SAP Fieldglass

Product Information | PUBLIC
SAP Fieldglass

SAP Fieldglass Configuration Manager

SAP

Content

1 Introduction

The Configuration Manager role allows buyers to establish super users who can access integration, system, and maintenance tools via a self-service dashboard.

Configuration Managers have access to configuration tools, system tools, and other maintenance tools through a self-service dashboard. The tools allow you to perform many administrative actions independently, eliminating the need to open support cases with SAP Fieldglass to implement those actions in your company.

Configuration Tools

Configuration Tools allow you to enable and manage the integration connectors. Using an intuitive wizard framework, you can enable, edit, manage, and troubleshoot integration connectors.

In addition, you can manage the following features:

- API Application Keys
- DocuSign Endpoints
- Encryption Keys and Certificates
- End Points
- Integration Subscriptions
- SAP Task Center Integration
- Time Processing Tenant

Encryption Keys and Certificates allow you to create and manage the company's security assets associated with the SAP Fieldglass application. Using customer-managed encryption keys and certificates eliminates having to contact SAP Fieldglass for assistance with creating and managing security assets.

SAP Task Center allows you to set up authentication to push task updates from SAP Fieldglass to SAP Task Center.

Partner Management

Partner Management provides access to a growing network of partner integrations that are being migrated from the SAP Fieldglass application to the self-service framework on the dashboard. When a migration is completed, a tile labeled with the partner's name is added to the Partner Management section. Selecting the tile opens that partner's administrative setup pages, where you can set up and manage the integration, without having to contact SAP Fieldglass for assistance.

Single Sign-On

Single Sign-On (SSO) tools allow you to manage the SSO configurations for your company. Using an intuitive wizard framework, you can configure, edit, manage, and troubleshoot your SSO setup, as well as receive notifications when your SSO certificate is close to expiration and needs to be updated. Additionally, you can enable SAP Task Center in SAP Fieldglass, which provides a single entry point for users to access all their assigned tasks across various SAP applications in a central inbox.

Publish/Subscribe Framework

Publish/Subscribe Framework tools allow you to manage real-time application activity. Using a setup wizard that allows you to configure the required elements in one workflow, you can create payloads and end points, and subscribe to application activities. Individual tools allow editing configurations and testing payloads.

Rates

Rates tools allow you to maintain rate components and view and test business rules.

Actions

Additional tools available currently include enabling and viewing the SAP Fieldglass Qualification Dictionary.

2 Getting Started with Configuration Manager

To get started, identify users to act as the configuration manager for your company. A company administrator can set up your configuration manager users from their main SAP Fieldglass user accounts.

The configuration manager is assigned an additional SAP Fieldglass Sign In ID. This ID only allows access to the Self-Service Dashboard in Configuration Manager. To perform other administrative or general actions in SAP Fieldglass, the ID associated with the user's original role must be used to sign in.

> **Note**
>
> Multiple configuration managers can be established for a company.

The configuration manager account is a copy of the SAP Fieldglass user account. All profile settings, preferences, and user details are copied to the new configuration manager account. However, these options are locked and can only be edited using the user account. When the configuration manager account is created, a linked account is automatically created between the user's account and the configuration manager's account, and it displays in the Linked Accounts list for both accounts.

> **Note**
>
> If a buyer user changes the locale language in *Personal Settings > My Preferences*, the new language applies to all configuration manager users associated with that buyer user.

After the configuration manager logs in, tiles display for the available tools. Use the tiles to view, create, and manage items within each tile. You also can use the quick *Create* menu to create new items without having to locate the appropriate tile.

Tiles on the dashboard are assigned categories. You can filter the tiles by category using the *Category* drop-down. Tiles are assigned to the following categories on the Self-Service Dashboard:

- Configuration Tools
- Partner Management
- Analytics
- Single Sign-On
- Publish/Subscribe Framework
- Rates
- Actions
- Implementation Tools

3 Configuration Tools

Describes the tools available in the Configuration Tools section of the Self-Service Dashboard.

The primary purpose of SAP Fieldglass integrations is to move data securely from one system to another system. There's a starting point where the data resides and an ending point where the data needs to be delivered.

Connectors are the transports that encompass the data, data format, and business logic required to seamlessly integrate with a client's application. Connectors eliminate the need for manual entry. The functionality decreases the amount of time it takes to process data and increases data accuracy by removing the chance for errors introduced by manual entry.

Connectors are grouped into two activity types:

- Upload Connectors – populate data from the client's system into SAP Fieldglass.
- Download Connectors – populate data from SAP Fieldglass into the client's system.

Configuration Tools allow you to independently manage the integration connectors for your company, eliminating the need to open support cases with SAP Fieldglass to implement those actions in your company. Using an intuitive wizard framework, you can enable, edit, and manage connectors, as well as monitor the progress of file uploads and downloads, and troubleshoot issues if they arise, and manage all connector-related activities.

