL Server".**
Select the Mode as **Add Templates** to add the FP templates or **Delete Templates** to delete the FP templates.



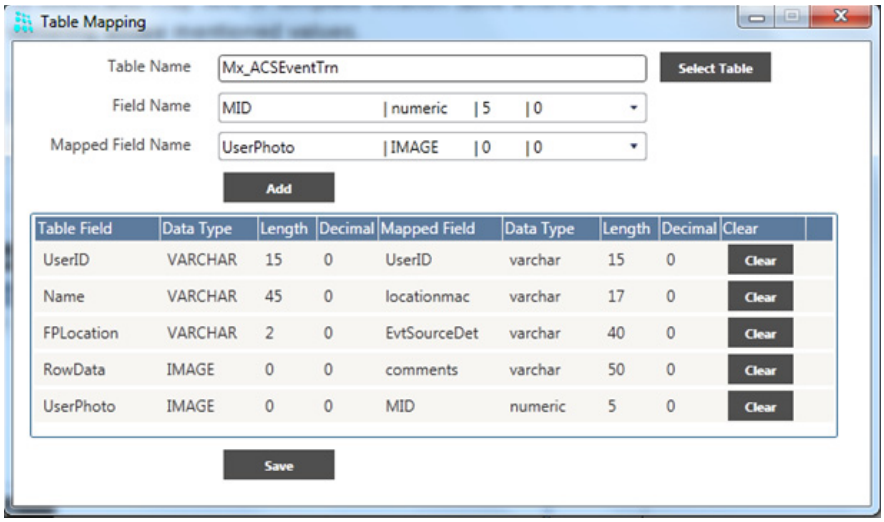
Click the **Table Mapping** button. Then select the table where the user details are to be mapped.



You have to map all the user fields shown below to the desired field selected from “Field Name” in above table mapping.

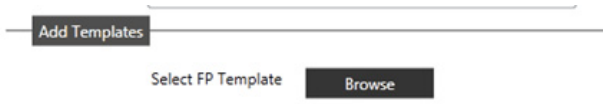


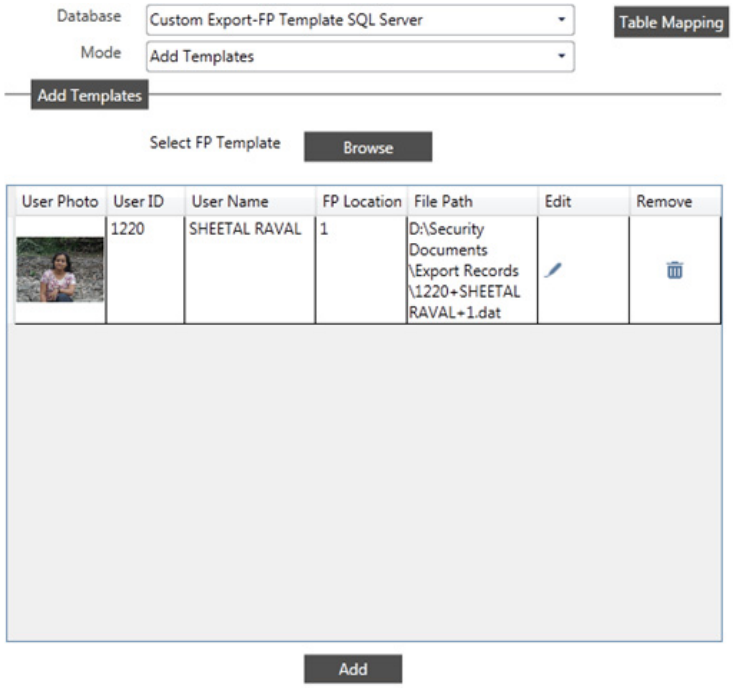
Eg: Name is mapped with locationmac as shown in second row.



After mapping all the user fields, click on **Save** button.

Now click on **Browse** button and select the FP template from the path (Local folder/FTP/SFTP) where the templates are stored.





The template with User photo, ID, Name and FP location will appear as shown above.

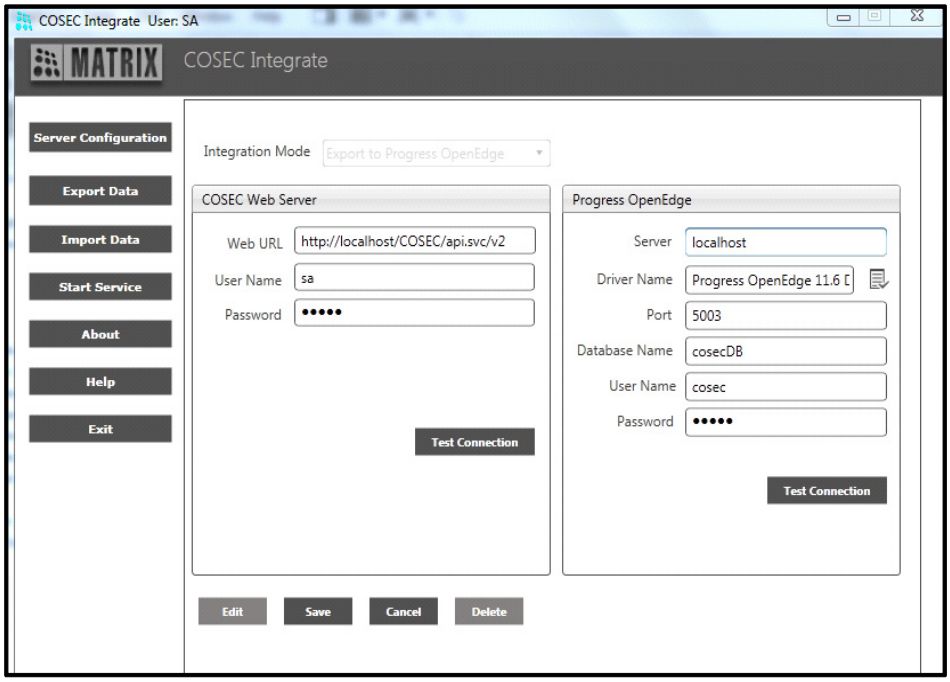
Finally click **Add** button. System will insert/update records in mapped template table.
Clicking **Remove** will remove all records from mapped template table with selected User ID.

Export to Progress OpenEdge

Click on the **Server Configuration** button to configure the Web server and Destination database for Export.

Select the **Export to Progress OpenEdge** option in the **Integration Mode** field. Click on the **Edit** button.

Integrate supports Export to Progress OpenEdge version OpenEdge 12.8

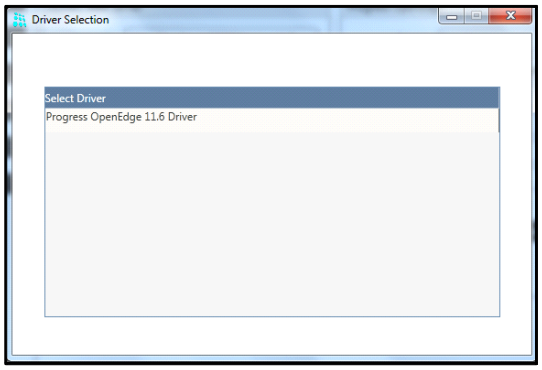


In the **COSEC Web Server** section:

- Specify the web url of the api service of the COSEC WEB application as shown.
- Enter the User Name and Password of the sa user as set in the COSEC WEB application.

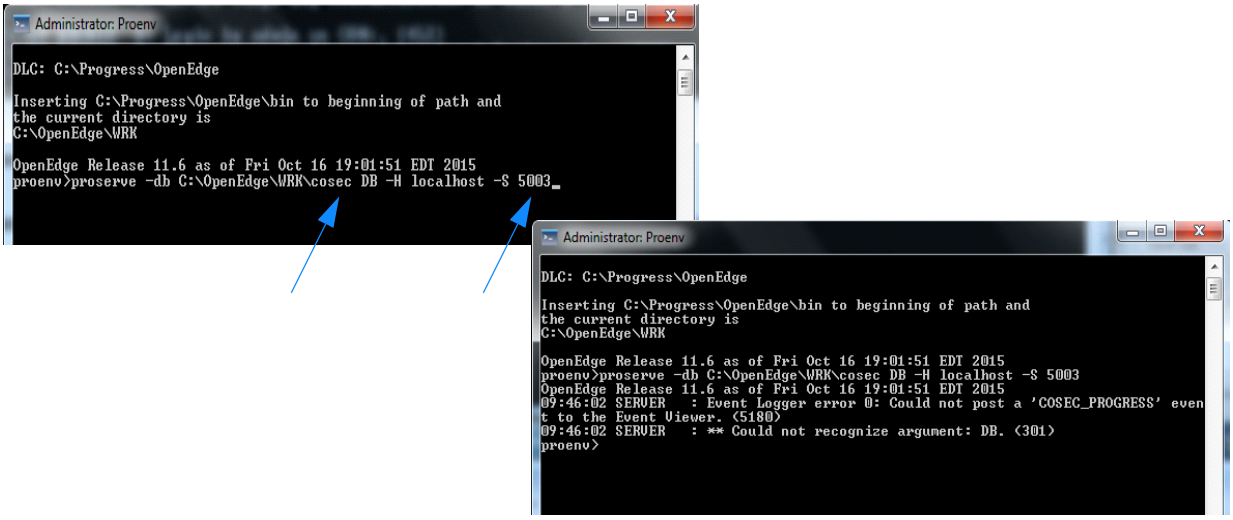
In the **Progress OpenEdge** section:

- **Server**: Enter the server name with which the Progress OpenEdge database is started.
- **Driver Name**: Select the Progress OpenEdge driver from the picklist. It is the software driver which will appear in picklist, once the database is installed.



- **Port:** Enter the port number at which the Progress OpenEdge database is running. It is the port number(eg: 5003) entered in command prompt while starting the database as shown below.

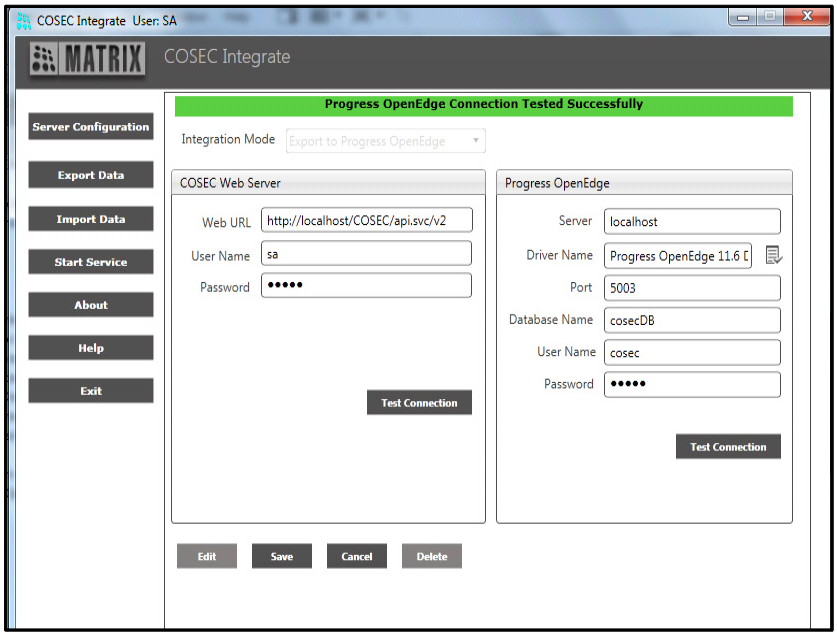
- **Database Name:** Enter the database name with which Progress OpenEdge database is started. It is case sensitive. Thus if Database is started with name cosecDB as shown below then enter the name as “cosecDB”.



- **User Name**: Specify the username as entered while creating the database.

- **Password**: Specify the password as entered while creating the database. Eg: Username is cosec and Password is cosec.

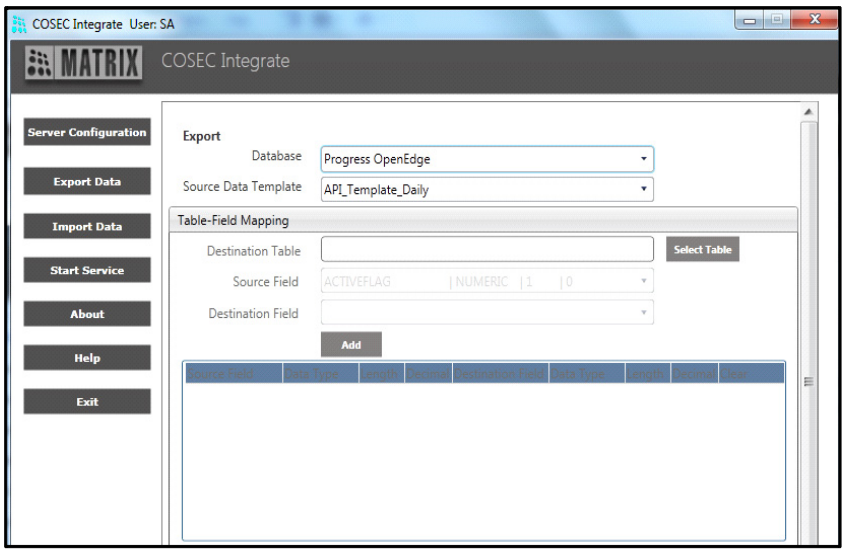
The **Test Connection** button is provided to test the connections with the web server as well as the Progress OpenEdge database.



Click on **Save** button to save the server configuration.

Export Data Configuration

This option enables the admin user to map the fields from the COSEC database tables to fields in a third party database. Click on the **Export Data** button. The following page appears.



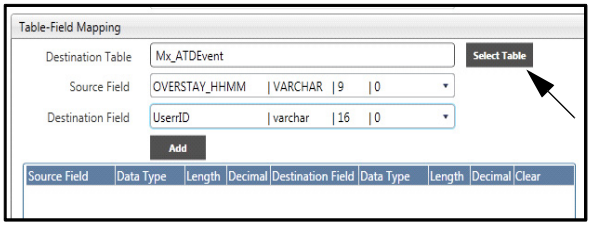
The COSEC INTEGRATE application provides four data templates in line with the default **Database Views** as shown. The COSEC System provides the following four Database views which would provide the relevant field options to be mapped with the fields of a destination database.

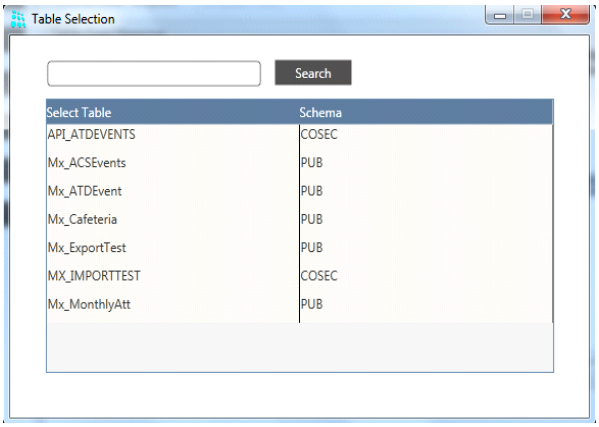
- Monthly Attendance Summary
- Daily Attendance Detail
- Attendance Events
- Access Control Events

Each of the above database views would provide the relevant fields whose values can be exported from the COSEC database. Select the required data template and click on the **Edit** button at the bottom of the page.

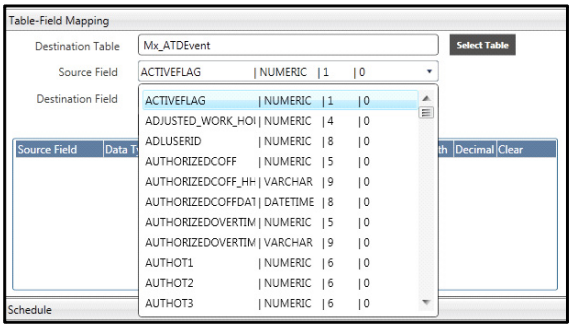
Now the admin user can start the **mapping of the fields** from the source database to that of the destination database as shown.

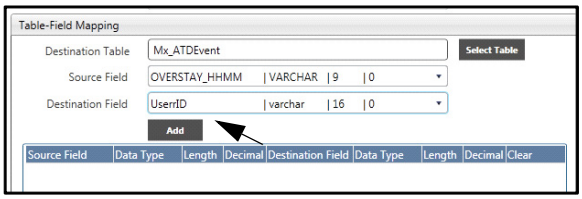
- Select the **Destination Table** by clicking **Select Table** button. The table selection picklist appears as below.



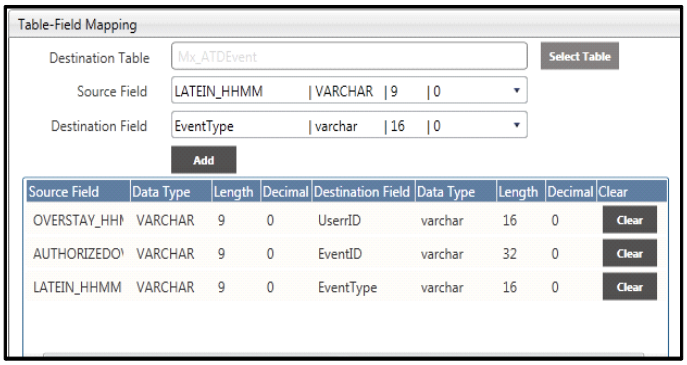


- Select the **Source field** from the COSEC database.





- Select the **Destination field** from the selected destination table.
- Click on the **Add** button. The mapped fields will be visible in the bottom grid as shown.

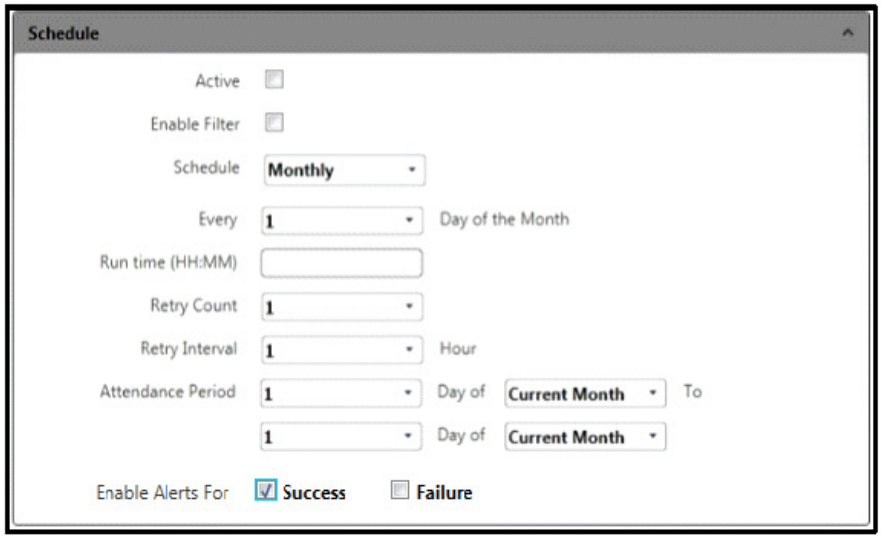


In the case of Attendance Events and Access Control Events the user needs to map the UserID and the EventDateTime_D source fields to fields in the destination table.

Map the UserID, PMonth and Pyear source fields to appropriate fields in the destination table in the case of the Monthly Attendance Summary.

Map the UserID and ProcessDate_D source fields to appropriate fields in the destination table in the case of the Daily Attendance Detail.

The **Schedule section** enables the admin user to schedule the data export process. The schedule option varies based on the selected Source Data Template. The **Daily Attendance detail** will have the following options as shown.



- Check the **Active** box to enable the schedule.
- The **Enable Filter** option is provided to enable the administrator to filter the users whose data is to be exported. Check this box and click on the **Filter** button. The Multiple selection window appears. Select the users whose data is to be exported.
- Specify the day of the month on which the export process is to be run.
- Specify the **Run time** in HH:MM format when the export process is to be run.
- Set the **Retry Count** from the drop down list.
- Set the **Retry Interval** in hours from the drop down list. This parameter specifies the time period between successive retries.
- Specify the **Attendance Period** by specifying the starting and the ending day of the attendance period for which the data is to be exported.
- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

  Select the checkboxes as per your requirement:

  Select **Success** checkbox to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

  Select **Failure** checkbox to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

  If you require Alerts for both the above events, select both the check boxes.

  In case of partial data transfer i.e. if both the above checkboxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

  Example: There are in total 100 records which are to be transferred.

Now, out of 100 records, only 60 records are transferred Successfully and the remaining 40 records have Failed. Such data transfers are known as partial data transfers.

So here the connection status will be Failure and an alert will be sent to the configured COSEC Server along with the reason for failed data transfer.

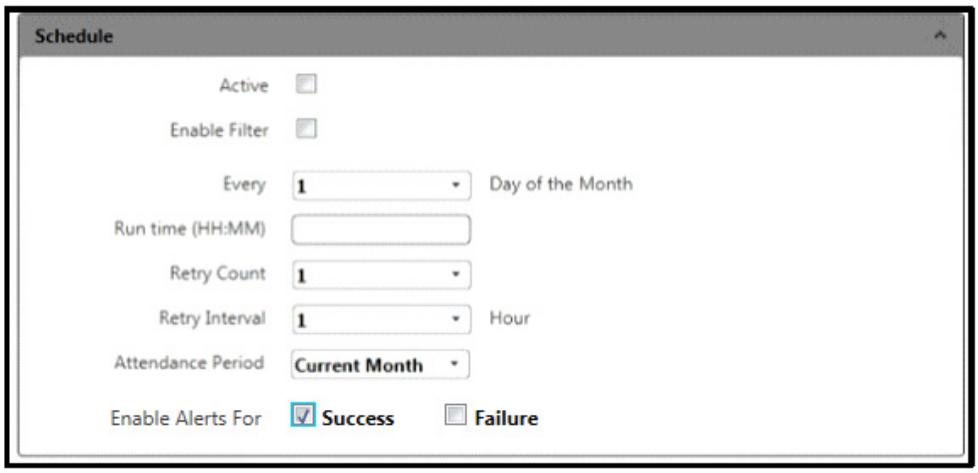
It is to be supported for all integrate modes defined in COSEC Integrate where enable alerts provision is present i.e. for all the integration modes except for Custom Export-FP Template & Export FP Template to File.

Select any one option for data transfer i.e, Daily or Monthly in the field **Schedule**.On selection of Monthly option, user can set data transfer process to run only once in a month.