Configuration Tools Tiles

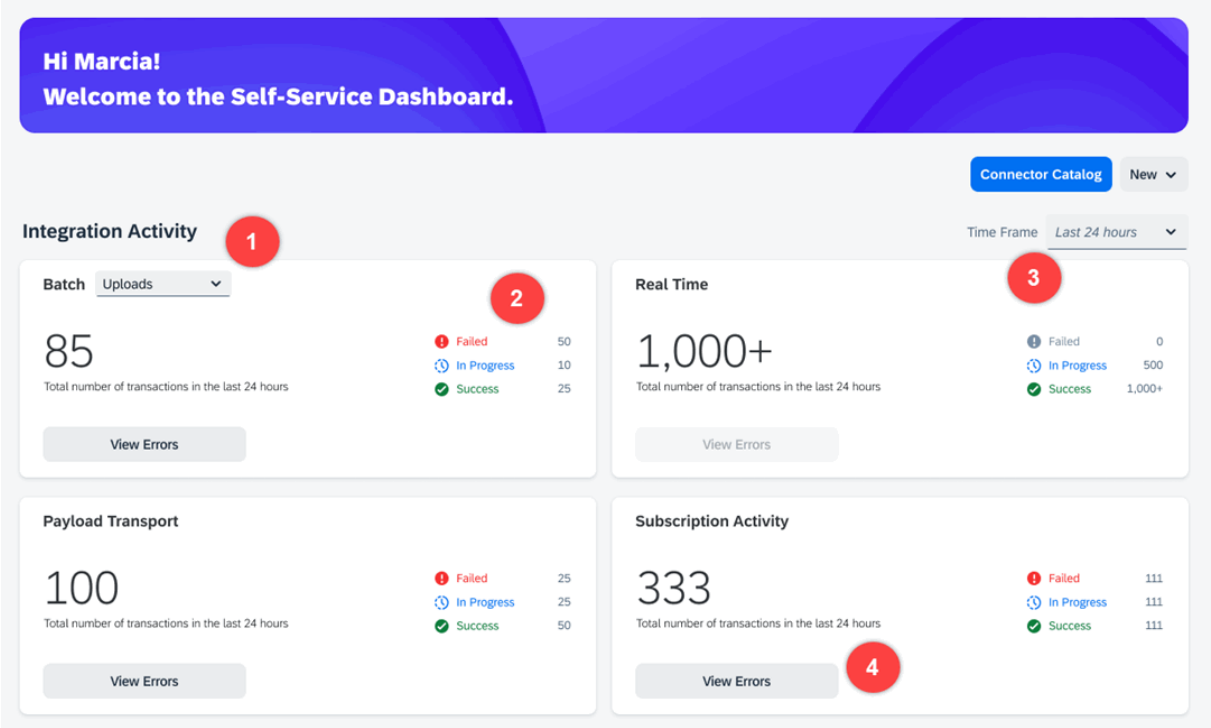
Tile Name	Description
Connector Wizard	Opens the Connector Wizard. Allows a buyer CM to locate and enable integration connectors for their company in SAP Fieldglass. The buyer CM can also define connector specifications, security, custom fields and templates, transfer methods, optional connector variants, and scheduling. This tile isn't applicable or visible to supplier CM users.
Connectors	Opens the Connector List page, a tabbed interface. The 'Company Connectors' tab lists all connectors enabled for your company. The 'Connector Catalog' tab contains options to view: All connectors including enabled, never enabled, enabled but then disabled; My Connectors – the same list that displays under the Company Connectors tab; and Available Connectors to be enabled.
API Application Keys	Opens the Basic Setup dialog box on the API Application Key page. Allows you to create and view API application keys, view and edit existing web service accounts related to the company, and create new web service accounts.
Encryption Keys and Certificates	Opens the Encryption Keys and Certificates page. Allows you to create and manage the company's security assets associated with the SAP Fieldglass application.
End Points	Opens the End Point List page. Allows you to add, view, and edit end points, as well as copy, remove, activate, and deactivate end points for the categories OData, SFTP subscription, Publish/Subscribe, WebService.

Tile Name	Description
Integration Subscriptions	Opens the Subscription List page. Allows you to set up and manage subscriptions to uploads and downloads.
Monitor Activity	Opens the Integration Audit Trail page. Allows you to view batch activity for connector upload and download transactions, real-time activity for event-driven data transport activities, and payload details for data transport activities.
SAP Task Center	Opens the SAP Task enter page. Allows you to enable SAP Fieldglass to automatically push task updates to SAP Task Center.

3.1 Integration Activity

The Integration Activity tiles show your company's integrations statuses and alerts for batch and real time integrations, as well as your payload transports and subscription activity.

The Integration Activity section shows up to 4 tiles that allow you to see the status of your integrations (Success, In Progress, and Failed) in real time.



1. You can switch between uploads and downloads in the Batch integration tile.
2. Each tile shows the statuses of your integrations along with visual alerts to indicate the state.
3. You can change the Time Frame to show activity for the last 24 hours, 7 days, or 30 days.
4. The *View Errors* button opens the Monitor Activity dashboard tile to a pre-filtered view based on error types. To support the pre-filtered view, a new multi-select **Status** field has been added to the Monitor Activity page that allows you to select more than one status to filter on.

3.2 Connector Wizard

Describes how to use the Connector Wizard to locate and enable a connector. Also describes the workflow in the Connector Wizard.

On top-right side of the dashboard, the *Connector Wizard* button opens the *Connector Wizard* dialog box. The dialog box contains a decision tree that guides you through a series of preconfigured questions and optional answers to help you with the selection of a connector that suits your needs.

> **Note**
>
> The ability to create new connectors is limited to buyer CM users. As such, the *Connector Wizard* button isn't visible to supplier CM users.

The decision tree supports all connector categories and currently contains preconfigured questions for connectors in the categories of 'Worker and Work Order', and 'Time'. After selecting one of these categories, you're guided through the series of questions. Based on your answers, if an appropriate connector is identified, a success message displays the connector name in a hyperlink at the bottom of the dialog box. Choose the connector name to open the **Enable Connector Details** dialog box and display details of the connector and any available variants, or you can enable (create) a new connector variant. If an appropriate connector isn't identified, you're prompted to browse the Connector Catalog to select a connector.

When selecting any of the following connector categories, you're prompted to browse the Connector Catalog to choose a connector:

- User
- Expense
- Rate Structure
- Invoice
- Financial Data
- Master Data
- Services
- Job Posting
- Configuration
- Project

To get started with the selection of a connector category, go to Begin Setup: All Connector Categories [page 12].

After choosing a connector category, the next step depends on the connector category you chose, either Continue Setup: Worker and Work Order or Time Connector Categories [page 12] or Continue Setup: All Other Connector Categories [page 13].

Once you complete the first step and the applicable continuation step, you're directed to the *Welcome* step, the step-by-step process in the setup wizard to create the new connector and configure the connector details.

Connector Wizard Navigation

When creating a new connector or variant, the setup wizard guides you through the steps required to enable and configure the connector. The steps include defining specifications, security, custom fields and templates, variant flows, transfer methods, and scheduling a file upload or download. Optional steps are noted, where applicable.

The following setup sections are organized sequentially in the pane on the left side of the wizard:

1. Welcome (required
2. Configure (required)
    1. Enable (required)
    2. Setup (required)
    3. Connector Header (optional – upload connectors only)
    4. Security (optional)
3. Customize (optional)
    1. Customize Fields (optional – download connectors only)
    2. Available Custom Features (optional – download connectors only)
    3. Upload Column Transform (optional – download connectors only)
4. Connectivity (optional)
    1. Transfer Method Connectivity
    2. Setup End Point, Test End Point (for Transfer/Subscription)
    3. Setup Subscription - or -
    4. Setup Webservice
5. Finished Setup (required)

When using the setup wizard, note the following:

- To enable/disable contextual help, choose the icon on the top-right side of the wizard. When enabled the icon displays next to any field configured for contextual help. To display contextual help, hover over the icon.
- After opening the wizard, you must complete the mandatory fields on any current page before you can navigate to a different page. If necessary, you can exit the wizard and return to the dashboard without retaining any changes.
- After completing the required *Welcome* and *Configure* (*Enable* and *Setup*) sections, all other setup sections are optional. To bypass optional setup and take a fast-path to connector setup, complete the required sections, and at the end of the *Setup* section, choose *Next Step* to go to the *Finished* section. Also, in any of the optional sections, choose *Next Step* to skip the current section and go to the next optional section. You can complete any of the optional setup steps after the connector is enabled.
- When editing a connector, since the connector is already set up, lock icons don't display next to the setup sections. You can choose any setup section to edit—you don’t have to go step by step as is required in the enable workflow. In addition, when you make an edit, the changes are committed in place—you're not required to cycle through to the *Finished* section.

3.2.1 Begin Setup: All Connector Categories

Describes how to begin connector setup to create a connector using the decision tree.

In this task, you locate a connector category. When navigating questions and answers in the decision tree, you can clear and reselect answers as needed.

To locate a connector:

1. On the top-right side of the dashboard, choose Connector Wizard.
   The Connector Wizard opens.
2. To select a connector category, in the *To which category do you want to add an Integration Connector?* dialog box, choose *Select Answer*.
   The *Select Answer* dialog box opens.
3. Do either of the following to choose a connector category:
   1. Choose one of the connector categories in the list.
   2. To search for a connector category, type keywords in the *Search Answers* field. The list of categories filters based on the values you enter. For example, if you type `Invoice`, only connectors related to Invoice integrations display. Make your selection or continue to answer any additional questions to complete the decision tree.
4. After choosing a connector category, choose *Select*.
5. Based on the connector category you selected, choose one of the following options to continue:
   - Continue Setup: Worker and Work Order or Time Connector Categories [page 12]
   - Continue Setup: All Other Connector Categories [page 13]

3.2.2 Continue Setup: Worker and Work Order or Time Connector Categories

Describes how to continue connector setup after selecting a connector category of Worker and Work Order or Time.

After selecting a connector category of Worker and Work Order or Time, proceed with this task to select a connector type (upload or download) and continue enabling the connector.

1. In the *Enable Connector* dialog box, choose the type of connector you want to create, either *Upload* or *Download*.
2. Based on the answer you selected, do one of the following:
   1. Continue with the question and answer process. When a connector is identified, the *Enable Connector* dialog box displays a success message with the recommended connector name formatted in a hyperlink. To activate the recommended connector, choose the connector name hyperlink. The *Enable Connector Details* dialog box displays. Go to step 3.
   2. To choose a different connector of the same category and type, or if a specific connector can't be identified, choose *Browse Catalog*.
      The Connector List page opens in the *Connector Catalog*, filtered to the selected category. For example, if you selected *Time* and *Upload*, only connectors related to invoice integrations and uploads display. You can filter the list to view *All*, *My Connectors*, and *Available Connectors*. For more information on these options, see Connector Integration Details [page 33].

Choose the connector name hyperlink of any disabled (status Off) connector. The connector opens on the Integrations page.
Choose *Enable*. The *Welcome* step opens in the setup wizard. To continue enabling the connector, go to Welcome Step [page 13].

3. The *Enable Connector Details* dialog box displays the details of the selected connector and any available variants. The variant feature allows you to create a copy of a connector and modify the details; it's often used to send data to multiple receiving systems.
   Do one of the following:
   1. To choose the current standard connector, on the *Enable New Connector* tab, choose *Enable*. The *Welcome* step opens in the setup wizard. To continue enabling the selected connector, go to Welcome Step [page 13].
   2. To choose an existing variant or create a new one, choose the *Select Existing Variant* tab, enable the option for the variant to select, and then choose *Edit*.
      The variant opens on the connector Integration page. Choose *Enable*. If the variant is already turned on, you can edit it or create a new variant in the setup wizard. To continue, go to Welcome Step [page 13].

3.2.3 Continue Setup: All Other Connector Categories

Describes how to locate a connector after choosing a connector category other than Worker and Work Order or Time.

After choosing a connector category other than Worker and Work Order or Time, proceed with this task to browse for a connector to enable.

1. In the *Enable Connector* dialog box, choose *Browse Catalog*.
   The Connector List page opens in the Connector Catalog, filtered to the connector category you selected. For example, if you chose *User*, only the connectors related to user integrations display.
2. Locate a connector, and then choose the connector name hyperlink.
   The connector Integration page opens.
3. On the top-right side page, choose *Enable*.
   The *Welcome* step opens in the setup wizard.
4. To continue enabling the connector, go to Welcome Step [page 13].

3.2.4 Welcome Step

Describes how to continue connector setup in the *Welcome* step of the Connector Wizard.

After selecting a connector in the decision tree or on the connector Integration page, the *Welcome* step opens in the setup wizard. The wizard provides an intuitive framework for completing all other connector setup.

The *Welcome* step is the starting point for enabling and configuring a connector in the setup wizard. At the top of the page, a progress bar indicates the completion status of the required steps. The setup sections display in the pane on the left side.

1. Choose *Let's Get Started*.
   In the *Configure* section, the *Enable* step displays.

2. To continue, go to Configure Step [page 14].

3.2.5 Configure Step

Describes how to enable a connector in the Connector Wizard, define connector specifications, and set up header values and security.

In this section, the *Enable* and *Setup* steps are required to successfully enable a connector for use with the minimum specifications.

After completing the required steps, the connector will be available for use in your company, in *Admin Configuration > Integration > Download Data or Upload Data*.

The optional steps in this section are *Header Values* and *Security*. Some optional steps are related to the connector type (upload or download) and are noted as such, where applicable.

To continue, go to Enable Connector [page 14].

Enable Connector

In this step you turn on (enable) a connector, configure the connector details, and make it ready to use in your company. The wizard guides you through the steps required to complete the process.