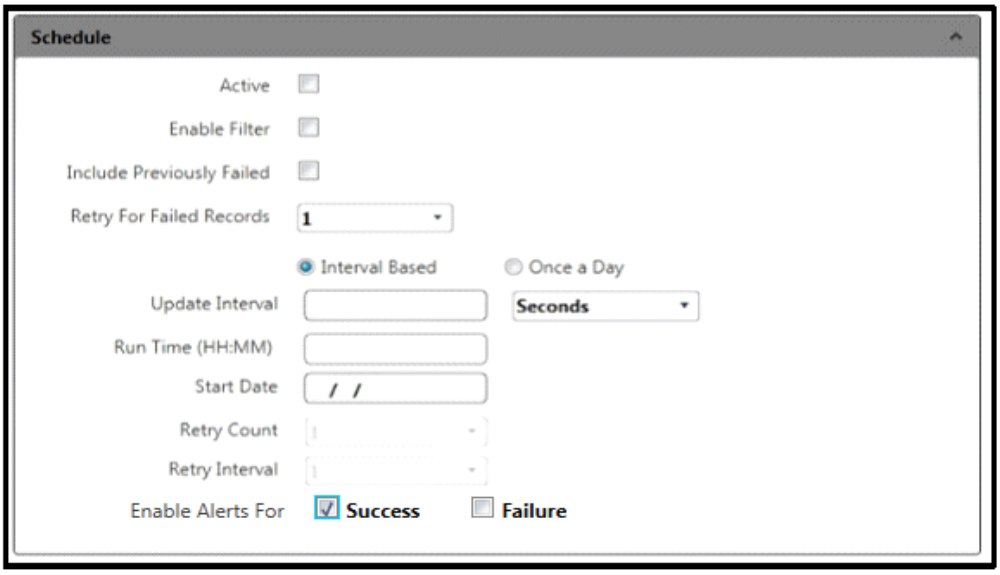
User can configure to transfer data for either previous day's attendance data or current day's attendance data with respect to schedule run day.

The **Monthly Attendance Summary** will have the following unique options:

- Select the **Attendance Period** for which the monthly Attendance summary data is to be exported.The Admin user can select either the **previous month** or **current month** option.

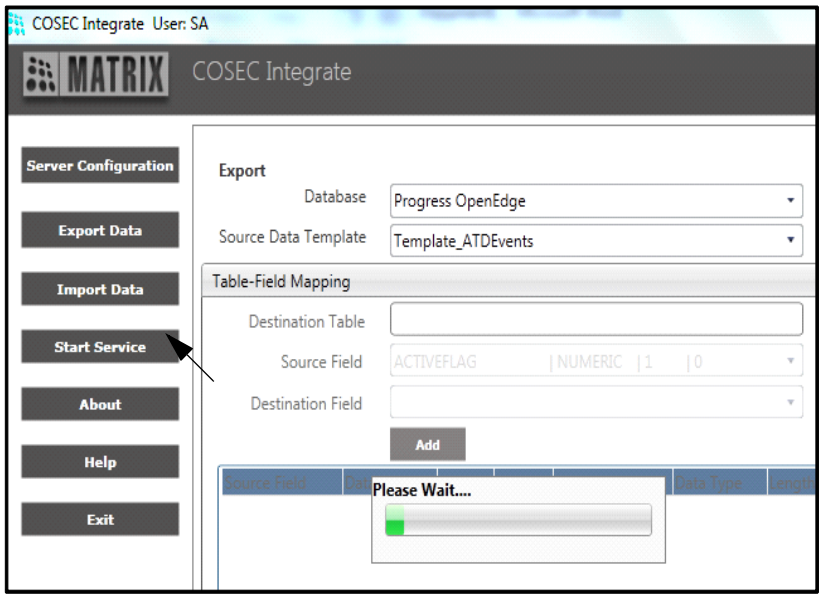


On selecting the **Attendance Events** or the **Access Control Events** the following schedule options will be available.



- Check the **Active** box to enable the schedule.
- Set the filter parameters as required.
- For **Interval based** schedule; Specify the **Update Interval** in seconds,minutes or hours to define the frequency at which the application will update the destination database.
  Specify the **Start Date** from which the export process is to be initiated.
- For **Once a Day** schedule, Specify the Run Time at which export will be intiated. You can mention Retry count and Retry Interval for which the retry for export will be done in case of failure.

After defining the above parameters, the admin user has to click on the **Start Service** button.



Import from MS SQL/Oracle/Postgre

The application allows the user to import user data from an external SQL, Oracle or Postgre database.

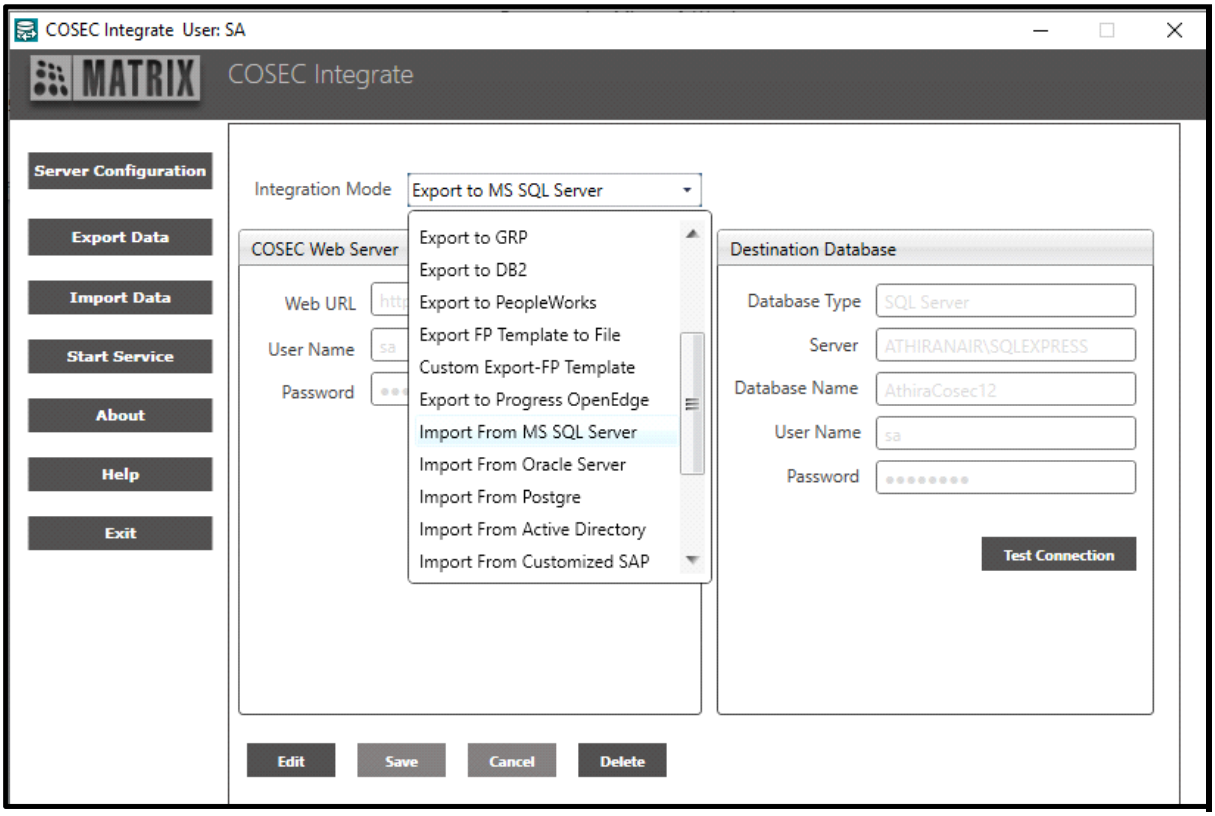
Click on the **Server Configuration** button to start the configuring process. The following page appears.

Select the **Import from MS SQL Server** option in the **Integration Mode** field. Click on the **Edit** button.

Integrate supports Import from MS SQL from version SQL Server 2005 to SQL Server 2022.

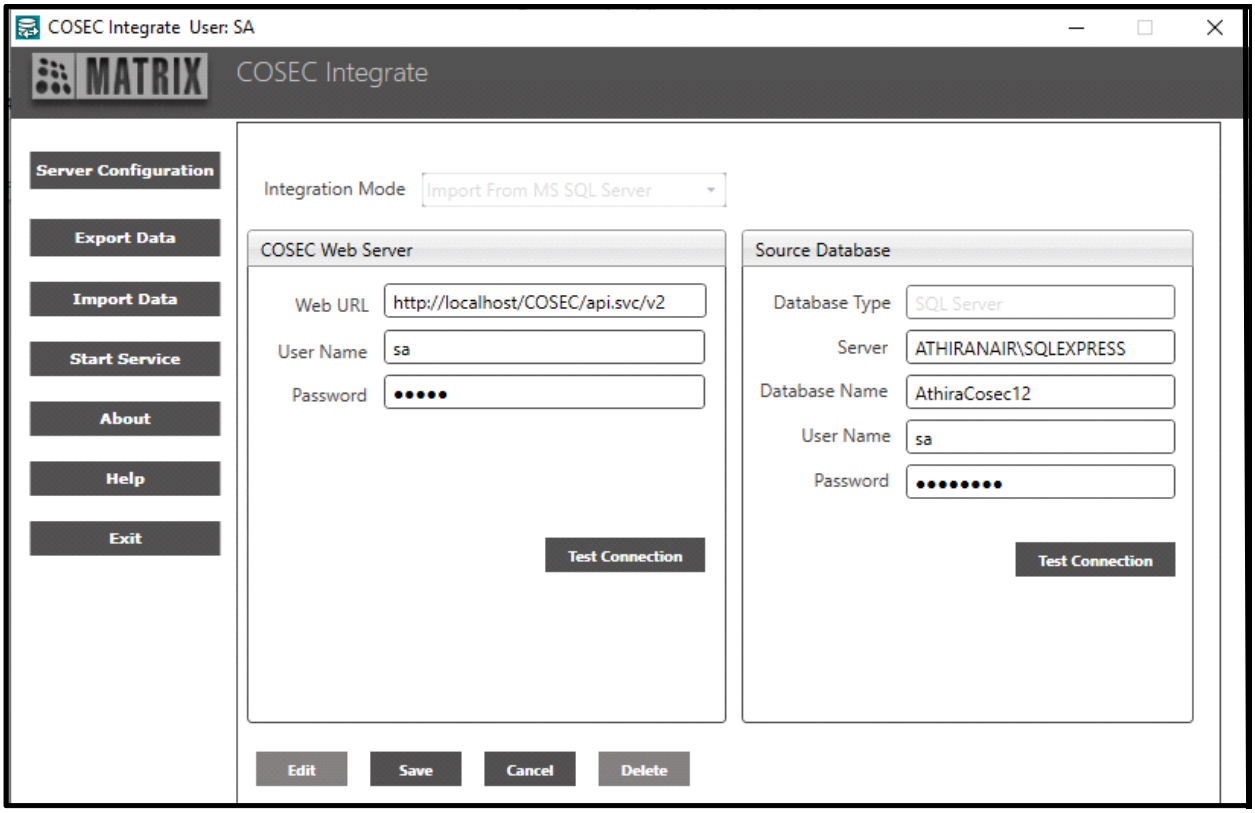
SQL Server 2005 and SQL Server 2008 R2:

- *for installation you need Windows 7 or below versions.*
- *to establish remote connections in these versions from the PC in which Integrate is installed, make sure you have enabled TLS 1.0 and 1.1 (that is, Best Practices settings).*



In the **COSEC Web Server** section:

- Specify the web URL of the API service of the COSEC WEB application as shown.
- Enter the User Name and Password of the SA user as set in the COSEC WEB application.



In the Source Database Server section:

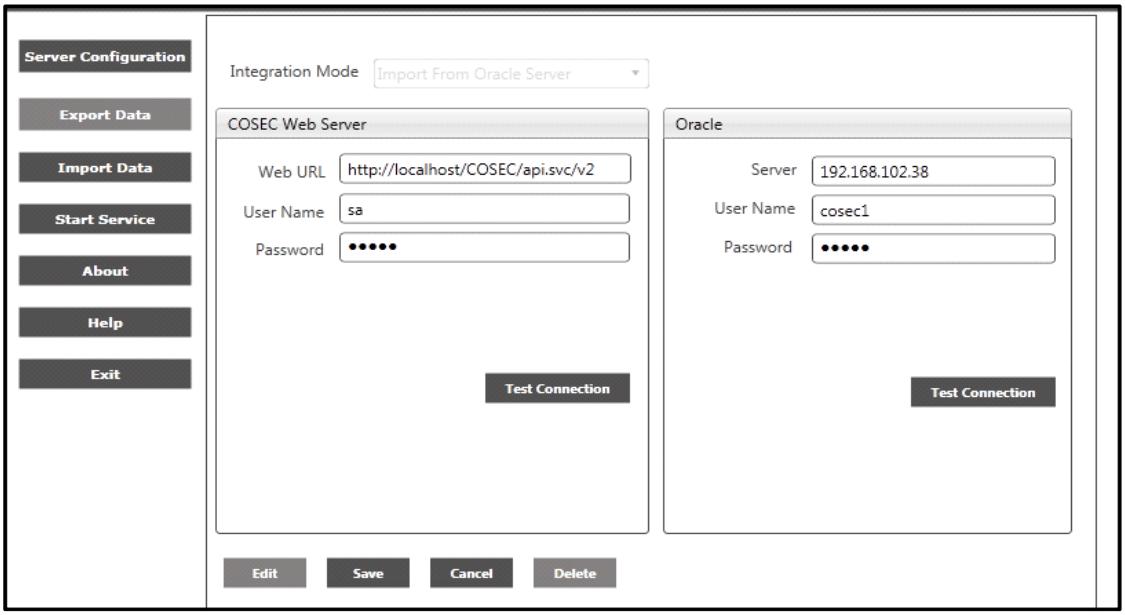
- Select the **Database Type** as SQL SERVER.
- **Server**: Enter the database server name in the following format:
- **Database server name\Instance Name** e.g. dbserver\sqlexpress.
- **Database Name**: Specify the database name of the source SQL database as per the site settings.
- **User Name**: Specify the database administrator ID in this field.
- **Password**: Enter the password of the Database administrator as per the site settings.

The **Test Connection** button is provided to test the connections with the web server as well as the MS SQL or Oracle Server database.

Click on **Save** once done.

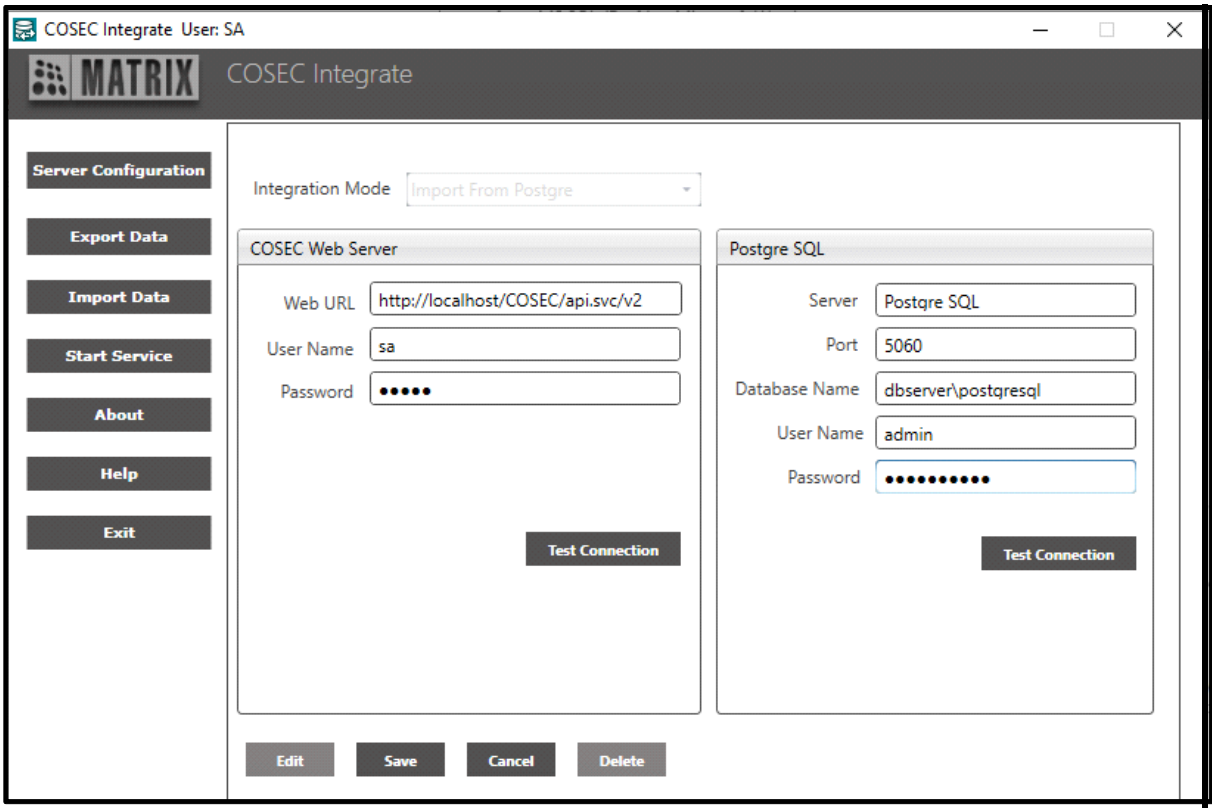
In the event of selecting the **Import from Oracle Server** option in the **Integration Mode** field, specify the source Oracle server address as well as the user name and the password (case-sensitive for Oracle server) in the respective fields as shown.

Integrate supports Import from Oracle from version Oracle 10g to Oracle 23AI.



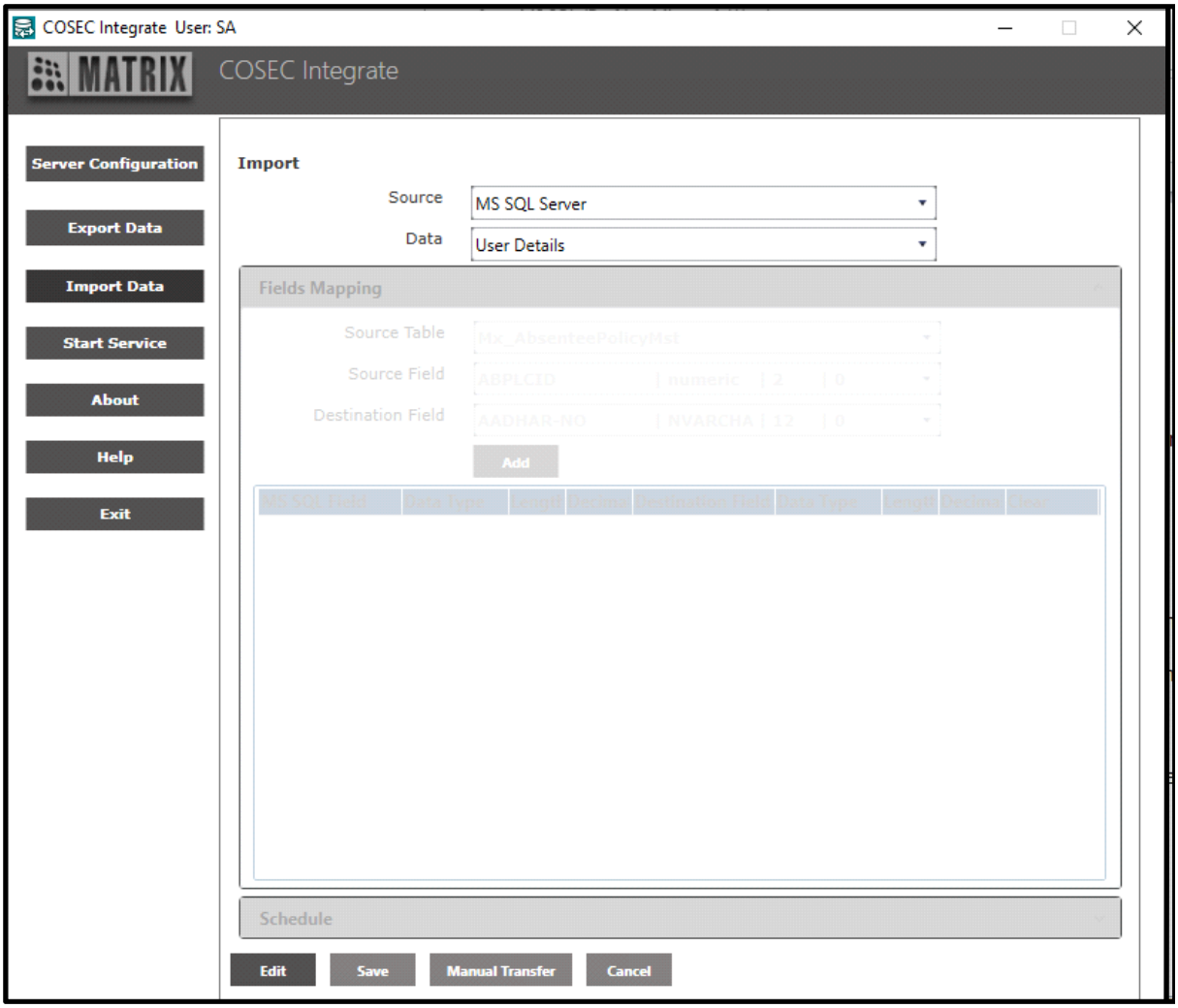
In the event of selecting the **Import from Postgre SQL** option in the **Integration Mode** field, specify the source Postgre SQL server address, Port number as well as the user name and the password (case-sensitive for Postgre SQL server) in the respective fields as shown.

Integrate supports Import from Postgre SQL from PostgreSQL 10.23 to PostgreSQL 12.18



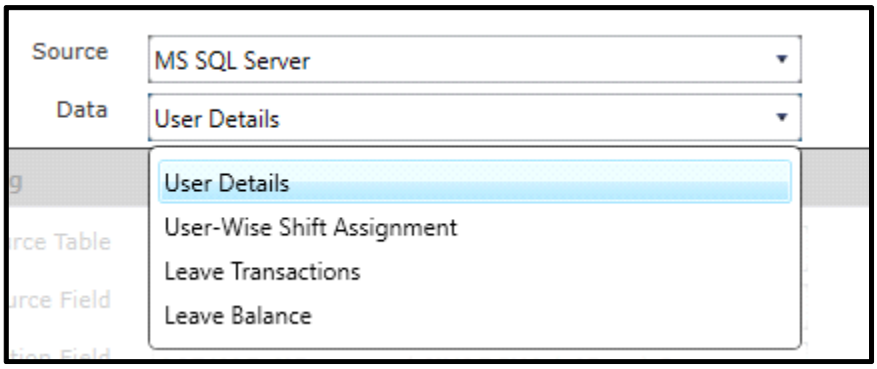
Import Data Configuration

After completing the server configuration, click on **Import Data** button. The page appears as shown below.



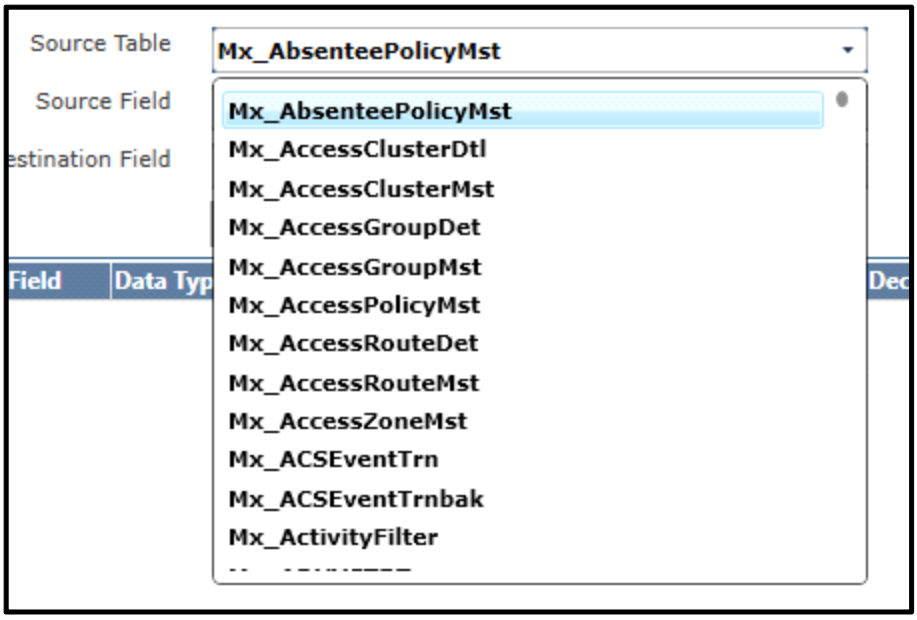
Source: If import from SQL server is to be done then the source will be MS SQL Server. If import from Oracle is to done then the source will be Oracle.

Data: You can select the option as User Details to import the details of user, User-Wise Shift Assignment to import the shifts assigned to user on specific dates, Leave Transactions to import leave transactions and Leave Balance to import the available leave balance.



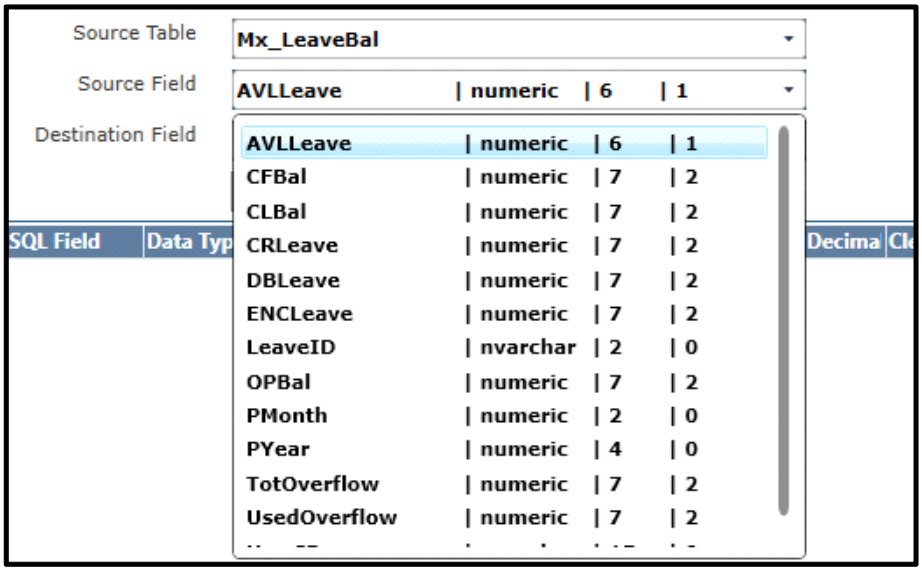
Now click on the **Edit** button. The Admin user can start mapping of the fields from the external source database table to that of the destination COSEC database table as shown.

- Select the **Source Table** whose fields are to be mapped.

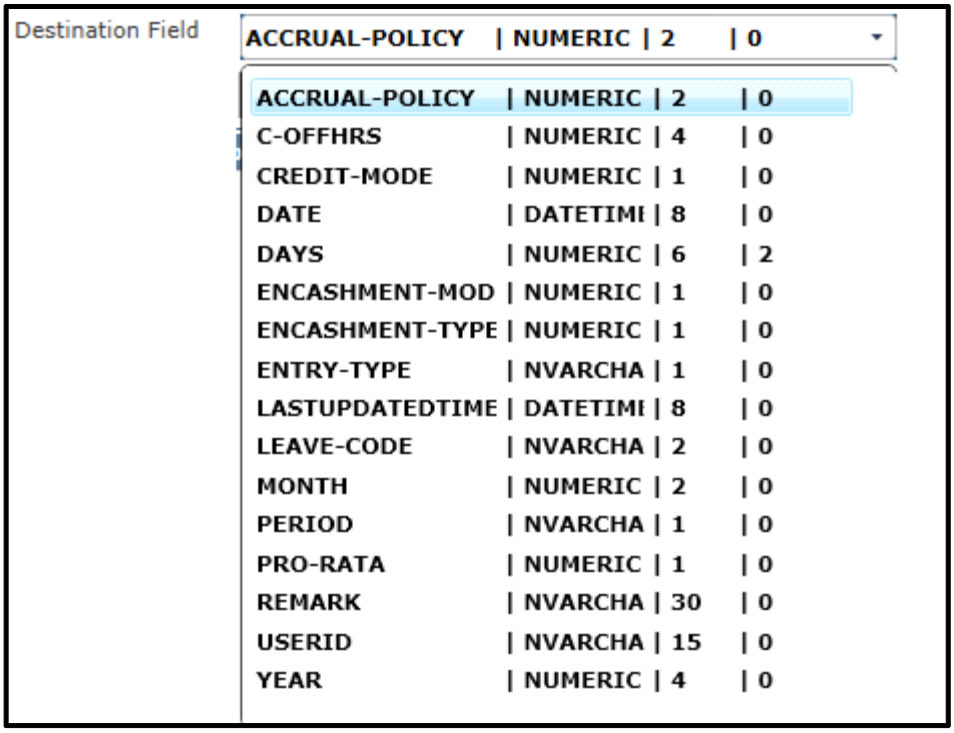


- Select the **Source field** from the COSEC database.Source field is dependent on the Source selected from the Source Table.

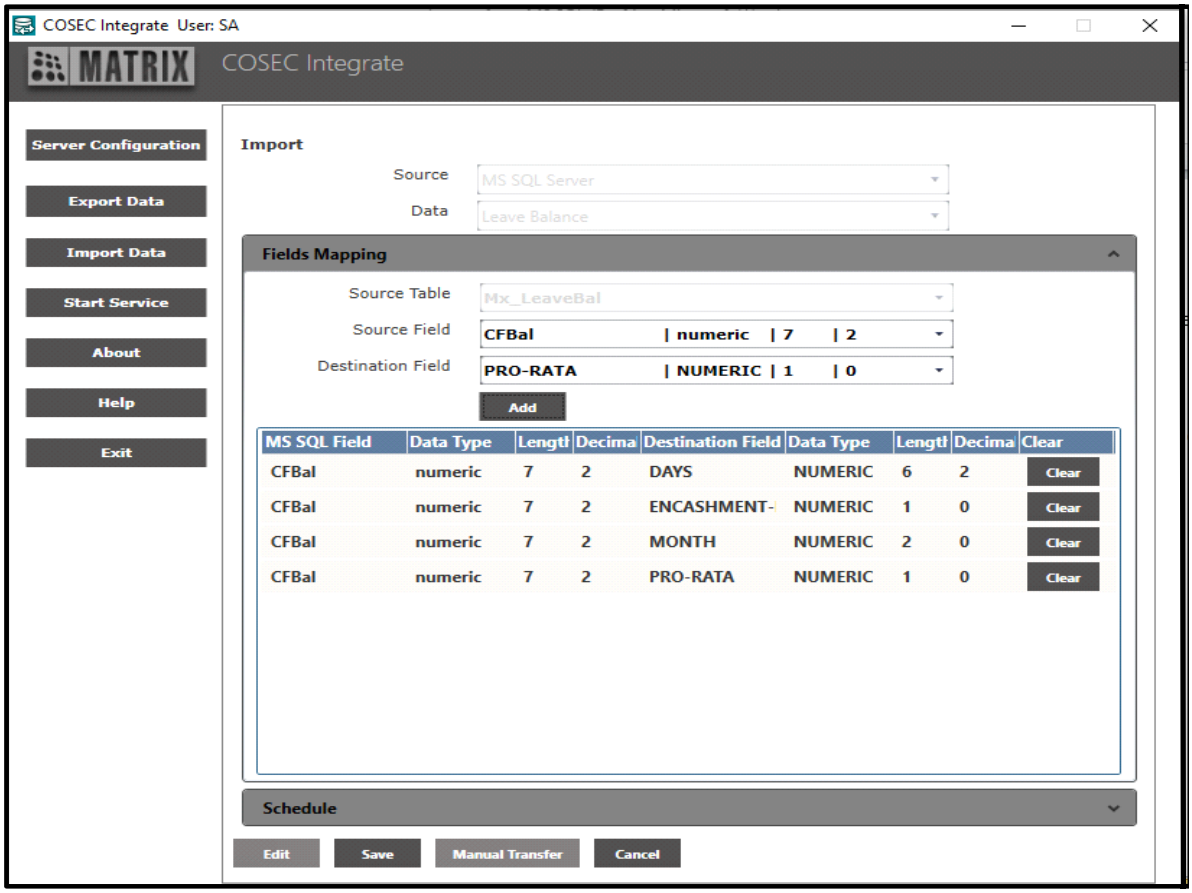
  E.g: If Mx_LeaveBal is selected as source from the Source table then the Source field will show all the fields related to leave balance as shown below.



- Select the **Destination** field from the drop down options to map with the source field. Destination field will always be fixed. It is dependent neither on Source table nor on Source field.



- Click on the **Add** button. The mapped fields will be visible in the bottom grid as shown.

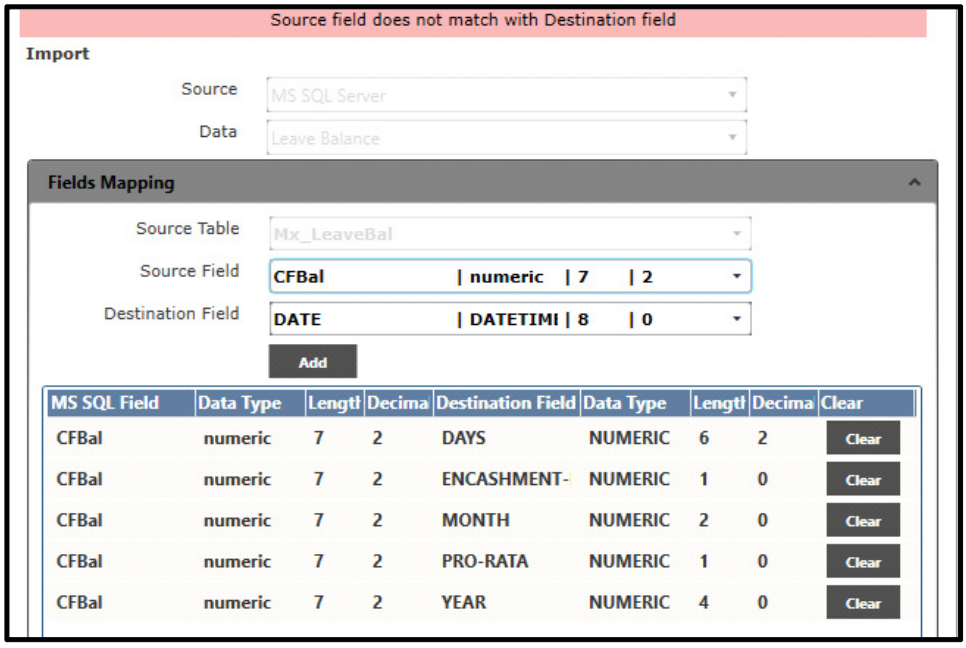


The mapping between the following data types is allowed. Only a warning message is shown in case of mismatch in data types.

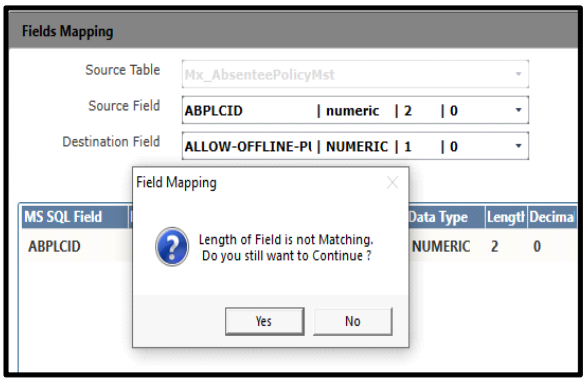
Source data type	Destination data type
Text(char, varchar,varchar2...)	Number (numeric, int, bigint, smallint, float, number, double,int32...)
Text	Datetime formats(depending on the date format configured for DB server. If format matches, the record will be accepted)
Number	Text
Date Time	Text

The mapping from Number and Date time to Date time and Number respectively is restricted.

Source field's data type must always match with the Destination field's data type. In case of mismatch, a warning is generated as shown below and mapping will not be done.



In case of mismatch of lengths of data types of source field and destination field, a warning is generated but if you click on ***Yes,*** *mapping will be done.*



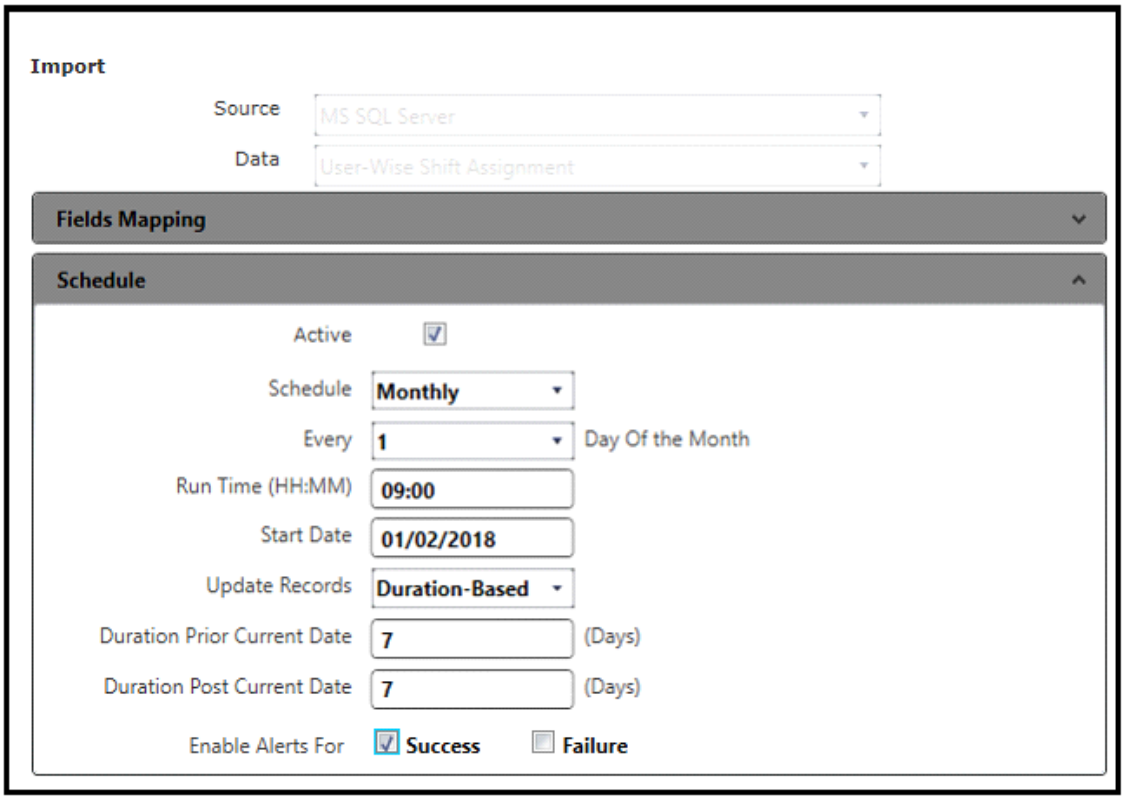
*In the case of selecting data as **User details**, the user needs to map the UserID, Name and BLNUPDATEFIELD/LASTUPDATEDTIME destination fields to fields in the source table.*

*In the case of selecting Data as **User-Wise Shift Assignment,** the user needs to map UserID, Shift-ID, StartDate and EndDate destination fields to fields in the source table.*

*In the case of selecting Data as **Leave Transaction**, the user needs to map UserID, StartDate, Leave-Code and LASTUPDATEDTIME destination fields to fields in the source table.*

*In the case of selecting Data as **Leave Balance**, the user needs to map UserID, Entry-Type, Days, Accrual-Policy, Leave-Code, Date, C-Offhrs and LASTUPDATEDTIME source fields to fields in the destination table.*

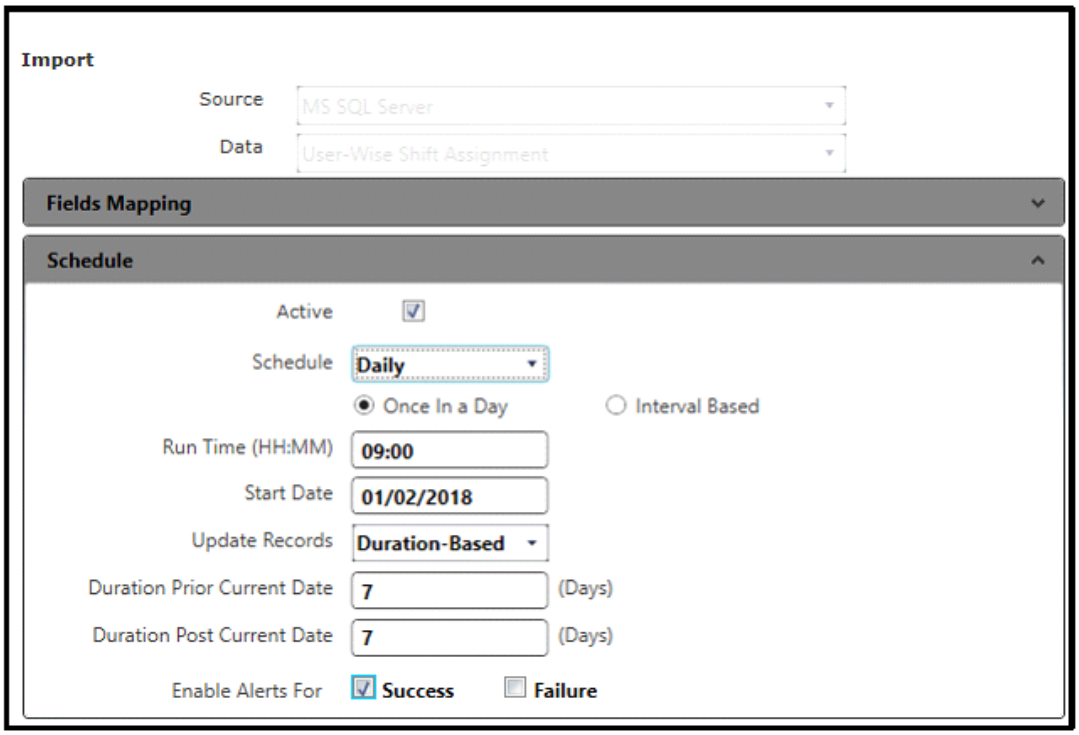
The **Schedule** section enables the Admin user to schedule the data import process. After saving the data you can manually transfer the data.



Check the **Active** box to enable the schedule.

Select the **Schedule** for data transfer as **Daily** or **Monthly**.

- On selection of **Monthly** option, user can select the day for data transfer process to run once in a month. By default, **Monthly** option would be selected.
- On selection of **Daily** option, you can run the schedule “once in a day” or “Interval based”. Enter the value in minutes or hours for interval based schedule.



- Specify the **Run time** in HH:MM format when the import process is to be run.
- Enter the **Start date** from which import process is to be started.
- **Update Records**: You can select the option as **Duration- Based** or **Differential** based on which records is to be updated.

Duration-Based

- **Duration Prior Current Date (Days):** Enter the no. of days to be considered for import before current date. Suppose Current date or the process date is 20th, and duration prior is set as 5 so the import will run from 15th.
- **Duration Post Current Date (Days):** Enter the no. of days to be considered for import after current date. Suppose Current date or the process date is 20th, and duration post is set as 8 so the import will run upto 28th.

Differential

If Update Records is switched from Duration-Based to Differential, a pop-up (with close icon and OK button) will be displayed with the message: All Records will be imported for First Time. Thereafter, only updated ones will be imported.

- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

  Select the checkboxes as per your requirement:

  Select **Success** checkbox to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

Select **Failure** checkbox to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

If you require Alerts for both the above events, select both the check boxes.

In case of partial data transfer i.e. if both the above checkboxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

Example: There are in total 100 records which are to be transferred.

Now, out of 100 records, only 60 records are transferred Successfully and the remaining 40 records have Failed. Such data transfers are known as partial data transfers.

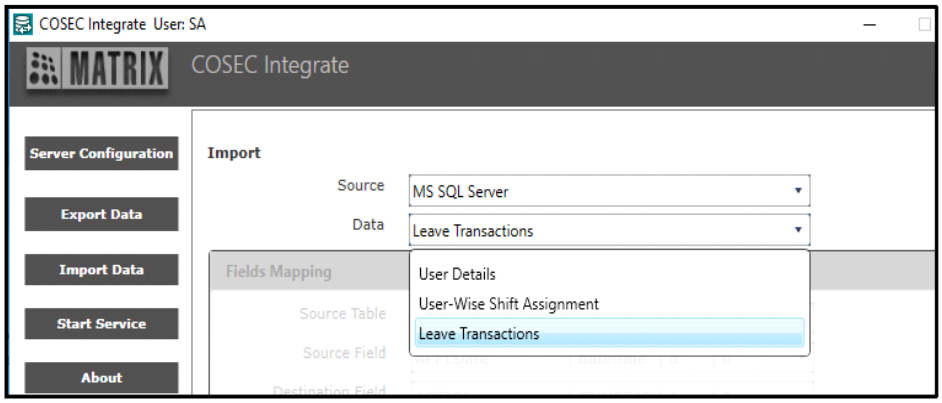
So here the connection status will be Failure and an alert will be sent to the configured COSEC Server along with the reason for failed data transfer.

It is to be supported for all integrate modes defined in COSEC Integrate where enable alerts provision is present i.e. for all the integration modes except for Custom Export-FP Template & Export FP Template to File.