To enable the connector:

1. In the *Enable* fields, enter/select the values as described in the following table.
2. When finished, choose *Next Step*.
   The *Setup* step displays. To continue, go to Setup Connector Details [page 15].

Enable Connector Field Descriptions

Field Name	Description
Connector Name	Name of the connector. The connector name defaults when selected in the decision tree or on the Integration page. If the connector name already exists, you're prompted to enter a new name.
Description	Displays a default description of the connector, if one was entered. You can also add a custom description for each connector variant. Both the default description (if available) and custom description display on the connector Integration page.
Version	Version of the connector. The default value is the most recent version of the connector. Required for upload connectors only.
Accessible	Allows restricting user groups that can access the connector. Options are: All Users, Buyer Users Only, list of MSP companies within the buyer (MSP Users – MSP company code). For example, 'MSP Users - M990' and 'MSP Users - V228'.

Field Name	Description
Upload Record Limit (optional)	When enabling an upload connector, you can optionally edit the upload record limit. When enabling an upload connector for the first time, the default upload record limit for API and API-A versions is 10,000 and is editable to a maximum limit of 1,000,000 for API and 10,000,000 for API-A. The default upload record limit for Bulk-Full and Bulk-Delta versions is 10,000,000 and is noneditable (technically, there's no record limit for Bulk uploads). **Note** For Bulk-Full, the `Max Allow Deletion Percentage` field allows you to alter the percentage of records that can be deleted from a single bulk-full upload. This is used as a safeguard to prevent unintentional deletions caused by partial files or other errors. Successful edits to the field are updated on the connector Integration page and an entry is created in the modification log.
Integration System	Integration system to be used for the data transfer. Required for upload and download connectors.

Setup Connector Details

In this required step you can configure delimiters (field separators), data formats, date formats, preprocessors, volume thresholds, and success/failure email notifications for connector uploads and downloads.

To set up the connector details, in the *Setup* fields, configure the field values as described in the following table.

Note

You can change these values when enabling or editing a connector.

Setup Field Descriptions

Field Name	Description
Delimiter	Delimiter used to separate fields in data transfer. Comma (,) is the default value. Options are: “,”, “&”, “;”, “\t” “|” “~”
Encoding	Options are ISO-8859-1 and UTF-8. Default value is ISO-8859-1. Optional for upload connectors only.
Asynchronous?	Asynchronous allows you to send or receive large files later. It's suitable when the upload or download transfer request is complex and takes longer to complete. Valid for uploads and downloads. Options are Yes or No.

Field Name	Description
Upload Data Format	Specify the format of data in an upload file. Displays for upload connectors only. Options are CSV, XML, or JSON. CSV is the default value. Input is optional. For CSV upload connectors, XML format isn't applicable, so the option doesn't display. Only CSV and JSON options are applicable, with CSV being the default. For XML upload connectors, CSV format isn't applicable, so the option doesn't display. Only XML and JSON options are applicable, with XML being default. For JSON upload connectors, currently there are no preprocessors to convert XML format to JSON format, thus the Upload Data Format field doesn't display. If the data format is updated, an entry is made in the Modification Log, which you can view on the connector Integration page.
Download Data Format	Specify the format of data in a download file. Valid for CSV download connectors only. Input is optional. CSV is the default value. Then, depending on the Download Data Format selected, the corresponding post-processor defaults for the connector (CSV to JSON or CSV to XML). If the data format is updated, an entry is made in the Modification Log, which you can view on the connector Integration page.
Date Format for Date Fields (optional)	Allows you to set the date format at the connector level for all date fields in a connector or connector variant download. The default value is blank. The date format options are: mm/dd/yyyy dd/mm/yyyy yyyy/mm/dd yyyymmdd If the date format isn't changed, then each date field retains the format based on the column definition for that field. If the date format is changed, an entry is made in the Modification Log, which you can view on the connector Integration page. **Note** You can also set the date format at the field level for date fields in a connector or variant download. The format set at the field level takes precedence over the format set at the connector level. For more information on this option, see Configure Fields for Connector Downloads [page 20].

Field Name	Description
Enable Delta Compare (optional)	When enabling or editing a connector download, this option allows you to enable and manage the delta compare functionality for supported connector downloads. Valid options are Yes (enabled) and No (disabled – default value). If you select *Enable Delta Compare Fields*, the *Define Delta Compare Fields* dialog box displays. Initially the delta compare fields option is set to `'All enabled columns Defaulted as Delta Compare fields'`, meaning all columns will be compared against. You can clear the '`All...`' setting and select only the fields that you want to compare against. Then select *Update* to save the selections or select *Cancel* to exit the changes. When enabled, you can configure the download to pull records only when the values of selected fields change. You define the delta compare fields on the Connector Details page. Click the *Actions* button to display the *Define Delta Compare Fields* and *Truncate Delta History Table* options. For more information, see Connector Integration Details [page 33].
Pre-Processors	After selecting an upload data format, the *Pre-Processors* option allows you to accept data in the format specified in the preprocessor. The options don't display if there are no preprocessors available or if all available preprocessors are added already. To add a preprocessor, choose *+Add Pre-Processor* and select an option from the list. For multiple preprocessors, select in the order noted in the setup document from your SAP Fieldglass representative. To remove a pre, choose *X* next to the entry. You can view the enabled preprocessors for a connector on the *Details* tab when viewing the connector details.
Duplicate File Check	When enabling or editing an upload connector, the *Duplicate File Check* field prevents processing the same file again, which helps prevent performance issues. If the exact file is loaded again, an error displays stating it has already been used. Displays for upload connectors only. The field is enabled by default. Input is optional.
Set Run Date (GMT) YYYY-MM-DD HH:MM: SS	When enabling a download connector or creating a variant of a download connector, you can set the last run date in the specified format. This is a mandatory field. The default field value is 6 months before the current date stamp. All records added or modified since the specified dates are processed. If the date specified is greater than a year, a message warns that the download could run into timeout issues because of the volume of records. Future dates aren't supported. All successful edits to the field create an entry in the modification log. **Note** You can also edit the last run date for a download connector on the connector Integration page. In the *Actions* list, choose *Edit Last Run Date*. The *Edit Last Run Data (timezone)* dialog box opens. Enter a new value in the *Last Run Date* field, and choose *Update*.