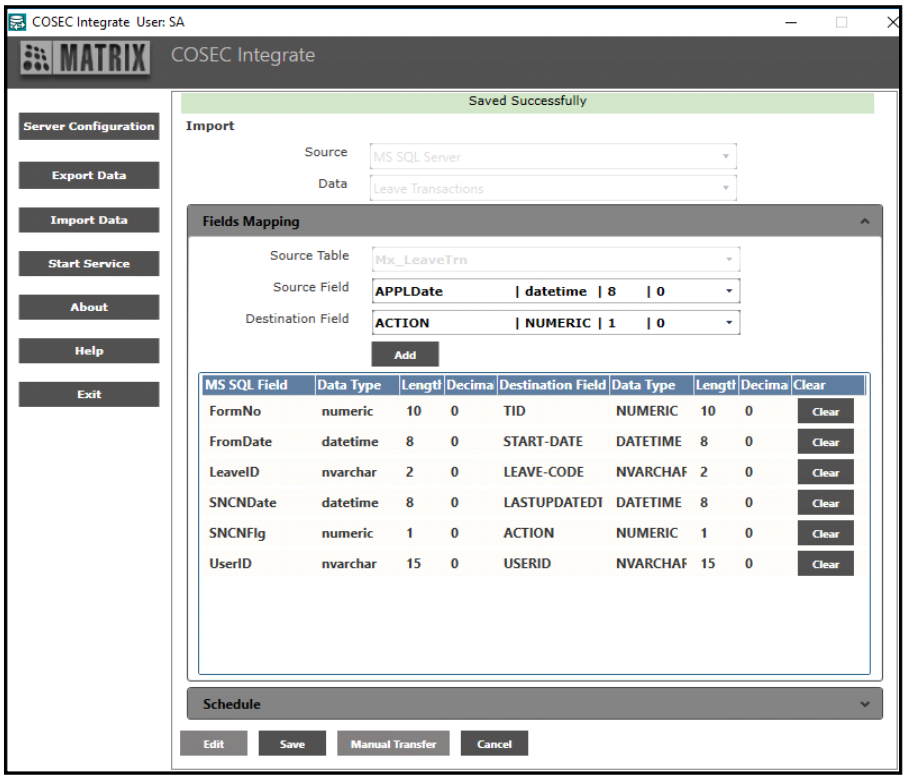
Import Leave Transactions

When leave data is in Human Resource software and T&A calculations are done by COSEC; then it is must to import leave data from Human Resource software to COSEC to perform calculations of T&A management.

The leave transactions can be imported from MS SQL database, Oracle database or Excel file via Integrate. Select the **Data** as Leave Transactions.

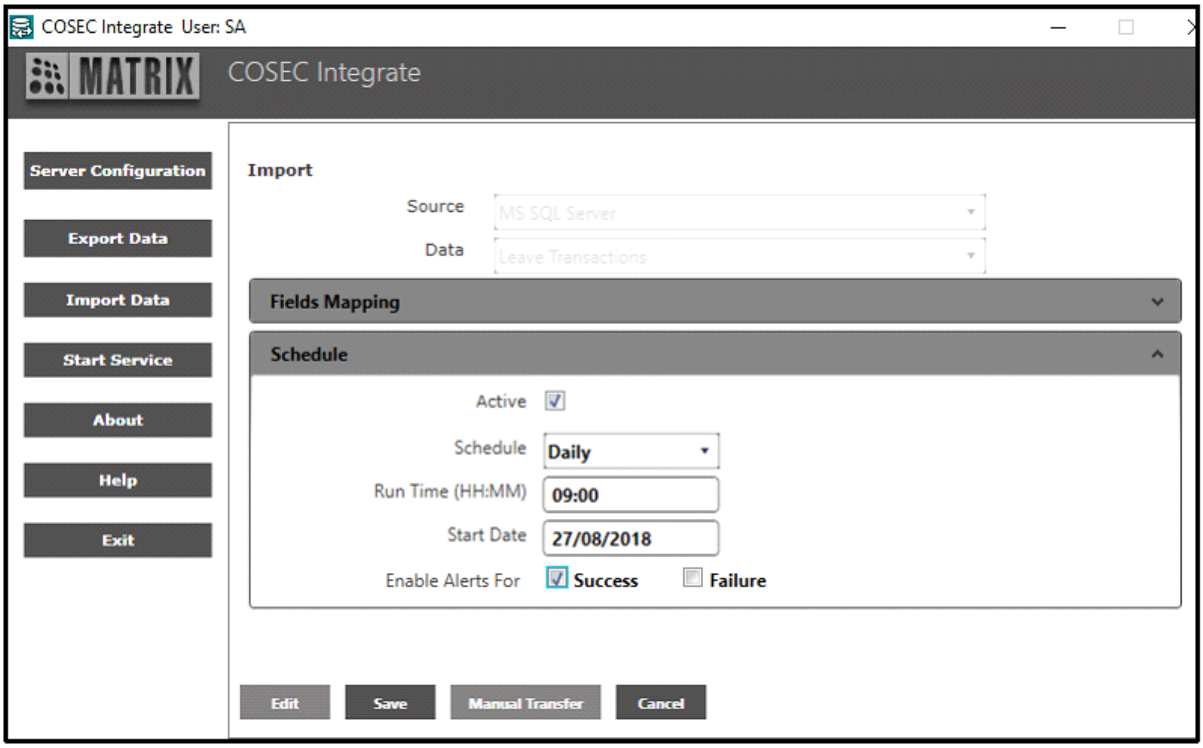


Then map the source and destination fields

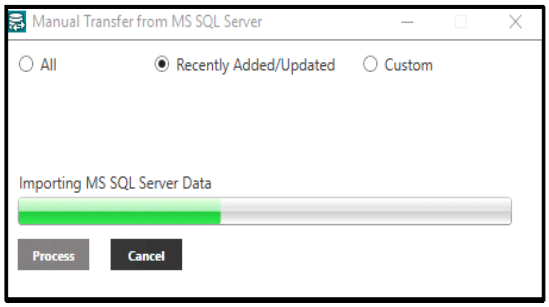


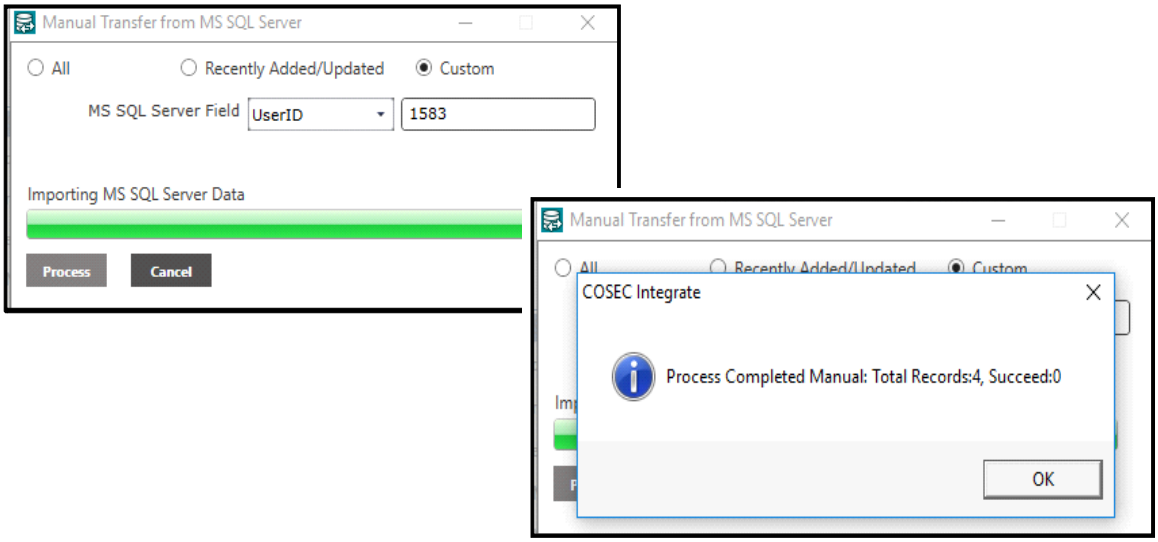
The fields USERID,START-DATE, LEAVE-CODE and LASTUPDATEDTIMESTAMP are mandatory for mapping. If TID is mapped; then ACTION is required to be mapped for importing based on TID.

After mapping, click on Save button.



The import can be scheduled or manual transfer can be done.





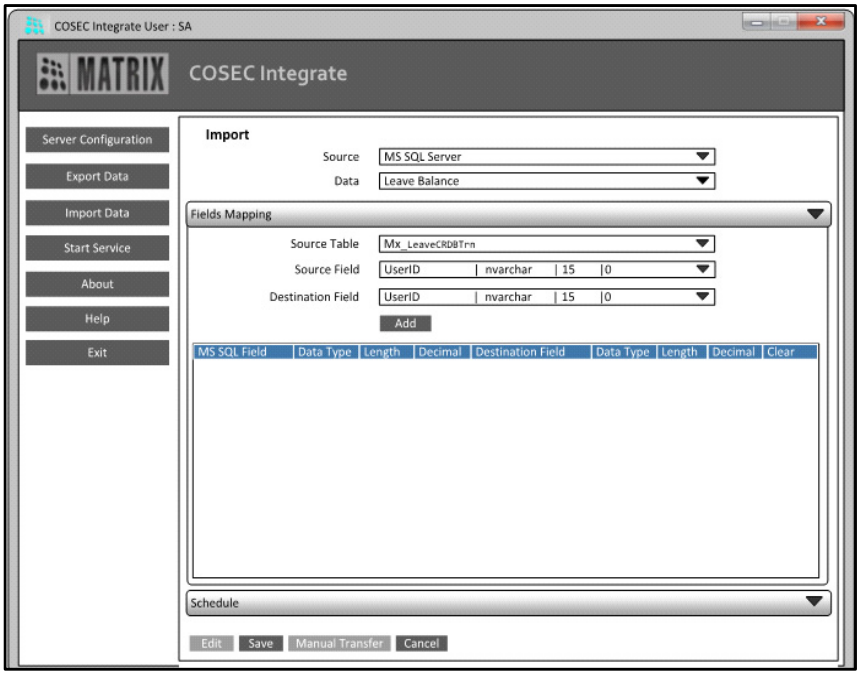
Client database should have a field containing primary key.

Import Leave Balance

Import Leave Balance allows user to perform **Leave Encashment** as the 'Credit/Debit', 'C-OFF Encashment' and 'Overflow Management' of the leave records. It can be done through the Import as shown below.

The Import can be done through the sources; **MS SQL/Oracle**, **Excel**, **Progress Open Edge**, **Postgre**, **Customized SAP** and **My SQL**. Select the respective source, the Data as Leave balance and configure the rest parameters the same way as described in Import Leave Transaction.

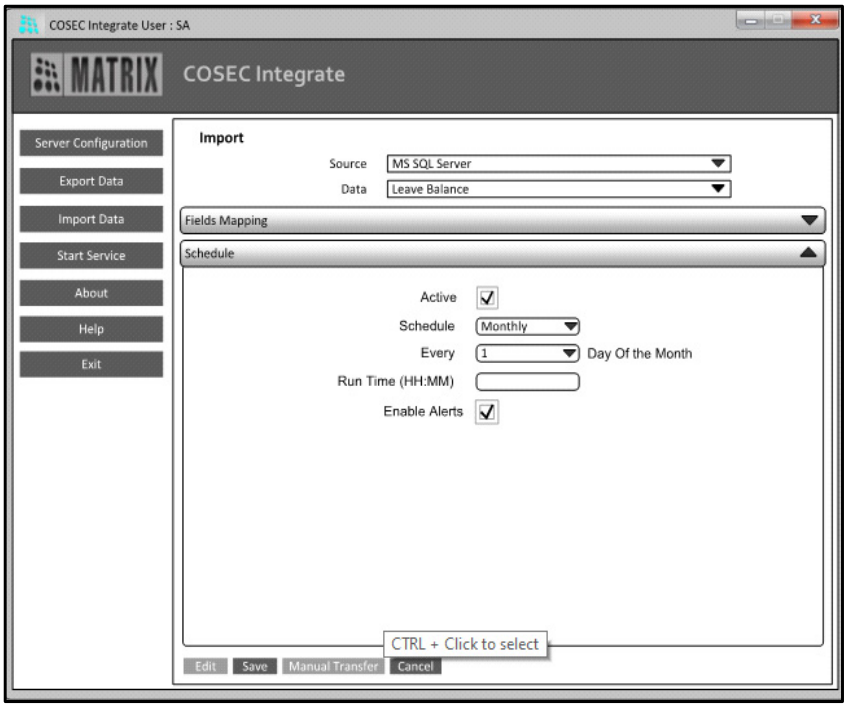
Map the source and destination fields from Fields Mapping.



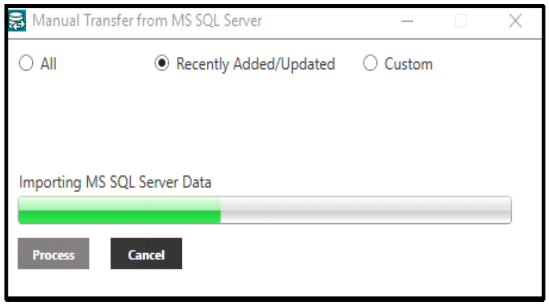
Map the source and destination fields from Fields Mapping.

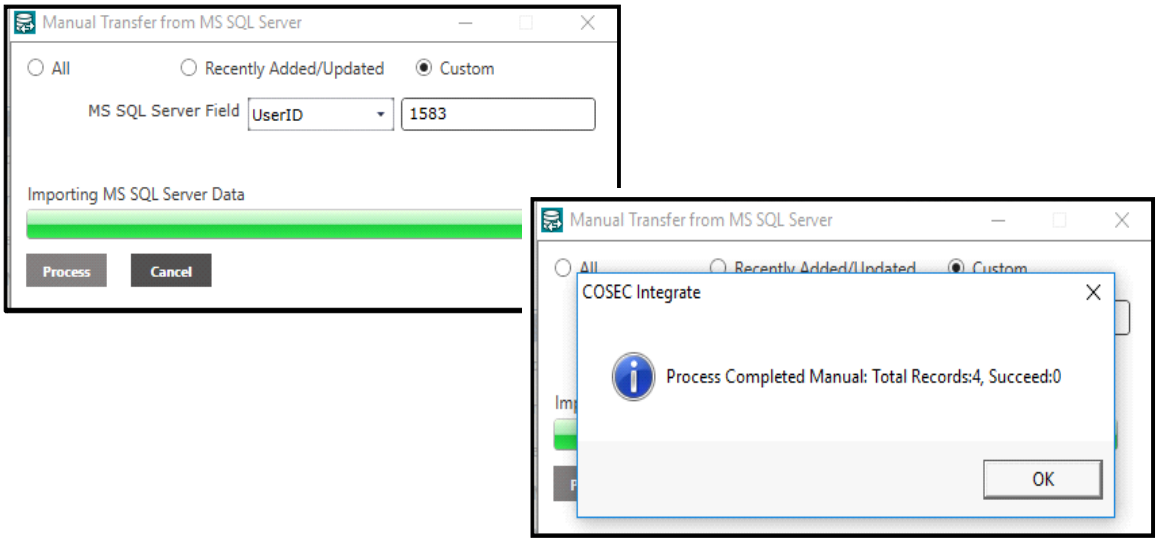
The fields USERID,START-DATE, LEAVE-CODE and LASTUPDATEDTIMESTAMP are mandatory for mapping. If TID is mapped; then ACTION is required to be mapped for importing based on TID.

After mapping, click on Save button.



The import can be scheduled or manual transfer can be done.





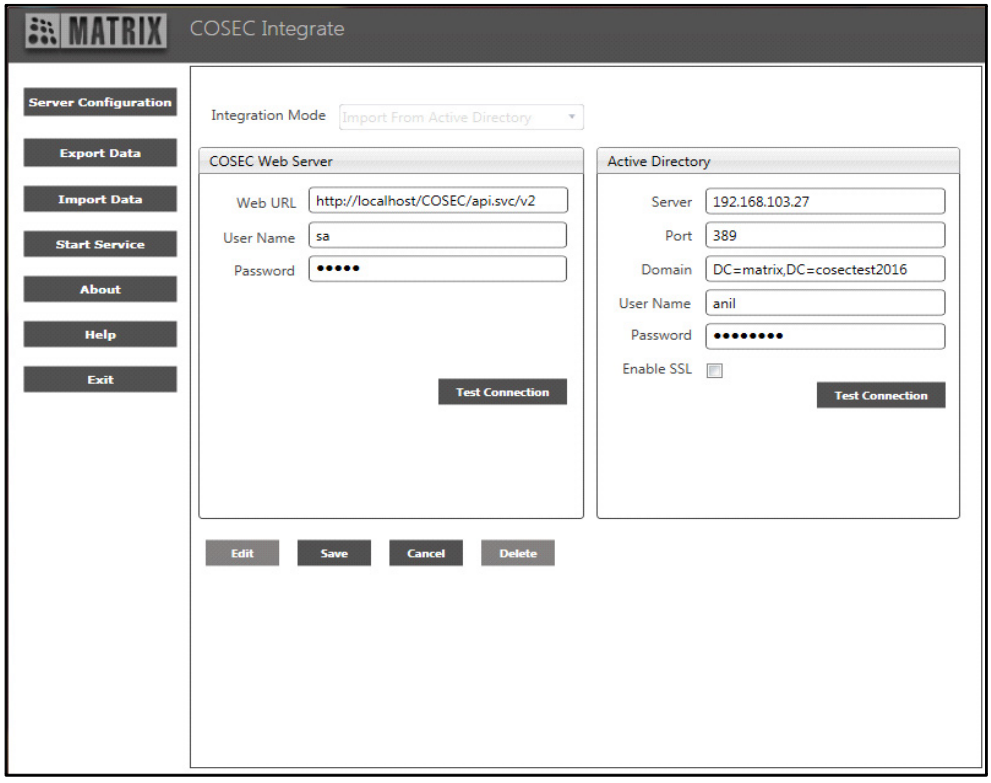
The Import with the other sources are explained in further examples.

Import from Active Directory

The COSEC INTEGRATE application provides the functionality to import user data from the Active Directory service of Windows.

The application allows the administrator to map the data fields of the COSEC application database to the data fields of the active directory.

Now user can click on the **Server Configuration** button to start the configuring process. The following page appears. Select the **Import from Active Directory** option in the **Integration Mode** field.



In the **COSEC Web Server** section:

- Specify the web url of the api service of the COSEC WEB application as shown.
- Enter the User Name and Password of the sa user as set in the COSEC WEB application.

In the **Active Directory** section:

- Specify the IP address or the network name of the Domain Controller.
- **Port**: Enter the port no. if configured.
- **Domain Name**: Specify the domain name as shown. For e.g. if the domain name is matrix.com the domain name is specified as: **dc=matrix,dc=com**.
- **User Name**: Specify the username having administrator rights in this field. e.g. **matrix\administrator**.
- **Password**: Enter the password of the administrator as per the site settings.
- **Enable SSL**: To establish secured connection and protecting Data, click on check-box given next to **Enable SSL**. It is compulsory to enable this check-box.

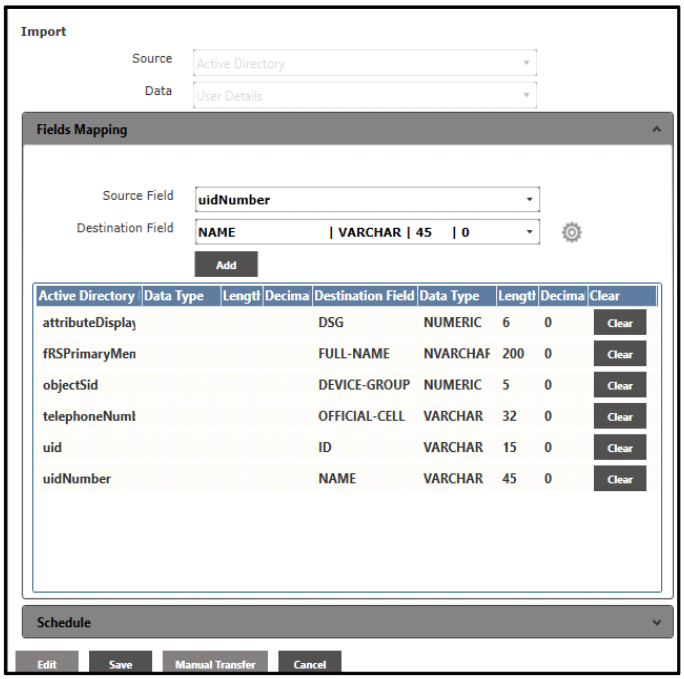
The **Test Connection** button is provided to test the connections with the web server as well as the Active Directory service.

Click on **Save** once done.

Active Directory Import Configuration

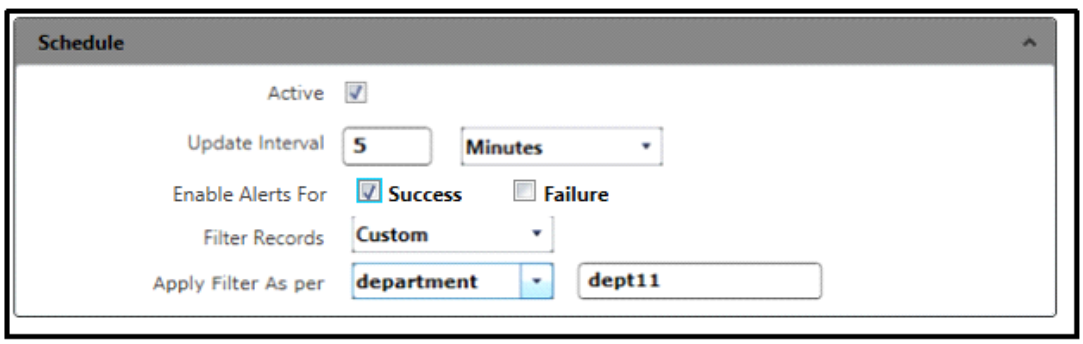
This option enables the Admin user to map the fields from the Active Directory service to the appropriate fields in the COSEC database. The application will list all the fields in the COSEC database which are relevant to the User Configuration. The administrator needs to select the relevant fields in the Active Directory and then map the same to the relevant fields of the COSEC database.

Click on the **Import Data** button. The following page appears.



- Select **Active Directory** from the **Source** drop down list.
- Click on **Edit**.
- In the **Fields Mapping** section, select the **Source Field** and **Destination Field** from the respective drop down lists.

Click on the **Add** button. The mapped fields will be visible in the bottom grid as shown. The schedule section enables the administrator to set the frequency at which the COSEC service will check the active directory for updates.



- Check the **Active** box to enable the schedule.

- Specify the **Update Interval** in seconds, minutes or hours to define the frequency at which the application will update the destination COSEC database.

- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

  Select the checkboxes as per your requirement:

  Select **Success** checkbox to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

  Select **Failure** checkbox to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

  If you require Alerts for both the above events, select both the check boxes.

  In case of partial data transfer i.e. if both the above checkboxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

  Example: There are in total 100 records which are to be transferred.

  Now, out of 100 records, only 60 records are transferred Successfully and the remaining 40 records have Failed. Such data transfers are known as partial data transfers.

  So here the connection status will be Failure and an alert will be sent to the configured COSEC Server along with the reason for failed data transfer.

It is to be supported for all integrate modes defined in COSEC Integrate where enable alerts provision is present i.e. for all the integration modes except for Custom Export-FP Template & Export FP Template to File.

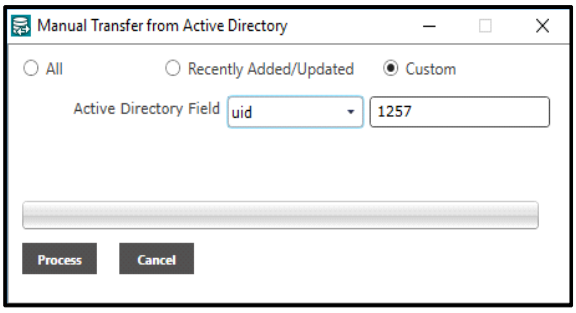
- **Filter Records:** You can filter the records that are to be imported at scheduled runtime by selecting All or Custom option.
  - If **Custom** option is selected then select the option for "**Apply Filter As Per"** and enter the respective value in the text box.

Click on **Save** once done.

Manual Transfer

The manual transfer option provides the admin user the flexibility to import user data from the active directory database as and when required. In order to access this functionality click on the **Stop service** button to stop the COSEC INTEGRATE service.

Click on the **Active Directory** button followed by the **Manual Transfer** button. The following window appears.



Select from one of the following options.

- **All** - Imports all users from the active directory database.
- **Recently Added/Updated** - Imports only those users whose records have been updated after the last import.
- **Custom** - Imports users as per the defined filter.

Click on the **Process** button. The application will import data of the users as per the specified filter and displays the status of the import process as shown.

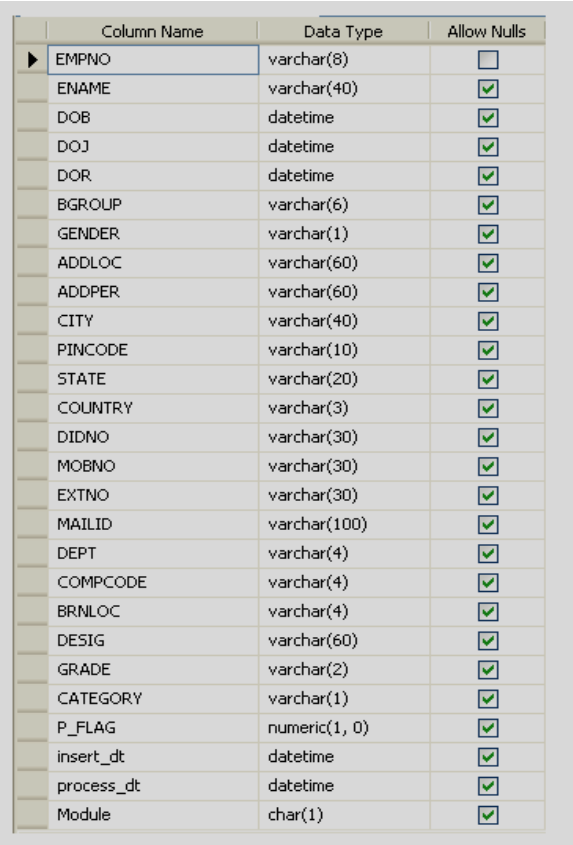
Click on **OK** to close the window.

Importing Data from a Customized SAP

The application allows the user to import user data from a customized external MS SQL or Oracle database table.

Integrate supports Import from Oracle upto version Oracle 23AI and Import from MS SQL upto version MS SQL 16.0.1000.6.

The following figure depicts a sample of the source table structure.

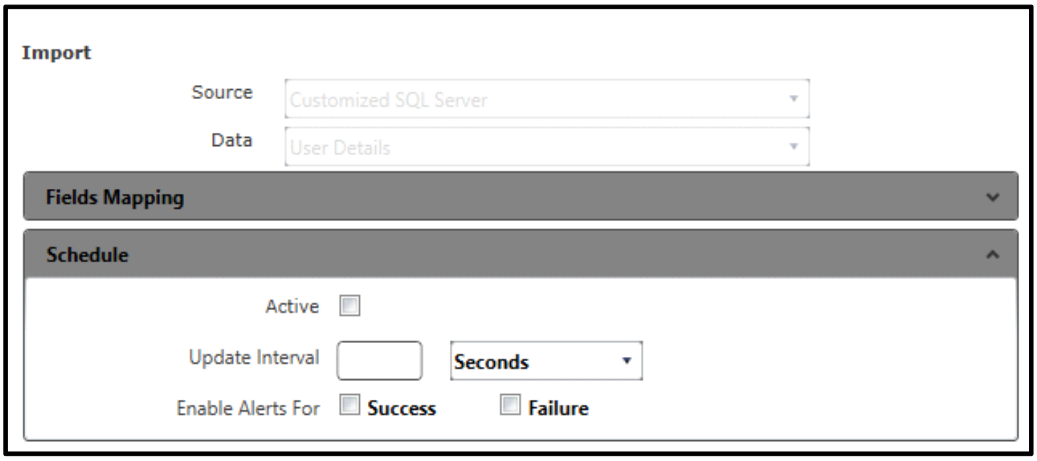


Column Name	Data Type	Allow Nulls
EMPNO	varchar(8)	☐
ENAME	varchar(40)	☑
DOB	datetime	☑
DOJ	datetime	☑
DOR	datetime	☑
BGROUP	varchar(6)	☑
GENDER	varchar(1)	☑
ADDLOC	varchar(60)	☑
ADDPER	varchar(60)	☑
CITY	varchar(40)	☑
PINCODE	varchar(10)	☑
STATE	varchar(20)	☑
COUNTRY	varchar(3)	☑
DIDNO	varchar(30)	☑
MOBNO	varchar(30)	☑
EXTNO	varchar(30)	☑
MAILID	varchar(100)	☑
DEPT	varchar(4)	☑
COMPCODE	varchar(4)	☑
BRNLOC	varchar(4)	☑
DESIG	varchar(60)	☑
GRADE	varchar(2)	☑
CATEGORY	varchar(1)	☑
P_FLAG	numeric(1, 0)	☑
insert_dt	datetime	☑
process_dt	datetime	☑
Module	char(1)	☑

The user can map the required fields as explained earlier. In this case too, the following destination fields need to be compulsorily mapped with appropriate fields of the source table as shown.

- id
- name
- BLNUPDATEFIELD

The import data options have the following **Schedule** options.



- Check the Active box to enable the schedule.
- Specify the **Update Interval** in seconds, minutes or hours to define the frequency at which the application will import the data from the source table.
- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

  Select the checkboxes as per your requirement:

  Select **Success** checkbox to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

  Select **Failure** checkbox to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

  If you require Alerts for both the above events, select both the check boxes.

  In case of partial data transfer i.e. if both the above checkboxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

  Example: There are in total 100 records which are to be transferred.

  Now, out of 100 records, only 60 records are transferred Successfully and the remaining 40 records have Failed. Such data transfers are known as partial data transfers.

  So here the connection status will be Failure and an alert will be sent to the configured COSEC Server along with the reason for failed data transfer.

It is to be supported for all integrate modes defined in COSEC Integrate where enable alerts provision is present i.e. for all the integration modes except for Custom Export-FP Template & Export FP Template to File.

Click on **Save** once done.

Import Events

The COSEC INTEGRATE application provides the functionality to import event data from 3rd party database i.e. MS SQL and Oracle as well as from Excel.

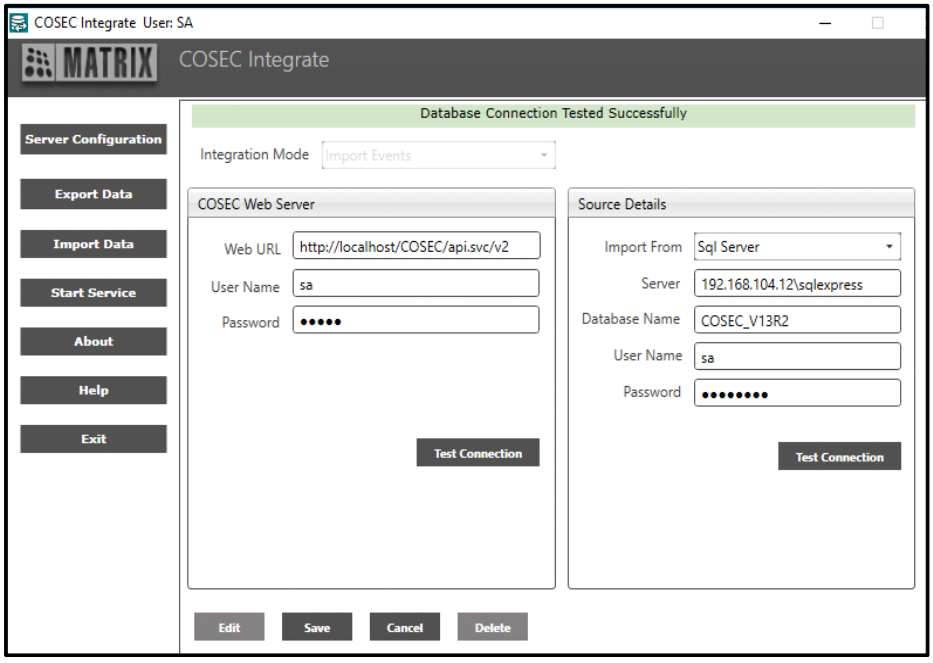
Integrate supports Import from Oracle from version Oracle 10g to Oracle 23AI.

Integrate supports Import from MS SQL from version SQL Server 2005 to SQL Server 2022.

SQL Server 2005 and SQL Server 2008 R2:

- *for installation you need Windows 7 or below versions.*
- *to establish remote connections in these versions from the PC in which Integrate is installed, make sure you have enabled TLS 1.0 and 1.1 (that is, Best Practices settings).*

Now user can click on the **Server Configuration** button to start the configuring process. The following page appears. Select the **Import Events** option in the **Integration Mode** field.



In the **COSEC Web Server** section:

- Specify the web URL of the api service of the COSEC WEB application as shown.
- Enter the User Name and Password of the SA user as set in the COSEC WEB application.

In the **Source Details** section:

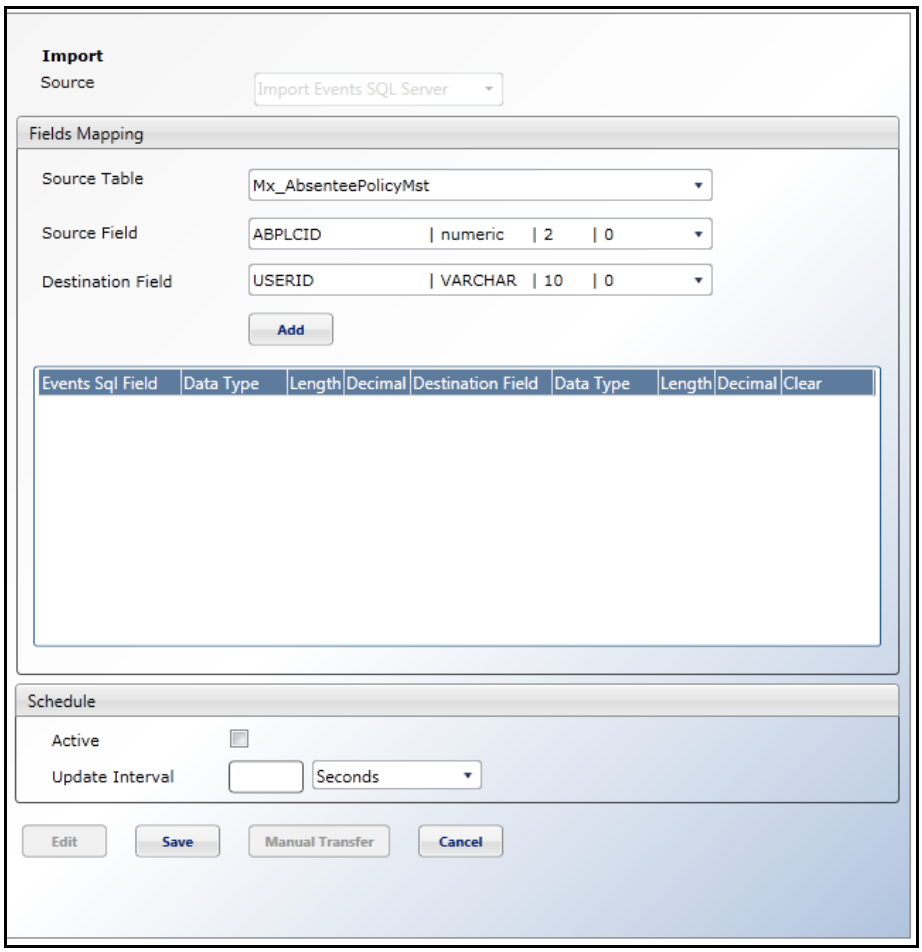
- Select the **Import From** option as SQL SERVER, ORACLE SERVER or EXCEL.
- **Server**: Enter the database server name in the following format - **Database server name\Instance Name** e.g. dbserver\sqlexpress.
- **Database Name**: Specify the database name of the source database as per the site settings.

- **User Name**: Specify the database administrator ID in this field.
- **Password**: Enter the password of the Database administrator as per the site settings.

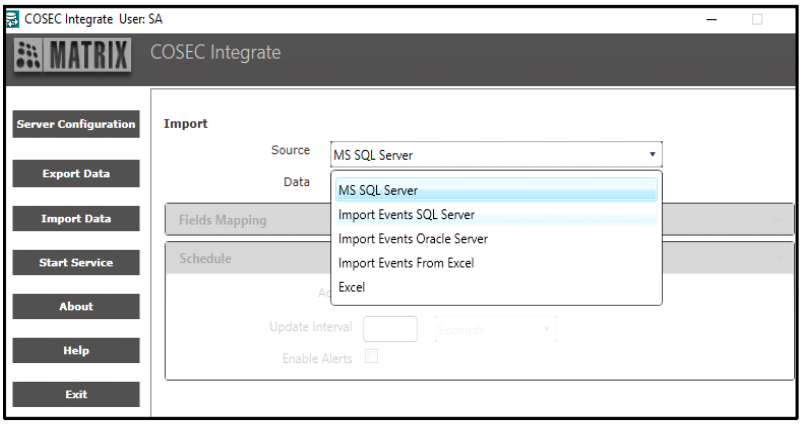
The **Test Connection** button is provided to test the connections with the web server as well as the MS SQL or Oracle Server database.

Click on **Save** once done.

Now click on **Import Data** button.The following page appears.This option enables the Admin user to select the external source database from where the data is to be imported in the destination COSEC table.



Select the source table from the drop down list. The system will get the details of the fields from the source table and display the same in the **Source Field** parameter.



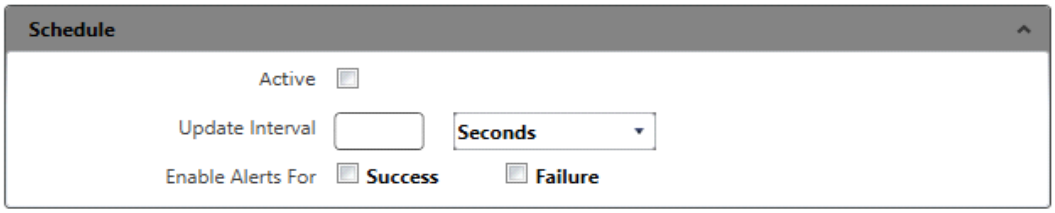
Now the Admin user can start the mapping of the fields from the source database to that of the destination database as shown. Select the appropriate source and the destination fields and click on the **Add** button.

The mapped fields will be visible in the bottom grid as shown. The following destination fields need to be compulsorily mapped with appropriate fields of the source table as shown.

- userid
- event-datetime
- BLNUPDATEFIELD

Click on **Save** button to commit the changes.

The **Schedule** section enables the administrator to set the frequency at which the COSEC service will check the active directory for updates.



- Check the **Active** box to enable the schedule.
- Specify the **Update Interval** in seconds, Minutes or Hours to define the frequency at which the application will update the destination COSEC database.
- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

  Select the checkboxes as per your requirement:

  Select **Success** checkbox to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

  Select **Failure** checkbox to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

  If you require Alerts for both the above events, select both the check boxes.

In case of partial data transfer i.e. if both the above checkboxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

Example: There are in total 100 records which are to be transferred.

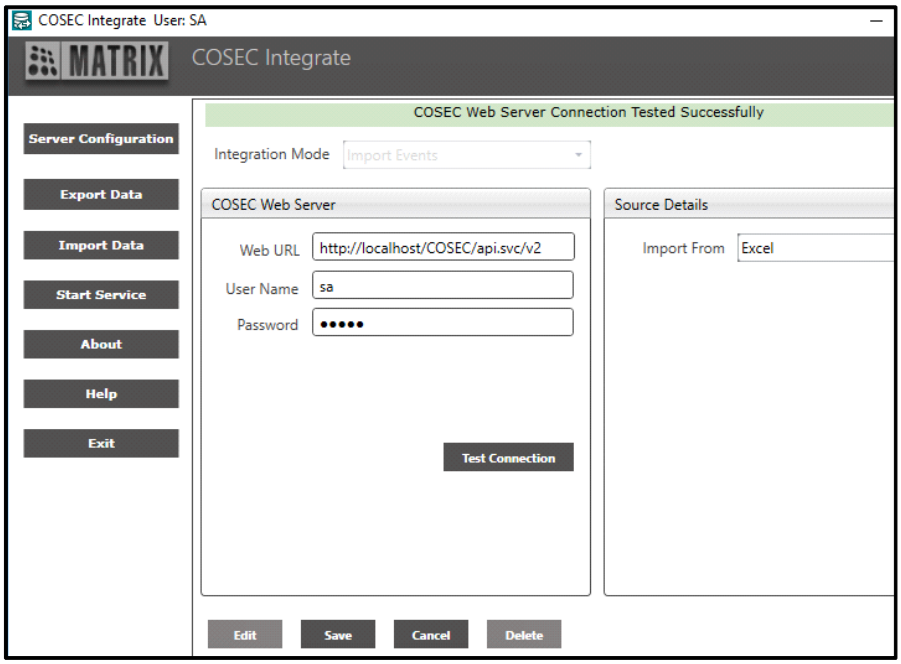
Now, out of 100 records, only 60 records are transferred Successfully and the remaining 40 records have Failed. Such data transfers are known as partial data transfers.

So here the connection status will be Failure and an alert will be sent to the configured COSEC Server along with the reason for failed data transfer.

It is to be supported for all integrate modes defined in COSEC Integrate where enable alerts provision is present i.e. for all the integration modes except for Custom Export-FP Template & Export FP Template to File.

Click on **Save** once done.

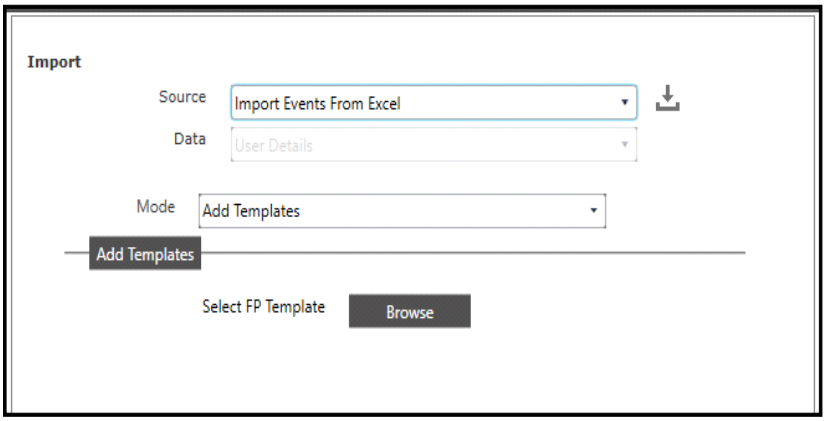
Import Events from Excel



- Select the **Import From** option as Excel.
- Click Test connection button to test the connection with COSEC web server.
- Then click **Save** button.

Import Data

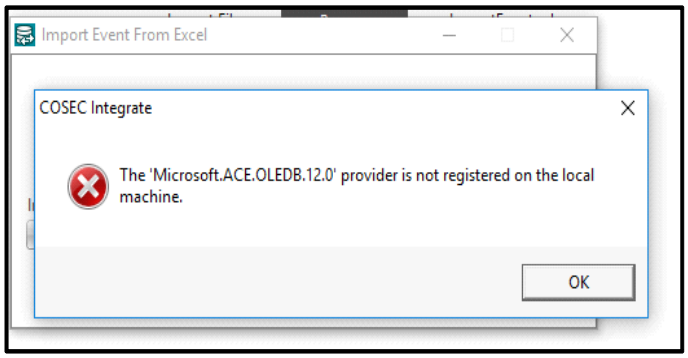
In Import Data page, select the Source as Import Events from Excel.



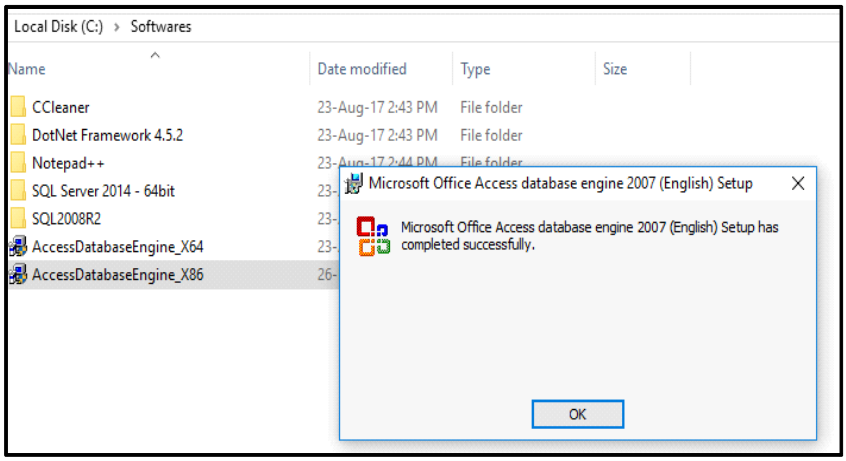
You can click on to import the sample Import Events file. Then save the sample file at desired location.

Click on **Browse** button and select the excel file for importing events. You can import excel file of max 15 MB.

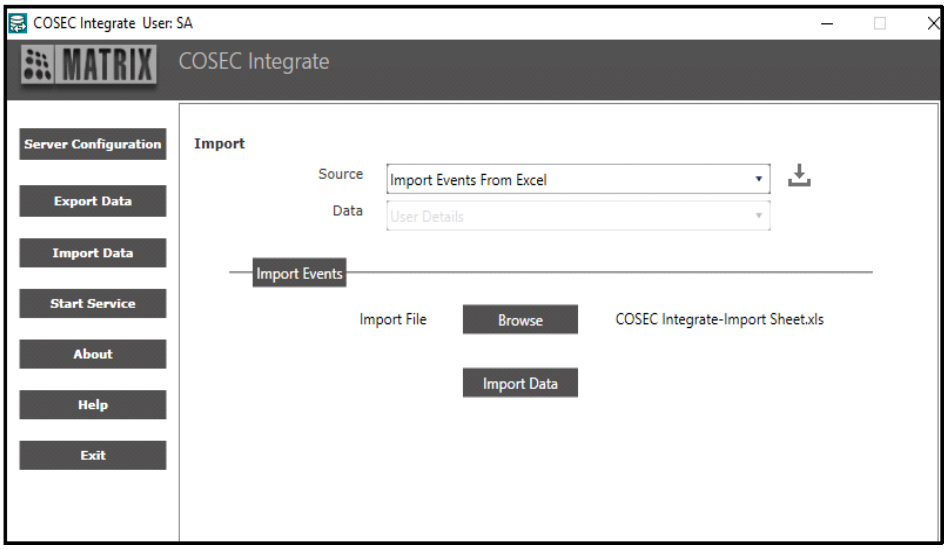
For importing excel file, you must have drivers to import.