Field Name	Description
Email Recipients on Success	Email addresses of recipients to notify on successful file transfers. Separate multiple addresses by a comma.
Email Recipients on Failure	Email addresses of recipients to notify on failed file transfers. Separate multiple addresses by a comma.
Email notification preference when no data is downloaded	If a download connector doesn't return any data, this field determines whether email notification is to be sent and to whom. By default, email notification is sent to the recipients included in the *Email Recipients on Failure* field. Select one of the following options: • Send to recipients included in "Email Recipients On Failure". This is the default value. • Send to recipients included in "Email Recipients On Success". • Send no email notification. When this field is changed, an entry is made in the Modification log. This field and the selected value display on the connector Integrations Detail page.
Max Allow Delete Percentage	Alters the percentage of records that can be deleted from a single bulk-full upload. This is used as a safeguard to prevent unintentional deletions caused by partial files or other errors. 10% is recommended. Input is optional.

The minimum setup required to use the connector is now complete. Proceed as follows:

- To continue with optional connector setup, choose *Next Step*.
  - If enabling an upload connector with a version of API, the *Header Values* setup step opens. To continue, go to Header Values [page 18].
  - If enabling a download connector or non-API upload connector, the *Security* setup step opens. To continue, go to Security [page 19].
- To bypass optional setup, click *Next Step* until you reach the *Finished* step. For more information, go to Finished Step [page 31].

Header Values

In this step, you can define header values for API version upload connectors. The visible fields in the *Header Values* dialog box vary based on the type of upload connector.

File headers can be defaulted if not presented in the file received.

To define header values in the file:

1. In the *Header Values* dialog box, enter/select the field values as described in the following table.
2. When finished, choose *Next Step* to open *Security* setup.

Header Values Field Descriptions

Field Name	Description
Language	Language to be used in the file. The list includes all languages supported in SAP Fieldglass. Default value is the company default.
Submit	Options are True and False. Default value is False.
Number Format	Number format to be used in the file. The list includes all number formats supported in SAP Fieldglass. Default value is the company default. If not specified, the default is based on the company configuration.
Date Format	Date format to be used in the file. The list includes all date formats supported in SAP Fieldglass. Default value is the company default. If not specified, the default value is MM/DD/YYYY.
Transaction	Determines how record errors are handled. Options are True and False. True means if any record errors, the entire upload fails. False means if only records that are in error fail, remaining records are committed successfully. If not specified, the default value is False.
Send Notification	Determines whether normal messaging workflow is allowed. Options are True and False. If not specified, the default value is True.
Approval Required	Determines if objects are required to go through an approval process. Options are True and False. If not specified, the default value is True.
Comments	Comment field containing text notes about the upload file.

Security

In this optional step, you can define security and encryption values to protect the data as it's transmitted, and specify whether to archive the data.

To define security and archive values:

1. In the *Security* fields, enter/select the field values as described in the following table.
2. When finished, to continue with the *Customize* step, choose *Next Step*, or to continue with the *Transfer Method* step, choose *Skip Customize*.

The following table describes required fields, optional fields, and any applicable rules.

Security Field Descriptions

Field Name	Description
Sensitive Data	Determines whether the file contains sensitive data. Applies to upload and download connectors. Options are Yes and No. Default value is No. If you set the value to Yes, then only users with the corresponding flag on their user profile (or the associated user role) can retrieve the contents of it.
Archive Data	Determines whether to archive data. Applies to upload connectors only. Options are Yes and No. Default value is Yes.
Enable connector to be used through user interface?	Determines whether the connector can be used through the SAP Fieldglass user interface. Applies to uploads and downloads. Required field. Options are Yes and No. Default value is Yes.

3.2.6 Customize Step

Describes how to configure fields and custom features in a download file, and how to upload column transforms in an upload file.

You can customize a connector to add fields to the file, rename individual field names, and apply custom features and templates that modify the data in the file. The custom options are based on the connector type.

To continue, go to Configure Fields for Connector Downloads [page 20].

Configure Fields for Connector Downloads

Describes how to configure fields, add native fields, add custom fields, and combine custom fields in a connector or connector variant download.

Based on the connector type, the following custom options are available:

- Modify the properties of fields in the file.
- Combine multiple custom fields and pull data into one combined field.
- Add or remove native or custom fields.
- Change the order of columns.
- Change the format of fields.

These features apply to download connectors being enabled or already enabled. To customize the fields in a connector that's already enabled, see Edit Connector [page 38].

> **Note**
>
> With reference to MSP vs. Non-MSP supplier data, currently, an MSP supplier running a worker download can see worker data across all their associated suppliers.
>
> Non-MSP suppliers have visibility to only the data that belongs to them. A custom field added by a supplier to any module is only visible to that supplier when customizing a Standard Worker Download connector.
>
> MSP suppliers have visibility to the data of their associated non-MSP suppliers, but only to native field values. MSP suppliers can't view custom fields of non-MSP suppliers and vice versa.

Configure and Customize Fields

The *Configure Fields* table displays in the *Customize Fields* section.

1. To customize fields in the connector download, in the *Configure Fields* table, proceed as follows:
    1. To move the position of a row, on the left side of the row drag the  icon to the new position. To save the change, choose *Save Column Order*. (The button is disabled until the position of a row is modified.)
    2. To remove a column, choose *X* at the end of the column row. When you delete a column, it's removed from the download file. To confirm the delete action, choose *OK* in the *Confirmation* dialog box.
    3. To change a column name, select the check box in front of the column name, and then choose the column name hyperlink. In the *Edit Column <Column Name>* dialog box, enter the new column name, and then choose *Update*.
    4. To change the date format at the field level for any native date field, optional date field, or a date field added through a feature or a custom field, select the column name.
    The *Edit Column Date* dialog box opens.
    Proceed as follows:
        1. In the *Conversion Format Type* list, select either `Date` or blank value. The default value is `Date`.
        2. In the *Select Date Format* list, select one of the following formats.
            - mm/dd/yyyy
            - dd/mm/yyyy
            - yyyy/mm/dd
            - yyyymmdd

            The default value is blank. If the date format isn't changed, then each date field retains the format based on the column definition for that field. If date format is changed, an entry is made in the Modification Log, which you can view on the connector Integration page.
        3. Choose *Update*.