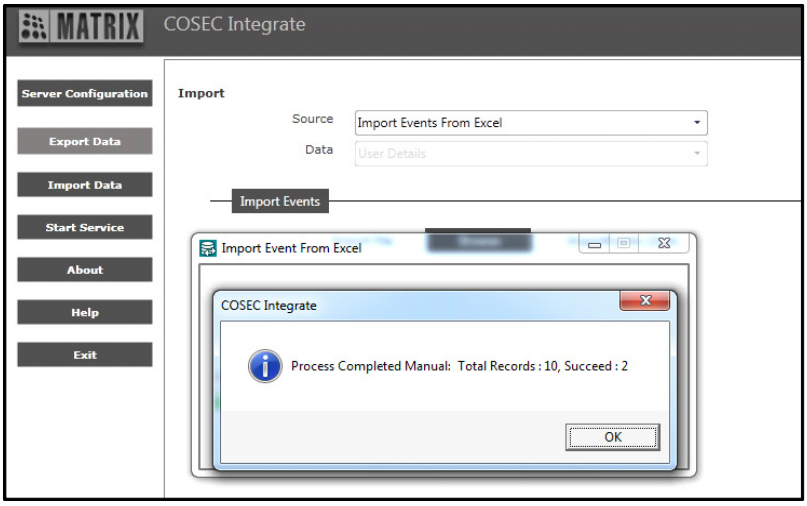
You must install Access Database Engine compatible to your computer as shown below.



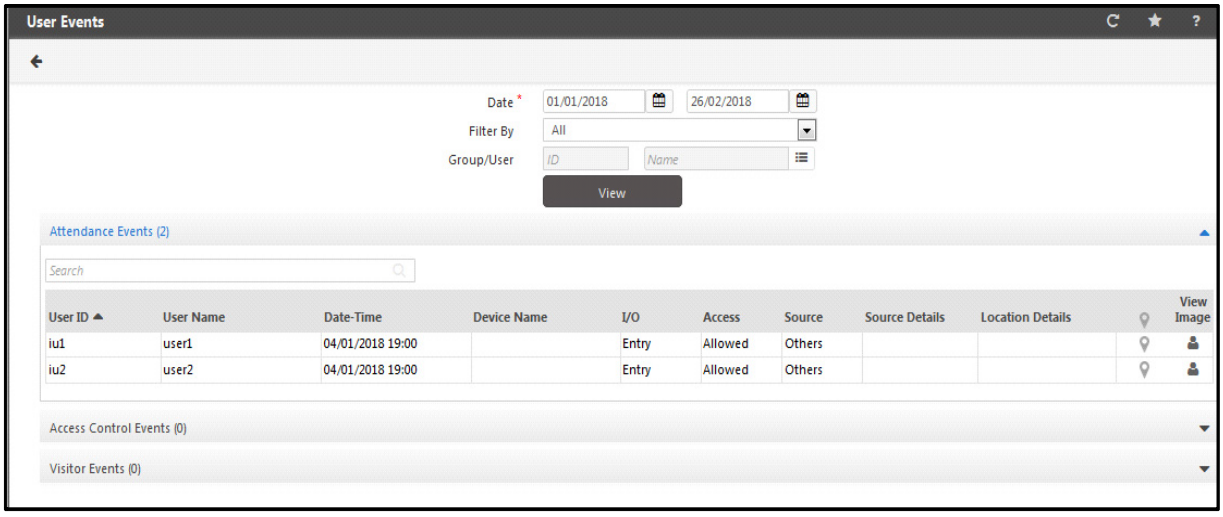
Now the Excel file is selected as shown below.



Then click on **Import Data** button. The import process is shown below.



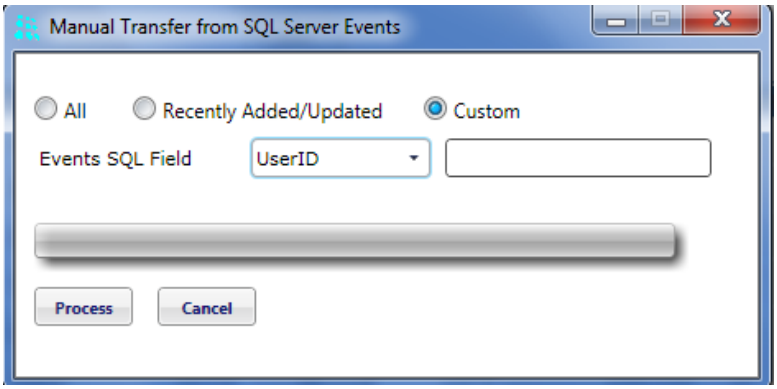
You can view the imported records in User events as shown below.



Manual Transfer

The manual transfer option provides the Admin user the flexibility to import events from the source database as and when required. In order to access this functionality click on the **Stop service** button to stop the COSEC INTEGRATE service.

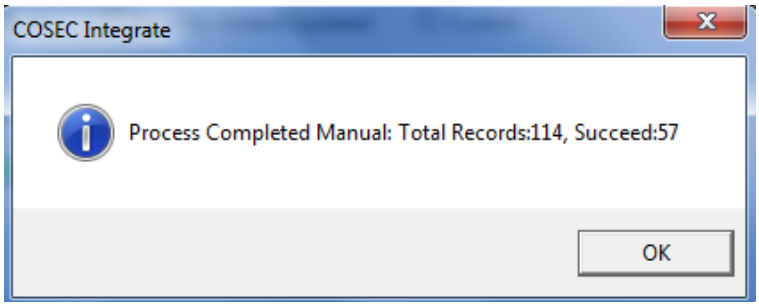
Click on the **Import Data** button followed by the **Manual Transfer** button. The following window appears.



Select from one of the following options.

- **All** - Imports all events from the source database.
- **Recently Added/Updated** - Imports only those events whose records have been updated after the last import.
- **Custom** - Imports events as per the defined filter.

Click on the **Process** button. The application will import data of the users as per the specified filter and displays the status of the import process as shown.

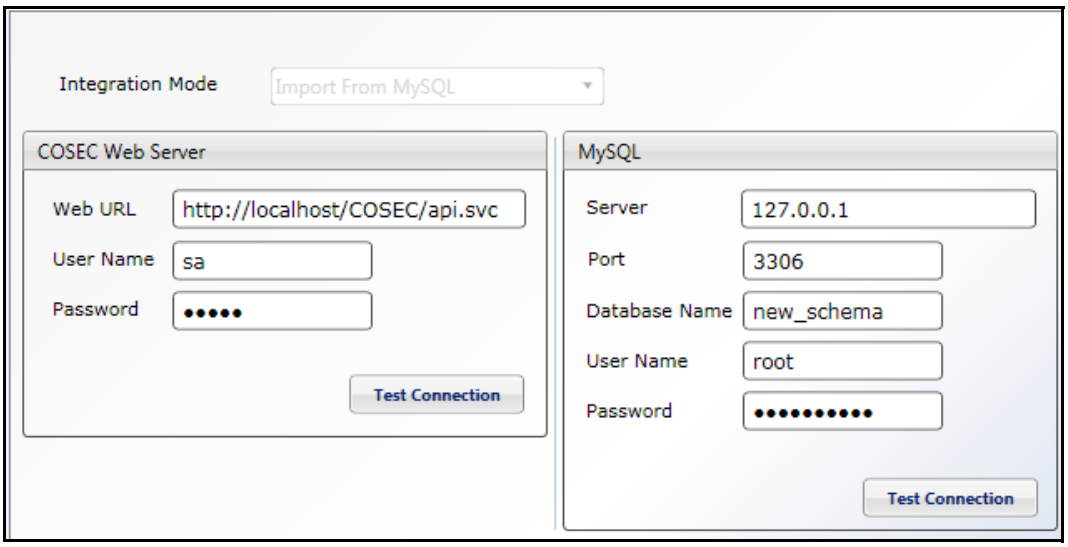


Click on **OK** to close the window.

Import from My SQL

Select the **Import from My SQL Server** option in the **Integration Mode** field. Click on the **Edit** button.

Integrate supports Import from MySQL from version MySQL 8.0.27 to MySQL 8.3.0.



In the **COSEC Web Server** section:

- Specify the web URL of the api service of the COSEC WEB application as shown.
- Enter the User Name and Password of the SA user as set in the COSEC WEB application.

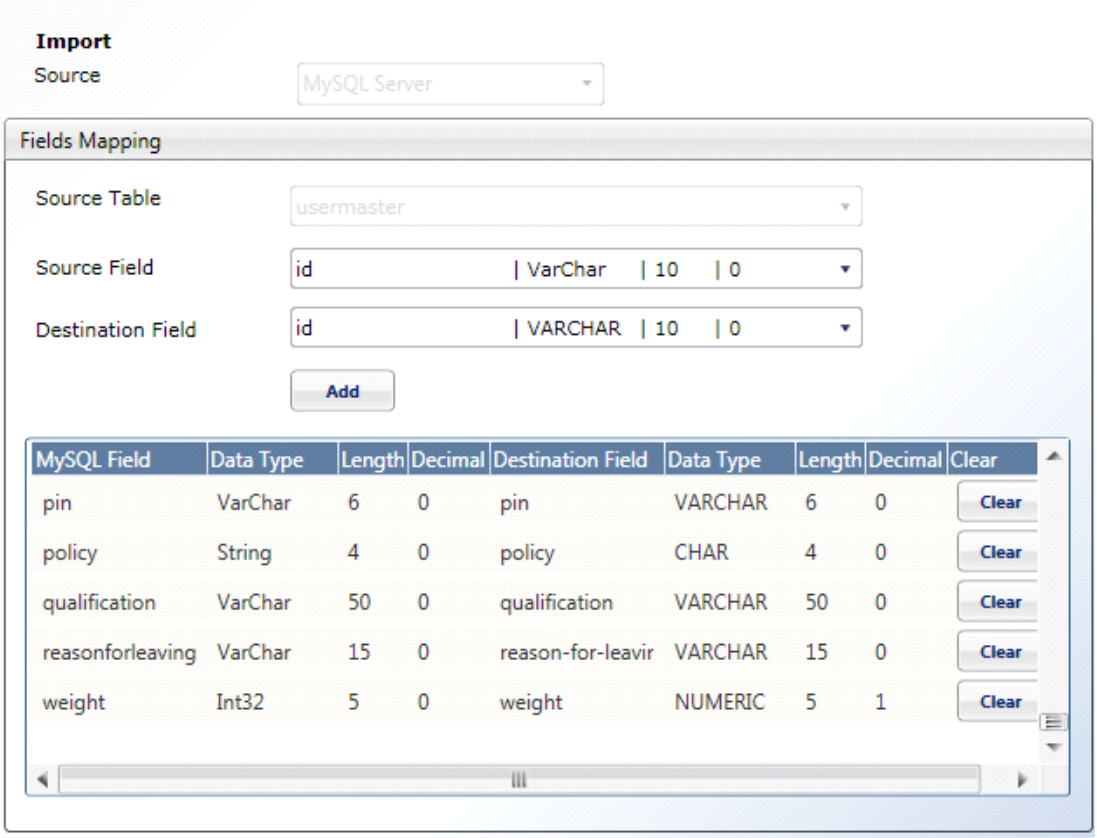
In the **Source Database Server** section:

- The **Database Type** will be SQL SERVER.
- **Server**: Enter the database server name in the following format - **Database server name\Instance Name** e.g. dbserver\sqlexpress.
- **Database Name**: Specify the database name of the source SQL database as per the site settings.
- **User Name**: Specify the database administrator ID in this field.
- **Password**: Enter the password of the Database administrator as per the site settings.

The **Test Connection** button is provided to test the connections with the web server as well as MS SQL.
Click on **Save** once done.

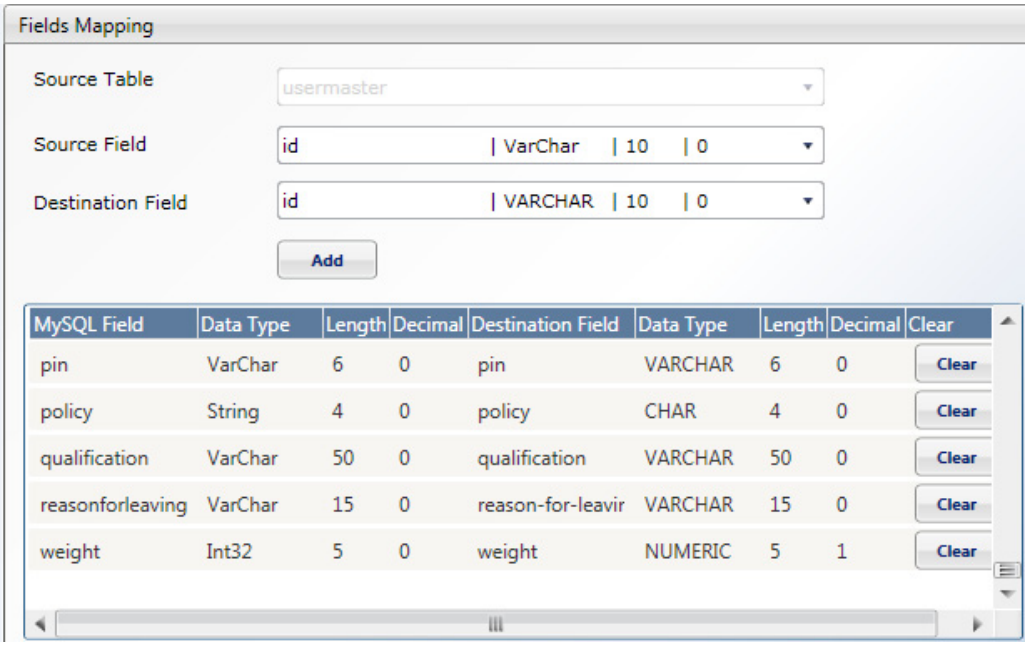
Import Data Configuration

This option enables the Admin user to map the fields from the external source database table to fields in the destination COSEC User table. Click on the **Import Data** button. The following page appears.



Select the source table from the pull down list. The system will get the details of the fields from the source table and display the same in the **Source Field** parameter.

Now the Admin user can start the mapping of the fields from the source database to that of the destination database as shown. Select the appropriate source and the destination fields and click on the **Add** button.



The mapped fields will be visible in the bottom grid as shown. The following destination fields need to be compulsorily mapped with appropriate fields of the source table as shown.

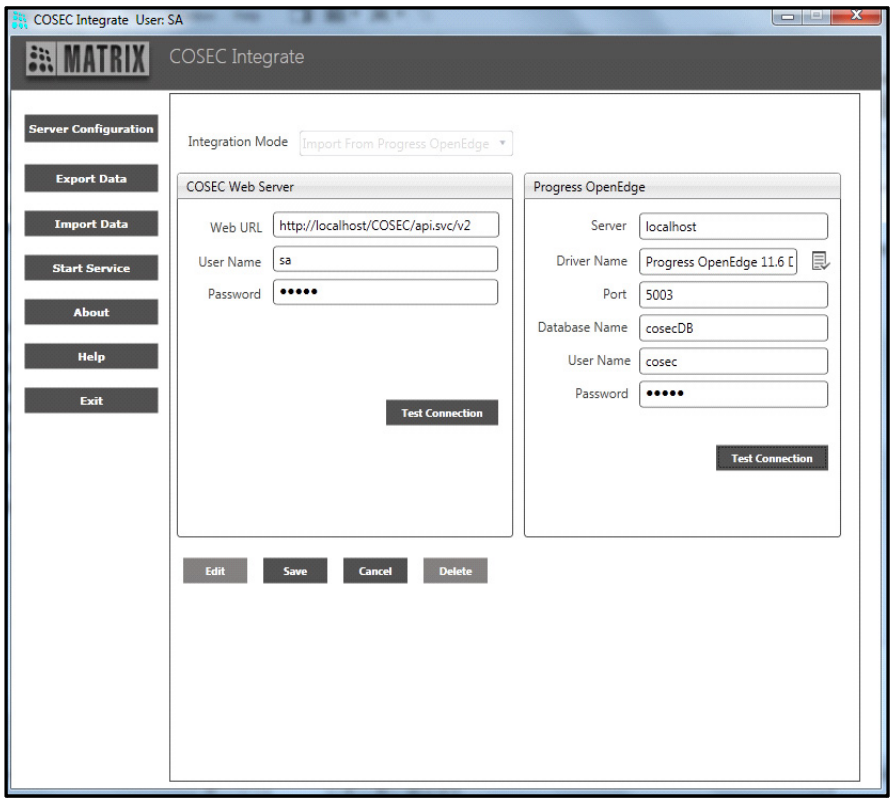
- id
- name
- BLNUPDATEFIELD

This is common to all the import options except the Active directory option.

Import from Progress OpenEdge

Select the **Import from Progress OpenEdge** option in the **Integration Mode** field. Click on the **Edit** button.

Integrate supports Import from Progress OpenEdge version OpenEdge 12.8.

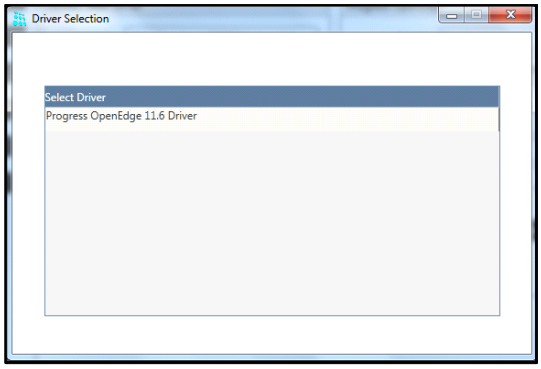


In the **COSEC Web Server** section:

- Specify the web URL of the api service of the COSEC WEB application as shown.
- Enter the User Name and Password of the SA user as set in the COSEC WEB application.

In the **Progress OpenEdge** section:

- **Server**: Enter the server name with which the Progress OpenEdge database is started.
- **Driver Name**: Select the Progress OpenEdge driver from the picklist. It is the software driver which will appear in picklist, once the database is installed.



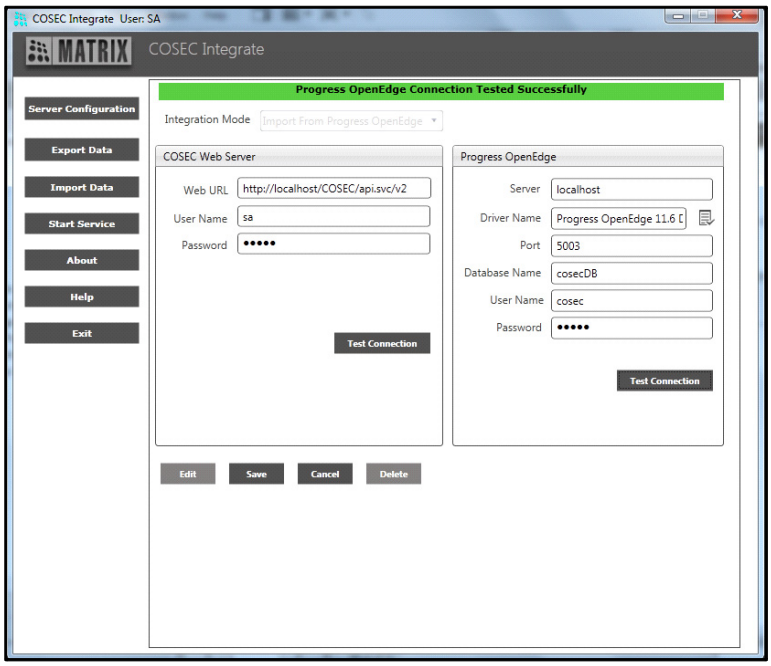
- **Port:** Enter the port number at which the Progress OpenEdge database is running. It is the port number (eg: 5003) entered in command prompt while starting the database as shown below.
- **Database Name:** Enter the database name with which Progress OpenEdge database is started. It is case sensitive. Thus if Database is started with name cosecDB as shown below then enter the name as “cosecDB”.

```
proenv>proserve -db C:\OpenEdge\WRK\cosecDB -H patricpillai -S 5003
OpenEdge Release 11.6 as of Fri Oct 16 19:01:51 EDT 2015
11:31:09 BROKER     This broker will terminate when session ends. (5405)
11:31:09 BROKER     The startup of this database requires 17Mb of shared memory.
  Maximum segment size is 128Mb.
11:31:09 BROKER  0: Multi-user session begin. (333)
11:31:09 BROKER  0: Before Image Log Initialization at block 0  offset 6031. (15
321)
11:31:09 BROKER  0: Login by admin on CON:. (452)
11:31:09 BROKER  0: This server is licensed for local logins only. (4393)
11:31:09 BROKER  0: Started for 5003 using TCP IPV4 address 127.0.0.1, pid 10172
. (5644)
```

- **User Name**: Specify the user name as entered while creating the database.

- **Password**: Specify the password as entered while creating the database. Eg: User name is cosec and Password is cosec.

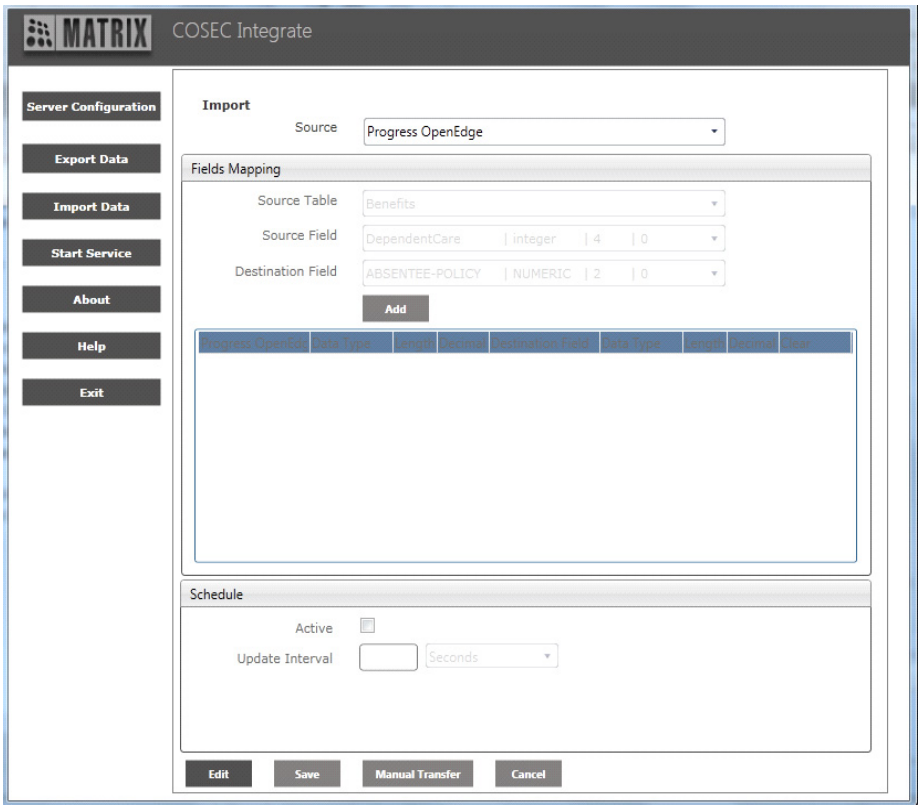
The **Test Connection** button is provided to test the connections with the web server as well as the Progress OpenEdge database.



Click on **Save** button to save the server configuration.

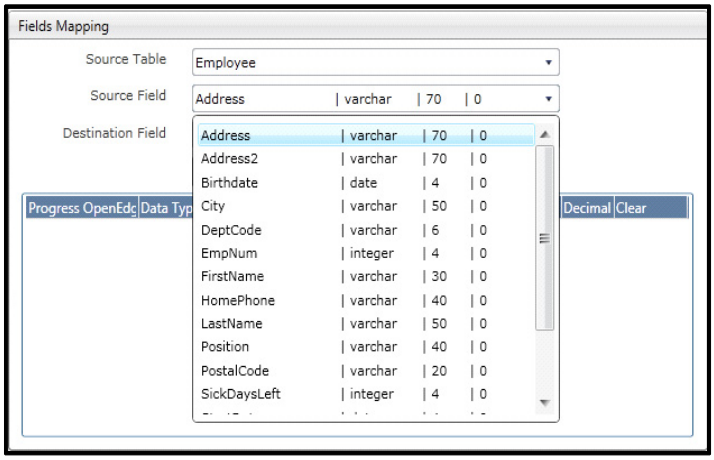
Import Data Configuration

This option enables the Admin user to map the fields from the external source database table to fields in the destination COSEC User table. Click on the **Import Data** button. The following page appears.

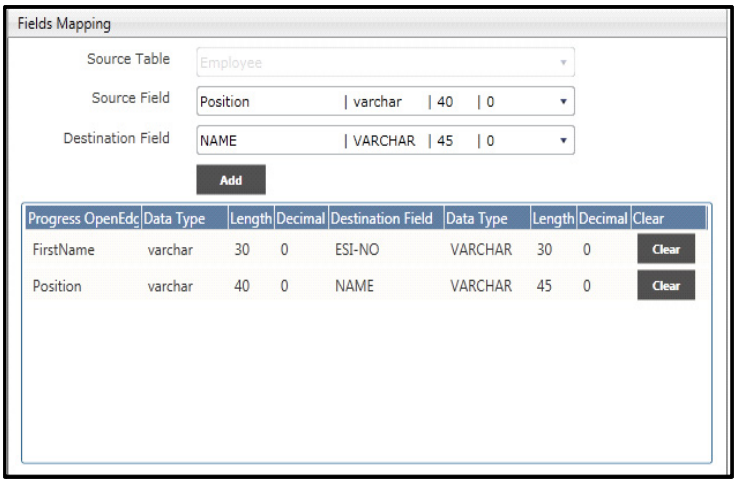


Select the Source and click on the **Edit** button at the bottom of the page.

Select the **Source Table** from the drop down list. The system will get the details of the fields from the source table and display the same in the **Source Field** parameter.



Select the appropriate **destination field** and click on the **Add** button. The mapped fields will be visible in the bottom grid as shown.

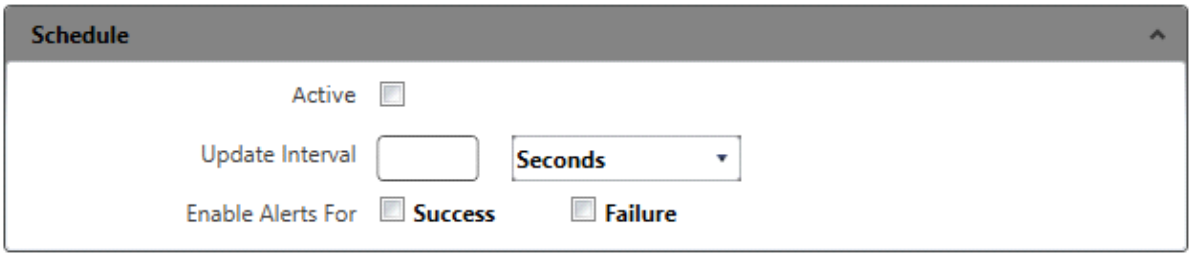


The following destination fields need to be compulsorily mapped with appropriate fields of the source table as shown.

- *id*
- *name*
- *BLNUPDATEFIELD*

This is common to all the import options except the Active directory option.

Schedule



- Check the **Active** box to enable the schedule.
- Specify the **Update Interval** in seconds, minutes or hours to define the frequency at which the application will update the destination database.
- **Enable Alert For:** When scheduled process gets completed then it will send an Alert to the configured COSEC Server. The Alert can be sent for both Successful as well as Failed transfers.

  Select the checkboxes as per your requirement:

  Select **Success** checkbox to send an alert mentioning the details of successfully transferred records to the configured COSEC Server.

  Select **Failure** checkbox to send an alert mentioning the details of failure in transferring records to the configured COSEC Server.

  If you require Alerts for both the above events, select both the check boxes.

In case of partial data transfer i.e. if both the above checkboxes are selected then the connection status will be considered as Failure and Reason for Failure will be displayed in the Alert.

Example: There are in total 100 records which are to be transferred.

Now, out of 100 records, only 60 records are transferred Successfully and the remaining 40 records have Failed. Such data transfers are known as partial data transfers.

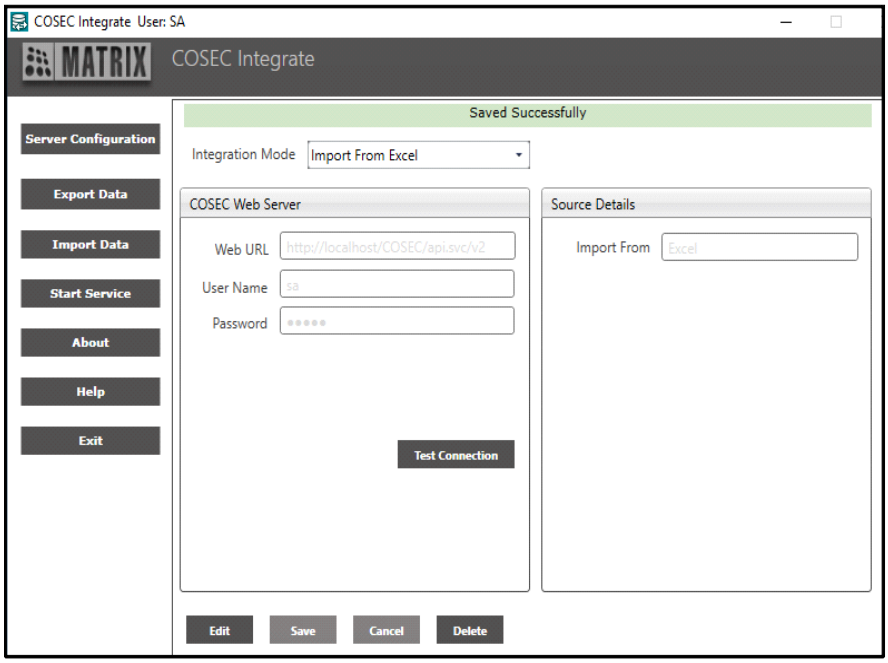
So here the connection status will be Failure and an alert will be sent to the configured COSEC Server along with the reason for failed data transfer.

It is to be supported for all integrate modes defined in COSEC Integrate where enable alerts provision is present i.e. for all the integration modes except for Custom Export-FP Template & Export FP Template to File.

Import from Excel

The COSEC INTEGRATE application provides the functionality to import leave transaction data from Excel.

Now user can click on the **Server Configuration** button to start the configuring process. The following page appears. Select the **Import From Excel** option in the **Integration Mode** field.



In the **COSEC Web Server** section:

- Specify the web URL of the api service of the COSEC WEB application as shown.
- Enter the User Name and Password of the SA user as set in the COSEC WEB application.

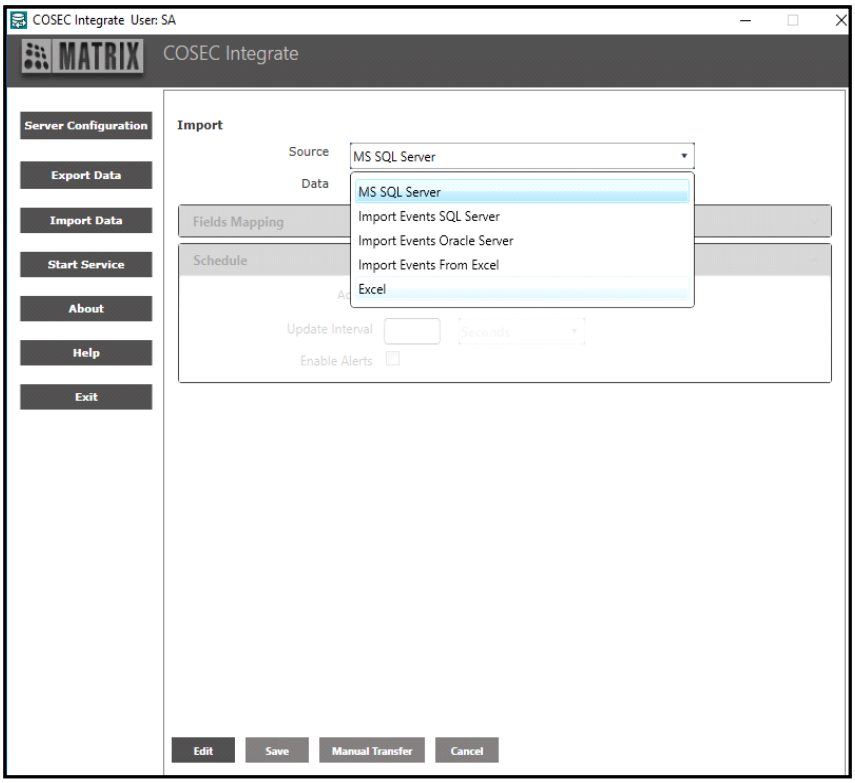
In the **Source Details** section:

- Select the **Import From** option as Excel.

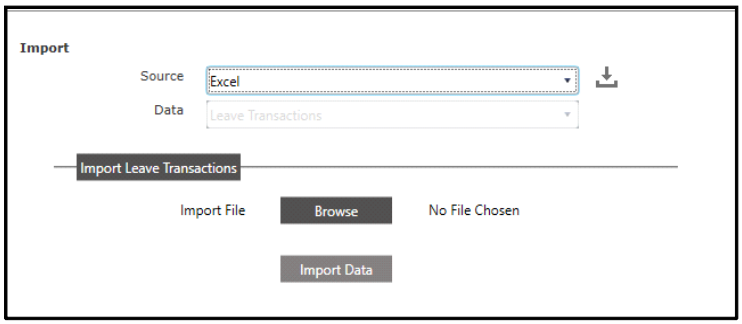
The **Test Connection** button is provided to test the connections with the web server.

Click on **Save** once done.

Now click on **Import Data** button.The following page appears.This option enables the admin user to select the external source database from where the data is to be imported in the destination COSEC table.



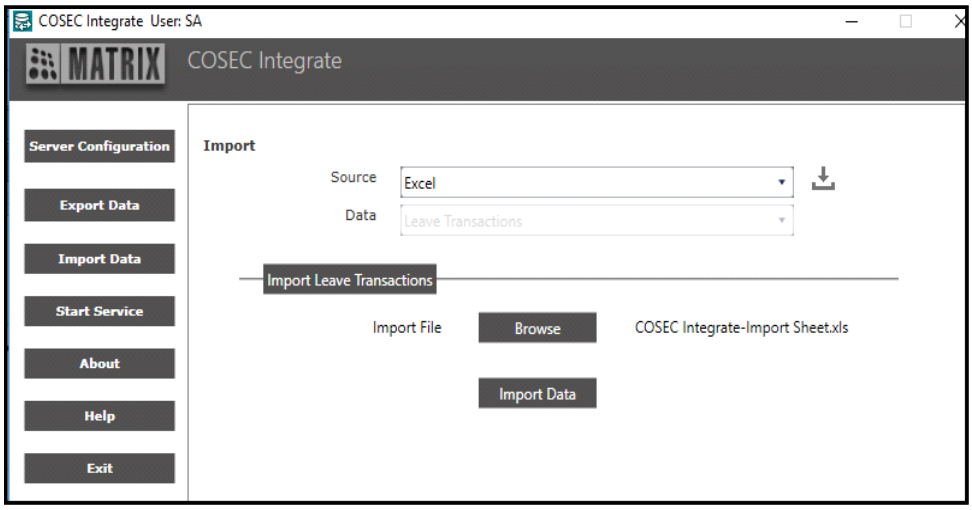
Select the source as **Excel.** The Data field shows the Leave Transaction.



You can click on to import the sample file for leave transaction. Then save the sample file at desired location.

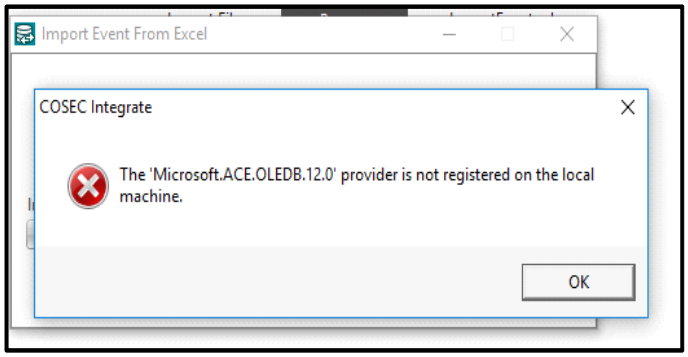
The leave records can be entered in the sample file.

Then click on **Browse** button to browse the file from where leave transactions are to be imported. Only .xls and .xlsx file of maximum size15 MB is allowed for import.

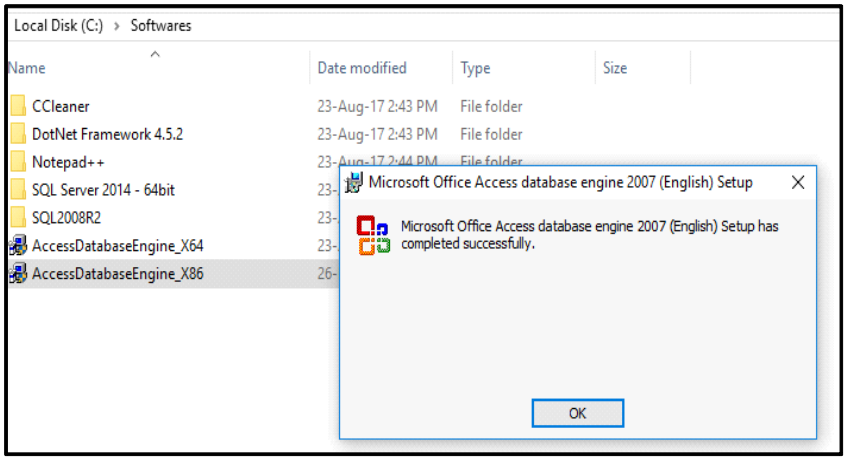


Then click on **Import Data**. The leave transaction data will be imported from the selected Excel file to the configured web server's database.

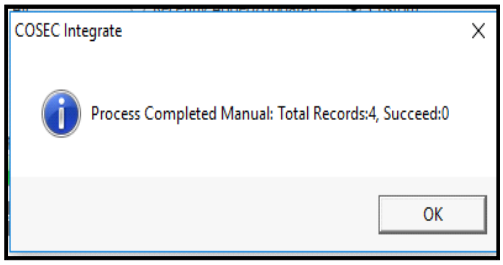
For importing excel file, you must have drivers to import.



You must install Access Database Engine compatible to your computer as shown below.



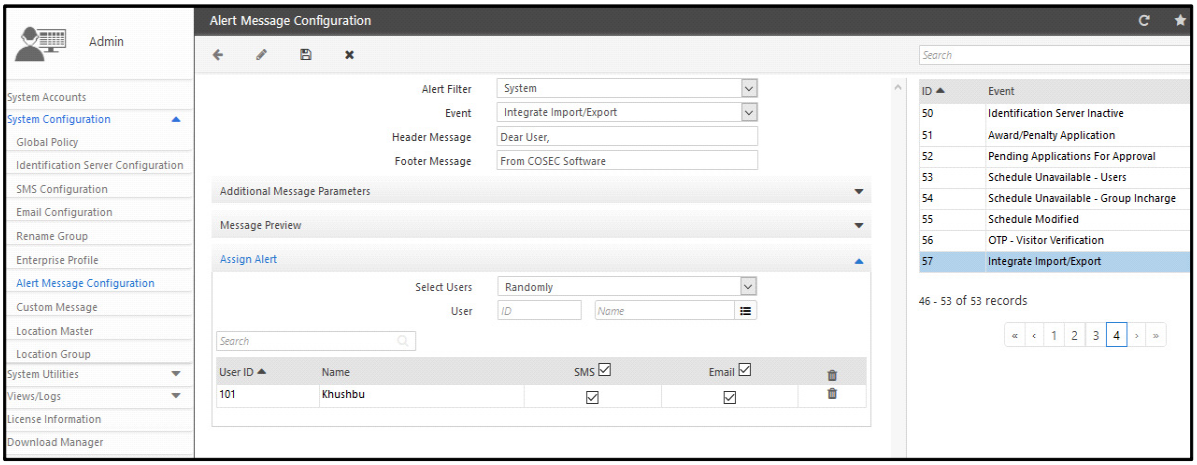
Then click on **Import Data** button. The import process is shown below.


COSEC Integrate
Process Completed Manual: Total Records:4, Succeed:0
OK

Integrate Alert

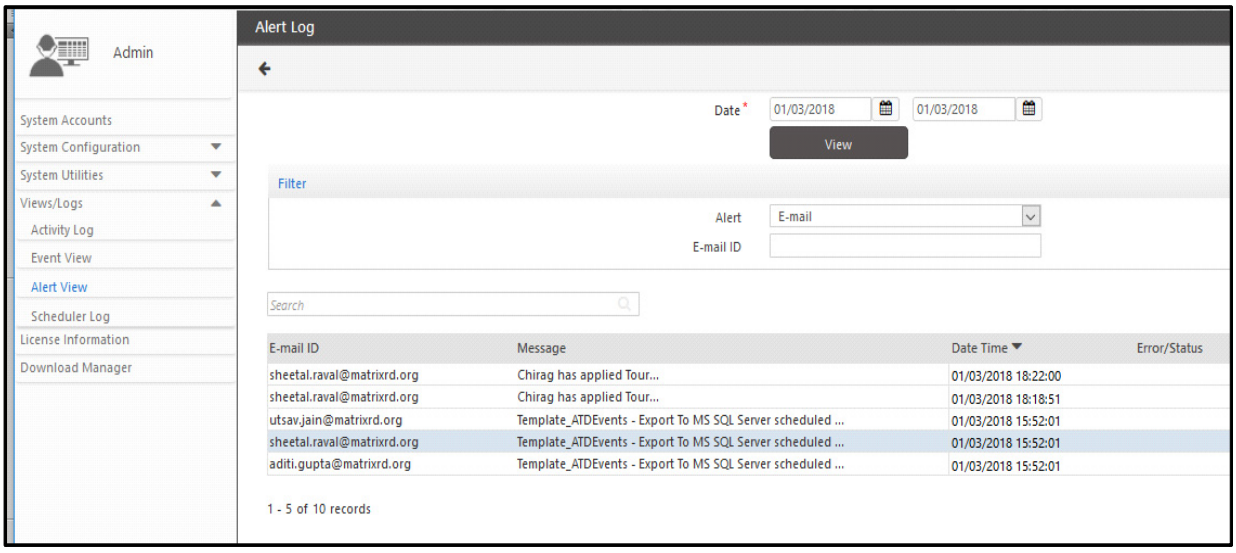
When the Integrate scheduled process gets completed, an API will be triggered to the configured COSEC server.

An Alert would be generated for the same and sent to those users as SMS or Email, for whom alert message is configured in Alert Message Configuration as shown below.

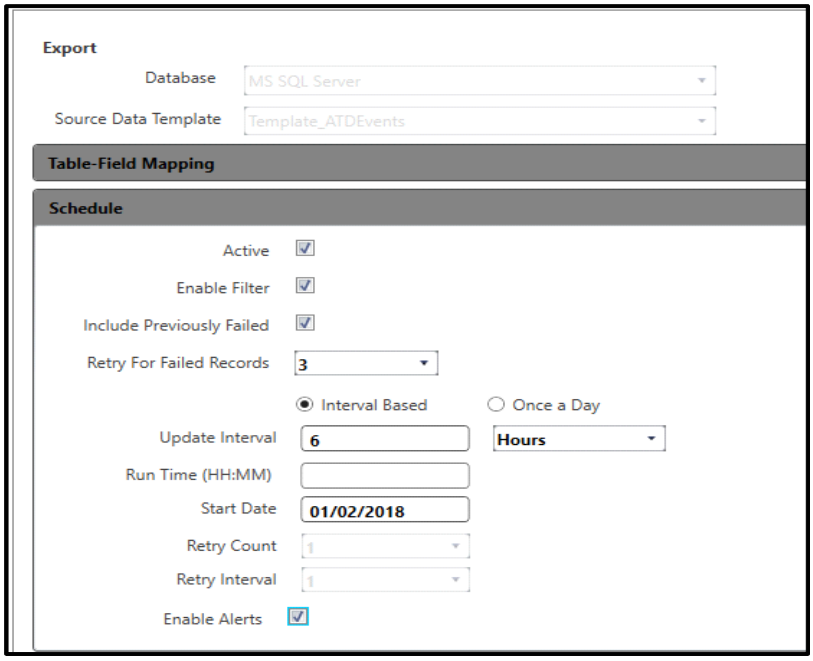


The Contact number and Email ID on which the alert is to be sent; must be specified in User Configuration.

An alert log with error/status message would be generated and displayed in Admin> Views/Logs > Alert View.



Consider a scenario, with configurations: **Include Previously Failed** is enabled and **Retry for failed records** =3, then count will be shown in Alert Message Configuration as displayed in below table.



Process number	Currently Scheduled Records	Successfully Transferred	Previously Failed Records	Successfully Transferred (from previously Failed Records)	To be displayed in Alert Message
1st Scheduled process	100	70	0	0	Scheduled|Success =100|70
2nd Scheduled process	50	20	30 (1st scheduler)	10 (1st scheduler)	Scheduled|Success =50|20
3rd Scheduled Process	100	90	20(1st scheduler) 30(2nd scheduler) Total=50	5(1st scheduler) 15 (2nd scheduler) Total=20	Scheduled|Success =100|90 Previously Failed|Success = 50|20
4th scheduled Process	50	50	15(2nd scheduler) 10(3rd scheduler) Total=25	10(2nd scheduler) 5 (3rd scheduler) Total=15	Scheduled|Success =50|50 Previously Failed|Success = 25|15

If the Integrate version and COSEC Server version are different then no alert would be sent to Server and assigned users even though Alert is configured.