    > **Note**
    >
    > You can also set the date format at the connector level, which allows you to apply the same format to all date fields in the connector or variant. The format set at the field level takes precedence over the format set at the connector level. For more information, see Setup Connector Details [page 15].
2. When finished configuring fields, choose *Save Column Order* (above *Column Name*).
3. To add native fields to the file, continue with the next task, or to finish, choose *Next Step*.

Add Native Fields

Download files include many native fields preconfigured by SAP Fieldglass. This feature allows you to add other related preconfigured fields to a download file.

1. To add native fields to a file, in the *Configure Fields* table, choose *+ Add Native Fields*.
   The *Add Default Fields to Connector* dialog box opens.
2. The list displays all native fields across all modules. Select the check boxes next to the fields to add, and then choose *Add Selected Fields*.
   The selected fields are added to the *Selected Fields* in the table.
3. To remove a native field, choose *X* to the left of the field.
4. To add selected fields to the download file, choose *Add*.
5. To add custom fields to the file, continue with the next task, or to finish customizing native fields, choose *Next Step*.

Add Custom Fields

You can create custom fields for many SAP Fieldglass modules to capture additional information that standard fields don't capture. For example, you could create custom fields to ask how many hours per week a candidate would like to work or to collect more detail about the work logged on a time sheet. In addition to displaying information in the user interface, custom fields can be used in integrations, reporting, and messages.

Custom fields offer flexibility in several areas:

- They can be mandatory, optional, or read-only.
  - Read-only custom fields allow you to store information for use in reports without making that information editable. You can also set up a read-only field so that it's hidden from users.
- Some custom fields can be associated to a specific object, such as a Business Unit, or can be made visible only to certain user types.
- Some custom fields allow linking, where the value captured on one module can be passed to another module in the workflow. (For example, a value captured on a job posting can be passed to a job seeker, and then to a work order.)

1. To add custom fields to a download file, in the Configure Fields table, choose *+ Add Custom Fields*.
   The *Add Custom Fields to Connector* dialog box opens.
   You can filter the list of native fields by module and visibility rule.
2. In the *Modules* list, select the module that needs the custom field. The available modules vary based on what features your company has enabled. Once you choose a module, the field is locked and your choice determines the other fields you need to complete. Based on the module you choose, you can choose one of several data types.
3. In the *Visible To* list, choose the user types who can view the custom field.
4. Select the check boxes next to the fields to add, and then choose *Add Selected Fields*.
   The fields display in the *Selected Fields* section in the table.
5. To change the column name, enter the new name in the *Custom Label* field.
6. To add one or more custom fields, choose *Add*.
   The Configure Fields table displays. The new custom fields display at the bottom of the table. The *Type* field defaults to `Enable by ID` for any custom fields and can't be changed.
7. To combine custom fields, continue with the next task, or to finish customizing fields, choose *Next Step*.

Combine Custom Fields

You can combine two or more custom fields that have the same *Enabled by* value. You can also sort the fields in the order that you want them to take priority over other fields.

Combining custom fields is primarily used when you have the same custom field on multiple modules and you want to check multiple modules to see if any of them are populated. The way it works is you add the custom fields and then sort the fields in the order of priority you want. For example, if you want to check WOR module

first, WO second, and then SOW Worker last, then sort them in that order and save the sort order. Then check the box next to the custom fields you want combined into one field, and select *Combine Custom Fields*.

For example, if you're only pulling from the WO and SOW Worker modules, if the download returns a contingent WOR the field would be blank because WOR is a separate module than WO. In this case, consider adding WOR custom fields as well, unless you only want WO and SOW Worker.

When combining custom fields, be sure to combine fields across all SOW, Contingent, WO, and/or WOR modules, as applicable to your use case.

1. To combine custom fields in a file, in the *Configure Fields* table, select the check boxes next to the custom fields you want to combine, and then choose *Combine Custom Fields*.
   The *Combine Custom Fields* dialog box opens.
2. In the *Name* * field, enter the new name for the combined custom field.
3. Choose *Add*.
   The new combined field displays at the bottom of the table. The *Type* field defaults to `Combined Custom Field`.
4. Choose *Next Step*. The *Available Custom Features* section opens. To continue, go to Configure Custom Features for Connector Downloads [page 23].

Configure Custom Features for Connector Downloads

Describes how to enable and disable custom features for connector downloads.

If no custom features are available, the *Available Custom Features* table is empty and a message displays: `No data to display.`

If a connector is already customized through a feature, enabling a new feature or re-enabling the current feature deletes all customizations applied through the current feature before the new customizations are applied. In addition, disabling a currently enabled custom feature deletes all customizations applied through that feature.

> **Note**
>
> To enable or disable custom features for a connector that is already enabled, on the Connector List page or Connector Catalog page, select the connector. On the connector Integration page, choose the *Available Custom Features* tab, and then choose *Edit* to open in the connector in the setup wizard. For more information, see Edit Connector [page 38].

1. To enable/disable custom features, in the *Available Custom Features* table, proceed as follows:
   1. To enable a new custom feature or re-enable an existing custom feature, select the option next to the custom feature, and then choose *Enable* (the button is unavailable until you select a feature). To confirm the action, choose *OK* in the *Confirmation* dialog box. To cancel the action, choose *Cancel*.
   2. To disable a custom feature, select an enabled custom feature, and then choose *Disable Current Feature* (the button is unavailable until you select an enabled custom feature). To confirm the action, choose *OK* in the *Confirmation* dialog box. To cancel the action, choose *Cancel*.
2. To proceed with the *Transfer Method* step, click *Next Step*, and then go to Connectivity Transfer Method Step [page 26].

Configure Column Transforms for Connector Uploads

Describes how to modify the data in an upload file by adding and editing fields, and using column transform templates.

This feature can be used to update the first three characters of a field in the upload file or to concatenate two fields into a new third field.

The following options are available for upload connectors:

- Add/Edit Native Fields
- Add Additional Fields
- Apply an Upload Column Transform Template
- Disable an Upload Column Transform Template

> **Note**
>
> To upload column transforms for a connector that is already enabled, on the Connector List page or Connector Catalog page, choose the connector to open it on the connector Integration page, and choose click the *Upload Column Transform* tab. Choose *Edit* to open the connector in the setup wizard. For more information, see Edit Connector [page 38].