BACnet Server Configuration

BACnet (Building Automation and Control Network) is an industry-standard protocol that is specifically used in Building Automation Systems. BACnet provides a standard framework for communication, management, monitoring and control of various automation functions specific to buildings, such as Lighting, HVAC, Fire Safety, Access Control and Energy Management Systems. BACnet supports multiple communication protocols, including Ethernet, TCP/IP, and RS-485, allowing for the integration of devices from different manufacturers and technologies.

Various Building Management Systems (BMS) rely on BACnet to communicate with each other for the exchange of data and to control devices and automation systems within a building.

Integration of BACnet with COSEC enhances its capability to integrate with 3rd party Building Management Systems. With this integration, COSEC Devices and their Events can be used to control various automation functions.

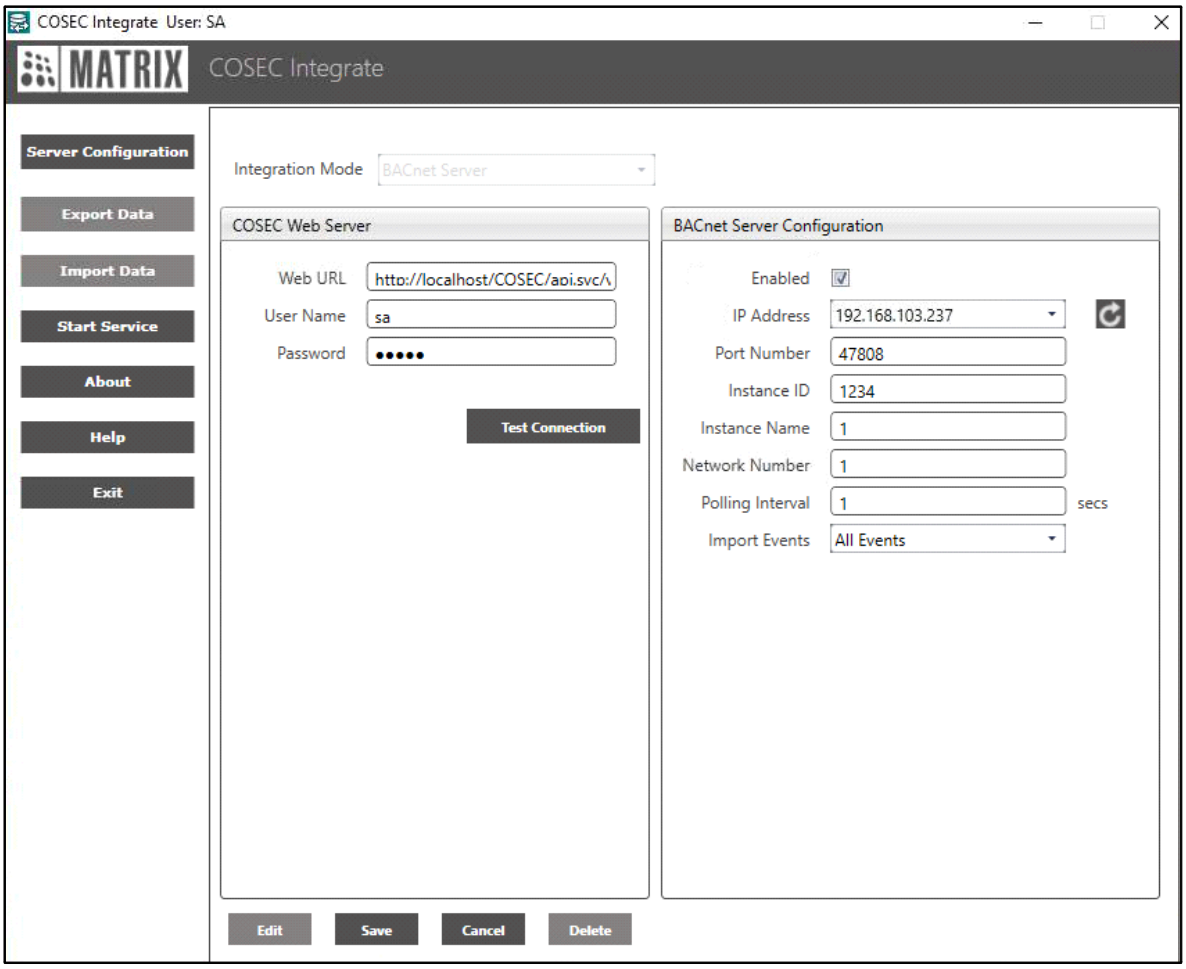
The COSEC Devices and their Event data will be sent to various 3rd party Building Management Systems (BACnet clients) through COSEC Integrate. Configuration of BACnet Server in COSEC Integrate will enable it to communicate with COSEC Server and fetch the desired data which in-turn will be shared with BACnet clients.

To integrate BACnet with COSEC, you need to:

- Configure the BACnet Server in COSEC Integrate. Once configured, these parameters will appear in Admin Module > System Configuration > BACnet Configuration > BACnet Server Configuration in COSEC Web.
- Configure the BACnet Server parameters in COSEC Web. For details, refer to Admin Module > System Configuration > BACnet Configuration > BACnet Server Configuration in the User Guide.
- Configure the BACnet Client List parameters. For details, refer to Admin Module > System Configuration > BACnet Configuration > BACnet Client List Configuration in the User Guide.

BACnet Server Configuration

Click **Server Configuration**. The following page appears.



Click **Edit** and configure the following parameters:

- **Integration Mode**: Select the **BACnet Server** option.

COSEC Web Server

- **Web URL**: Configure the Web URL of the API service of the COSEC Web Server application.
- **User Name**: Configure the User Name, for example sa (It can be any user who has API Access Rights of the COSEC Web Server application.)
- **Password**: Configure the Password as set for the COSEC Web Server application.

BACnet Server Configuration

- **Enable**: Select the check box to enable BACnet Server configuration.
- **IP Address**: Select the IP Address to be assigned to the BACnet Server from the drop-down list. Click **Refresh** to refresh the IP List. This is the IP Address list of multiple networks incase the PC on which Integrate is installed has multiple network connections (excluding loopback IP, that is 127.0.0.1)

- **Port Number**: Configure the Port Number of the BACnet Server (this is the free port of the PC on which Integrate is running. This port will be used for communication between the Integrate via BACnet Server and the BMS Client).
- **Instance ID**: Configure the Instance ID which will be used by BACnet Server to communicate with the Client. This will be provided by the Client.
- **Instance Name**: Configure the Instance Name which will be used by BACnet Server to communicate with the Client. This will be provided by the Client.
- **Network Number**: Configure the Network Number which will be used by BACnet Server to communicate with the Client. This will be provided by the Client.
- **Polling Interval**: Specify the Polling Interval in seconds between two consecutive data fetch requests from COSEC Integrate to COSEC Web Server.
- **Import Events**: Select the Events to be imported from COSEC Web Server options — Live Events or All Events.
- **Event Retrieval In**: If Import Events is selected as **Live Events**, configure the Event Retrieval time in seconds between two consecutive retrieval requests from COSEC Integrate to COSEC Web Server for Live events.

Click **Test Connection** to test the connection with COSEC Web Server.

Click **Save** to save the configuration. Now, click **Start Service**. Once the service starts, the BACnet Server Configuration will be fetched by the COSEC Web Server.

Configure the BACnet Server and BACnet Client List parameters in COSEC Web to enable the data transfer from COSEC Web to the BACnet clients via COSEC Integrate. For details, refer to Admin Module > System Configuration > BACnet Configuration in User Guide.

For details regarding the Event interactions handled in BACnet, refer to “List of Event Interactions handled in BACnet Integration”.

List of Event Interactions handled in BACnet Integration

Door_Alarm_State values based on the event Interaction.

Event ID	Description	Enum Description	Enum Value	Remark
301 → Dead-man timer expired Alarm– User IN	Dead Man timer expiry alarm generated by <user id : Username : Username>	dead-man-timer-expired	256	
302 → Duress detection	Duress detection alarm detected for <user id : Username>	duress-alarm	257	
303 → Panic Alarm	Panic Alarm generated by <user id : Username>	panic-alarm	258	
304 → FP Memory Full – Alarm	FP Memory Full Alarm generated for Internal memory	fp-full-alarm	259	
	FP Memory Full Alarm generated for external memory			
305 → Door Held open too long	Alarm for door held open for too long generated.	door-open-too-long	2	
306 → Door Abnormal	Door Abnormal alarm generated.	door-abnormal-alarm	260	
307 → Door force open	Door Force Open alarm generated.	forced-open	3	
308 → Door Controller Offline	Door Controller Offline Alarm generated.	door-offline	261	
309 → Door Controller -Fault	Alarm for fault in Door Controller generated	door-fault	5	
310 → Tamper Alarm	Tamper Alarm generated.	tamper	4	
314 → RTC	Power ON/OFF Detected <for external reader> (time not in sync)	rtc-fault	262	
	low battery detected <for external reader>			
	RTC Not Detected <for external reader>			

315 → Event Buffer Full	Event Buffer Full	event-buffer-full	263	
316→ Zone Empty	Zone Empty alarm generated.(This event is discarded)	zone-empty-alarm	264	
317→ Intercom - panic	Intercom Panic Alarm by extension number {extn number}generated.	intercom-panic	265	
318→ Occupancy Violated Alarm	Occupancy Rule Violated by <user id : Username>	occupancy-violation	266	
319→ Tail- Gating Alarm	Tail - Gating by <user id : Username>	tail-gating	267	
320→Man Trap Timer Violated Alarm	Man Trap Timer Violated by <user id : Username>	man-trap-timer-violation	268	
321→Access Denied Aalrm	Access Denied Alarm generated.	access-denied-alarm	269	
322→Multiple Unauthorized Access Alarm	Multiple Unauthorized Attempts count reached by by <user id : Username>	multiple-unauthorized-access	270	
323-> Custom Alarm 1	Custom Alarm 1 generated.	custom-alarm1	271	
324->Custom Alarm 2	Custom Alarm 2 generated.	custom-alarm2	272	
325-> Custom Alarm 3	Custom Alarm 3 generated.	custom-alarm3	273	
326→ User Unidentified	User Unidentified Alarm Generated	user-unidentified-alarm	274	
327->Anti-Pass Back Violated Alarm	Anti-Pass Back Rule Violated by <user id : Username>	passback-violation	275	
328->Access Route Violated Alarm	Access Route Violated by <user id : Username>	access-route-violation	276	
329-> Raise Alarm	IO Link Activated by <user ID : UserName>	raise-alarm	277	
330 → Lock Open Too Long	Alarm for lock open for too long generated.	lock-open-to-long	278	
331 → Lock Abnormal	Lock abnormal alarm generated.	lock-abnormal	279	

332 → Manual Lock Override	Manual lock override alarm generated.	manual-lock-override	280	
351 → Alarm acknowledged	Alarm acknowledged through System Interlock/ Web Jeeves/ACMS/special Functions. Alarm auto acknowledged	alarm-acked	281	
352 → Alarm cleared	Alarm cleared through System Interlock/Web Jeeves/ACMS/Special Functions. Alarm auto cleared	normal	0	When Multiple Alarms are active and any of them is cleared (while door is still in alarm mode) then Door Alarm State will be set to 'alarm (1)' value. Enum value will be 1.
353 → Alarm Re-issued	Alarm Re-issued	This will get the previously issued Alarm state.		
354 → Anti-Loiter Zone Violated Alarm	Anti-Loiter Zone Rule Violated by <user id : Username>	anti-loiter-violation	282	
333 → Access Route Timer Violated Alarm	Access Route Timer Violated by <User ID : Username> at <Door Name>	access-route-timer-violation	283	
334 → Threshold Temperature Exceeded	Threshold Temperature Exceeded by <User ID : Username>	thresold-temperature-exceeded	284	
335→ Face Mask Not Detected	Face Mask Not Detected for <User ID : Username>	face-mask-not-detected	285	
		Alarm	1	When Multiple Alarms are active and any of them is cleared (while door is still in alarm mode) then Door Alarm State will be set to 'alarm (1)' value. Enum value will be 1.

Door_Status values based on the event Interaction.

Event ID	Description	Enum Description	Enum Value	Remark
201 → Door Status changed	Door status normal.	Normal	1024	

(generate this event whenever the door state is changed through special function or Door M&C page)	Door status locked.	LOCKED	1025	
	Door status unlocked.	UNLOCKED	1026	
(Also generate this event for API commands and when external IO link command is received)	Door Status armed	ARMED	1027	
	Door status disarmed.	DISARMED	1028	
202 → Dead-man timer changed	Dead man timer activated.	No Change in State.		
(generate this event whenever Dead-man timer activated or expired/ deactivated)	Dead man timer deactivated.	No Change in State.		
203 → DND status changed	DND Status activated	DND-ACTIVE	1029	
	DND Status deactivated	DND-INACTIVE	1030	
204 → Aux input status changed	Aux input activated.	AUX-IN-ACTIVE	1031	
Generate this event whenever Aux input status is changed.	Aux input normal.	AUX-IN-NORMAL	1032	
	Aux input fault(open)	AUX-IN-FAULT-OPEN	1033	
(This event with Disabled in special field-1 is generated against Door M&C user input.)	Aux input fault(short)	AUX-IN-FAULT-SHORT	1034	
	Aux input disabled.	AUX-IN-DISABLE	1035	
205 → Aux output status changed	Aux output activated.	AUX-OUT-ACTIVE	1036	

(This event with Disabled in special field-1 is generated against Door M&C user input.)(Also generate this event for API commands and when external IO link command is received)	Aux output normal.	AUX-OUT-NORMAL	1037	
	Aux output disabled.	AUX-OUT-DISABLED	1038	
206 → Door sense input status	Door sense input normal	DOOR-SENSE-NORMAL	1039	
(This event with Disabled in special field-1 is generated against Door M&C user input.)	Door sense input fault(open)	DOOR-SENSE-FAULT-OPEN	1040	
	Door sense input fault(short)	DOOR-SENSE-FAULT-SHORT	1041	
	Door sense input disabled.	UNUSED	4	
207 → Door Controller Communication status	Door controller ON Line	DOOR-ONLINE	1043	
(generate this event whenever the DC status changed to ON line or change to OFF Line)	Door controller OFF Line	DOOR-OFFLINE	1044	
	Door controller is upgrading	DOOR-UPRGRADING	1045	
208 → Door Open/ Close	<User id : Username> has opened the door	OPENED	1	
	Door Open/Close - Open	OPENED	1	
	Door state changed to Close	CLOSED	0	
	<User id : Username> has not operated the door	CLOSED	0	
	Door Open/Close - NotOperated	CLOSED	0	

209 → Lock Open/ Close	<User id : Username> has opened the lock.	OPENED	1	
	<User id : Username> has closed the lock.	CLOSED	0	
	<User id : Username> has not operated the lock	CLOSED	0	
	Manual lock override.	LOCK-OVERRIDE	1046	

Present Value in Panel Custom Object based on Event Interaction

Event ID	Description	Property Value
302 → Duress detection	Duress detection alarm detected for <user id : Username>	duress-alarm
308 → Door Controller Offline	Door Controller Offline Alarm generated.	door-offline
311 → Master Controller Mains fail Alarm	Alarm for Mains fail of Master Controller generated.	master-controller-mains-fail-alarm
312 → Master Controller Battery fail	Alarm for Battery fail of Master Controller generated.	master-controller-battery-fail-alarm
313 → Master Alarm – MC Alarm input	MC input Master alarm generated	master-alarm-input
315 → Event Buffer Full	Event Buffer Full	event-buffer-full
316→ Zone Empty	Zone Empty alarm generated.(This event is discarded)	zone-empty-alarm
318→ Occupancy Violated Alarm	Occupancy Rule Violated by <user id : Username>	occupancy-violation
353 → Alarm Re-issued	Alarm Re-issued	alarm-reissued
352 → Alarm cleared	Alarm cleared through System Interlock/Web Jeeves/ACMS/Special Functions. Alarm auto cleared	normal
204 → Aux input status changed	Aux input activated.	AUX-IN-ACTIVE
Generate this event whenever Aux input status is changed.	Aux input normal.	AUX-IN-NORMAL

	Aux input fault(open)	AUX-IN-FAULT-OPEN
(This event with Disabled in special field-1 is generated against Door M&C user input.)	Aux input fault(short)	AUX-IN-FAULT-SHORT
	Aux input disabled.	AUX-IN-DISABLE
205 → Aux output status changed	Aux output activated.	AUX-OUT-ACTIVE
(This event with Disabled in special field-1 is generated against Door M&C user input.)(Also generate this event for API commands and when external IO link command is received)	Aux output normal.	AUX-OUT-NORMAL
As no event is received for PANEL connected and disconnected.	Door controller ON Line	PANEL_ONLINE
	Door controller OFF Line	PANEL_OFFLINE

Generic Notes

Sheet Name	Applicable Device	Naming Convention	Description	Instance Number
Binary Output-IO	IO 800	{COSEC_Door Name}_AUXOUT_{PortNo}_{1}{MID}{0}/{2}{MID}{DID}		
		{COSEC_Door_Name}	Device Name mentioned in COSEC Software. Example: IO Controller 1	
		Direct Door	Naming Convention : {COSEC_Door Name}_AUXOUT_{PortNo}_{1}{MID}{0}	Direct Door : {PortNo}{1}{MID}{0}
		Panel Door	Naming Convention : {COSEC_Door Name}_AUXOUT_{PortNo}_{2}{MID}{DID}	Panel Door : {PortNo}{2}{MID}{DID}
		PortNo	1 to 8	
Multistate Input	IO 800	{COSEC_Door Name}_AUXIN_{PortNo}_{1}{MID}{0}/{2}{MID}{DID}		
		{COSEC_Door_Name}	Device Name mentioned in COSEC Software. Example: IO Controller 1	
		Direct Door	Naming Convention : {COSEC_Door Name}_AUXIN_{PortNo}_{1}{MID}{0}	Direct Door : {PortNo}{1}{MID}{0}

		Panel Door	Naming Convention : {COSEC_Door Name}_AUXIN_{PortNo}_{2}{MID}{DID}	Panel Door : {PortNo}{2}{MID}{DID}
		PortNo	1 to 8	
COSEC Panel	COSEC PANEL (All variants)	PANEL	{COSEC_Panel Name}_{MID}	{MID}
		{COSEC_PANEL_Name}	Device Name mentioned in COSEC Software. Example: PANEL 1	
Access Door	Direct Doors and Panel Doors All the Door Controllers	{COSEC_Door Name}_{1}{MID}{0}/ {2}{MID}{DID}		
		{COSEC_Door_Name}	Device Name mentioned in COSEC Software. Example: Door 1	
		Direct Door	Naming Convention : {COSEC_Door Name}_{1}{MID}{0}	Direct Door : {1}{MID}{0}
		Panel Door	Naming Convention : {COSEC_Door Name}_{2}{MID}{DID}	Panel Door : {2}{MID}{DID}

Binary Output-IO

Event ID	Description	Present Value	Value	Remarks
205 → Aux output status changed	Aux output activated.	ACTIVE	1	By default, when there are no AUX Out event then Present Value will be INACTIVE.
205 → Aux output status changed	Aux output normal.	INACTIVE	2	Whenever an Event is generated for AUX Out Activated then Event_State will be set to OFF_NORMAL. Present value reference shall be updated to ACTIVE.

Multistate Input-IO

Event ID	Description	Present Value will be fetched from Array	State Text
204 -> Aux input status changed	Aux input activated.	0	{{"AUX-IN-ACTIVE"},{"AUX-IN-NORMAL"},{"AUX-IN-FAULT-OPEN"},{"AUX-IN-FAULT-SHORT"},{AUX-IN-DISABLED}}

204 -> Aux input status changed	Aux input normal.	1	{{"AUX-IN-ACTIVE"},{"AUX-IN-NORMAL"},{"AUX-IN-FAULT-OPEN"},{"AUX-IN-FAULT-SHORT"},{AUX-IN-DISABLED}}
204 -> Aux input status changed	Aux input fault(open)	2	{{"AUX-IN-ACTIVE"},{"AUX-IN-NORMAL"},{"AUX-IN-FAULT-OPEN"},{"AUX-IN-FAULT-SHORT"},{AUX-IN-DISABLED}}
204 -> Aux input status changed	Aux input fault(short)	3	{{"AUX-IN-ACTIVE"},{"AUX-IN-NORMAL"},{"AUX-IN-FAULT-OPEN"},{"AUX-IN-FAULT-SHORT"},{AUX-IN-DISABLED}}
204 -> Aux input status changed	Aux input disabled.	4	{{"AUX-IN-ACTIVE"},{"AUX-IN-NORMAL"},{"AUX-IN-FAULT-OPEN"},{"AUX-IN-FAULT-SHORT"},{AUX-IN-DISABLED}}

COSEC Panel

Event ID	Description	Present Value State text reference	Event Type
302 -> Duress detection	Duress detection alarm detected for <user id : Username>	duress-alarm	ALARM
308 -> Door Controller Offline	Door Controller Offline Alarm generated.	door-offline	ALARM
311 -> Master Controller Mains fail Alarm	Alarm for Mains fail of Master Controller generated.	master-controller-mains-fail-alarm	ALARM
312 -> Master Controller Battery fail	Alarm for Battery fail of Master Controller generated.	master-controller-battery-fail-alarm	ALARM
313 -> Master Alarm – MC Alarm input	MC input Master alarm generated	master-alarm-input	ALARM
315 -> Event Buffer Full	Event Buffer Full	event-buffer-full	ALARM
318 -> Occupancy Violated Alarm	Occupancy Rule Violated by <user id : Username>	occupancy-violation	ALARM
353 -> Alarm Re-issued	Alarm Re-issued	alarm-reissued	ALARM
352 -> Alarm cleared	Alarm cleared through System Interlock/ WebJeeves/ACMS/SpecialFunctions. Alarm auto cleared	normal	ALARM
204 -> Aux input status changed	Aux input activated.	AUX-IN-ACTIVE	Transaction

Generate this event whenever Aux input status is changed.	Aux input normal.	AUX-IN-NORMAL	Transaction
	Aux input fault(open)	AUX-IN-FAULT-OPEN	Transaction
(This event with Disabled in special field-1 is generated against Door M&C user input.)	Aux input fault(short)	AUX-IN-FAULT-SHORT	Transaction
	Aux input disabled.	AUX-IN-DISABLE	Transaction
205 -> Aux output status changed	Aux output activated.	AUX-OUT-ACTIVE	Transaction
(This event with Disabled in special field-1 is generated against Door M&C user input.)(Also generate this event for API commands and when external IO link command is received)	Aux output normal.	AUX-OUT-NORMAL	Transaction

MATRIX COMSEC

Head Office:
394-GIDC, Makarpura, Vadodara - 390010, India.
Ph:(+91) 18002587747
E-mail: Tech.Support@MatrixComSec.com

www.MatrixComSec.com