Edit/Remove Columns

On the Configure Column Transformation page, existing column transformations display in the *Configured Column Transformation* section.

1. To edit or remove columns, proceed as follows:
    1. To edit a column transformation, choose the column name hyperlink. The *Column Transformation* dialog box opens. Change the *Standard Column Name*, *File Column Name*, *Default Value*, and *Skip on update* fields as needed, and then choose *Update*. For a description of the fields, see the following table of field descriptions.
    2. To remove a column, choose *X* at the end of the row.
2. To add/edit native fields, continue with the next task, or to continue with the *Transfer Method* setup, choose *Next Step*, and then go to Connectivity Transfer Method Step [page 26].

The following table describes the required fields, optional fields, and any applicable rules.

Column Transform Field Descriptions

Field Name	Description
Standard Column Name	When adding a native column, you can select a field from the drop-down list. *Standard Column Name* refers to the native column name of the upload. When adding an additional field, you must enter the name of the additional column in the standard SAP Fieldglass format, such as [c] Custom Field, [SA] Signature Authority. *Standard Column Name* must be the first field completed.
File Column Name	New name of the column header. The *Standard Column Name* maps to the *File Column Name*, if defined.

Field Name	Description
Default	The initial value for the field. Enclosing quotes aren't required.
Skip on update	Select this option to add the column value on the initial connector update and skip the column on subsequent updates.

Add/Edit Native Fields

The value of each native field can be modified or mapped to a new column.

1. To add or edit native fields, on the Configure Column Transformation page, click *+ Add Native Fields*.
   The Column Transformation dialog box displays.
2. Choose a *Standard Column Name* from the drop-down list. The list displays all native fields, including any fields modified previously.
3. Enter/select the other the values based on the field descriptions described in the Transform Column Field Descriptions table.
4. Choose *Update*.
5. To add additional fields, continue with the next task, or to proceed to the *Transfer Method* setup, choose *Next Step*, and then go to Connectivity Transfer Method Step [page 26].

Add Additional Fields

Any non-native fields not defined in the original upload file can be added to the file. The new fields are formatted as hyperlinks.

1. To add additional fields, on the Configure Column Transformation page, choose *+ Add Additional Fields*.
   The *Column Transformation* dialog box opens.
2. Enter/select the values based on the field descriptions described in the Transform Column Field Descriptions table.
3. Choose *Update*.
4. To apply an upload column transform template, continue with the next task, or to proceed to the *Transfer Method* step, choose *Next Step*, and then go to Connectivity Transfer Method Step [page 26].

Apply Upload Column Transform Template

Enabling a column transform template transforms upload columns based on the template layout. Column transform templates allow you to make standardized customizations to connectors by defining a set of fields that you apply to one or more connectors. Once enabled, the template is added to the connector.

You can't create new templates, but once a template is enabled, all fields in the template display along with the manually transformed fields. The template fields can be identified by the flag, `Template Enabled`.

1. To apply an upload column transform template, on the Configure Column Transformation page, choose *+ Apply Template*.
   The *Apply Upload Column Transform Template* dialog box opens.
2. In *Name* list, choose an upload column transform template.
   The *Description* field updates automatically.
3. To apply the template, choose *Enable*.
   The template fields display in the *Configured Column Transformation* section.
4. To disable a column transform template, continue with the next task, or to finish uploading column transforms, choose *Next Step*, and then go to Connectivity Transfer Method Step [page 26].

Disable Column Transform Template

Disabling a column transform template removes all fields inserted or created by the template.

1. To disable a column transform template, on the Configure Column Transformation page, choose *Disable Template*.
2. To confirm the action, choose *OK* in the *Confirmation* dialog box.
3. To proceed to the *Transfer Method* step, choose *Next Step*, and then go to Configure Column Transforms for Connector Uploads [page 24].

3.2.7 Connectivity Transfer Method Step

Describes how to create an end point and subscription for SFTP, and how to set up Web Services transfer methods.

The transfer method defines the technical details for how an integration file is transferred between SAP Fieldglass and the third-party systems you manage. In this section, you can set up SFTP subscriptions or web service transfer methods.

To define connectivity details:

1. In the Connectivity step, choose one of the following *Transfer Method* options:
   - *Subscription* (described in the next section)
   - *SAP Fieldglass SOAP Web Service*
   - *Manual* (use to disable a subscription)
2. Choose *Next Step*.
3. Proceed as follows:
   1. If you chose *Subscription*, the *Configure End Point* step opens. To continue, go to End Point Setup [page 26].
   2. If you chose *SAP Fieldglass SOAP Web Service*, the *Setup Web Service* step opens. To continue, go to Web Service Setup [page 29].
   3. If you chose *Manual*, the *Finished* step displays. To continue, go to Finished Step [page 31].

End Point Setup

Describes how to create a new end point and how to use an existing end point, and then test the end point.

After choosing the subscription transfer method in the previous step, the *Configure End Point* step opens.

At least one end point must be in place for the subscription transfer method to work. The End Point List page contains a list of all existing end points. If an end point exists with the connector name, it's preselected in the *End Point List* drop-down and can then be submitted for update. If not, you can create a new end point and submit it.

The following tasks explain how to create a new end point and how to use an existing end point, as well as how to test the end point connectivity. You can also create end points directly from the dashboard; for details, see End Points [page 65].

Create a New End Point

1. In the *Create End Point* step, choose *Create New*.
   The *Create End Point* step opens.
2. Specify the end point details. For information on the properties, see the property descriptions in Create End Point [page 66].
3. To test the end point connectivity, select the *Test Connectivity* button. The results display in a *Success* or *Failure* dialog box.
4. After testing the end point details, choose *Submit*.
5. Choose one of the following:
   1. To continue with the subscription setup, choose *Next Step*. The *Setup Subscription* step opens. Go to Subscription Setup [page 27].
   2. To return to the *Configure End Point* step without retaining any changes, choose *Cancel*.

Use an Existing End Point

> **Note**
>
> Newly added end points don't display in the *End Point* list until SSH (Secure Socket Shell) authentication information gets added by the SAP Fieldglass administrator.

1. To use an existing end point, choose the end point in the *End Point* list, and then choose *Next Step*.
   The *Edit End Point* setup displays.
2. To edit the end point values, make any necessary changes, and then choose *Update*.
3. After changing or creating an end point, it's important to test connectivity to the target end point server. To test the end point, choose the *Test Connectivity* button. The test runs, and then returns either a success message or a failed message. If the test is successful continue with the next step, if the test is unsuccessful, resolve the issue and try again.
   Note that you can also test the connectivity after creating or editing an end point.
4. Do any of the following:
   1. To return to *Configure End Point* setup without retaining any changes, choose *Cancel*.
   2. To continue with the subscription setup, choose *Next Step*. The Setup Subscription step opens. Go to Subscription Setup [page 27].

Subscription Setup

Describes how to set up a subscription for scheduling connector uploads and downloads.

A subscription consists of two parts – the configuration/scheduler, which is referred to as the subscription, and the transfer method details (host, username, and so forth), which are referred to as the end point. The subscription contains the details of when the data transfer must run between SAP Fieldglass and the end point. The end point defines the properties of the server that SAP Fieldglass must communicate with to push or pull connector files.

The following tasks explain how to create a new subscription and how to use an existing subscription, as well as how to test a subscription.

Create a New Subscription

After selecting *Subscription* in the *Connectivity* step, the *Setup Subscription* step opens.

1. At the bottom of the page, choose *Create New*.
   The *Setup Subscription* dialog box opens.
2. Enter/select the following details:
   1. In the *End Point* list, choose the target end point for the subscription. A value is required.

      > **Note**
      >
      > Newly added end points don't display in the *End Point* list until SSH authentication information is added by the SAP Fieldglass administrator.

   2. In the *Subscription Class* field, the default value is `insite.subscription.WebserviceUploadSubscription`. You can leave the default value or enter any special subscription class value provided by your SAP Fieldglass representative.
   3. In the *Parameters* field, enter one or more parameters to pass in the subscription. Valid for uploads and downloads. If only one parameter is required, specify that value. If multiple parameters are required, specify the values separated by a comma with no space in between. For example, if parameters are Start Date and End Date in mm/dd/yyyy format, then specify the values as: 01/01/2020,12/31/2020. Parameters are used by some integration connectors to disposition objects in SAP Fieldglass. For example, the Invoice Buyer Download requires a parameter be set to disposition the invoice record to 'Payment Pending' or 'Paid' when the download runs. The parameter indicates what status the invoice should be changed to after downloading so it's not downloaded again – parameter 33 sets the status to 'Payment Pending'; parameter 52 sets the status to 'Paid'. To determine if a connector requires parameters, see the connector specification documents in the SAP Fieldglass Connector Library.

      > **Note**
      >
      > You can view parameters defined for a subscription on the connector Integration page. Choose the *Connectivity* tab, and in the *Subscription Name* section, the parameters display under *Details*.

   4. In the *Subscriber* field, click in the drop-down list and then choose a username. This is an optional field.
   5. In the *Notify On Missed Run*, check yes, if you want to be notified if a subscription fails to run. This is an optional field that's only visible if your company code has been added to the *FG_SUBSCRIPTION_ALERT* Feature Toggle.
   6. In the *Notification Email* field, enter an optional email address to send transfer status notifications (success or failure).
   7. In the *Delivery Time* section, choose values for *Minute*, *Hour*, *Date*, *Month*, and *Day* to schedule the delivery of the subscription. Values are required.
      As you choose options, a description of the runtime displays in an information box. For example:
      `At minute 0 past hour 2 on day-of-month 5 and on Sunday in every month`
      As you change the delivery time, the description changes in real time.
   8. In the *Time Zone* list, choose the time zone where the subscription runs. A value is required.
   9. Choose a *Status* option. The subscription and end point must be active to test or run.
3. Do either of the following:
   1. To create the subscription, choose *Save*.
      The subscription is added to the system. After the Setup Subscription page refreshes, the new subscription displays in the *Select Subscription* list. Choose *Next Step*. The *Finished* step opens. To continue, go to Finished Step [page 31].
   2. To cancel the action and return to the previous page to select an existing subscription, choose *Cancel*. In the *Confirmation* dialog box, choose *OK*.

Use an Existing Subscription

Existing subscriptions display by name in a list on the Setup Subscription page. The subscription status also displays.

1. To select an existing subscription, choose the subscription name hyperlink.
   The *Setup Subscription* dialog box opens.
2. Change the values for *End Point*, *Parameters*, *Subscriber*, *Notification Email*, *Delivery Time*, and *Time Zone* as needed. For a description of the fields, see *Create a New Subscription* above.
3. Do one of the following:
   1. To activate the subscription, choose *Enabled* (only displays for disabled subscriptions), and then choose *Save*.
      The subscription is activated in the system. The Setup Subscription page refreshes, and the active subscription displays in the list. Choose *Next Step*. The *Finished* step opens. To continue, go to Finished Step [page 31].
   2. To deactivate the subscription, choose *Disabled* (only displays for enabled subscriptions).
      The subscription is deactivated in the system. The Setup Subscription page refreshes and the inactive subscription displays in the list.
   3. To use the selected subscription, choose *Submit*. The *Finished* step opens. To continue, go to Finished Step [page 31].
   4. To cancel the action and return to the previous selection page without saving details, choose *Cancel*. In the *Confirmation* dialog box, choose *OK*.

Test Subscription and End Point

> **Note**
>
> The connector, end point, and subscription must be enabled before you can test the subscription.

To test the connectivity of a subscription and endpoint, do the following:

1. On the dashboard, choose *View Connector*. The Connector List page opens.
2. Choose the connector. The connector Integration page opens.
3. Choose the *Connectivity* tab. All subscriptions defined for the connector display by name in the list.
4. Choose the subscription you want to run. The subscription details display in the preview pane below.
5. Choose *Run Now*. The *Confirmation* dialog box opens.
6. Choose *OK* to run the subscription now. The following message should display:
   `The subscription run was triggered successfully. Please check the Integration Audit Trail for more details.`
   You can also view subscription activity from the **Monitor Activity** tile on the dashboard, which displays all activities for the selected subscription. For more information, see Monitor Activity.
   From this point forward, the subscription runs based on the delivery time established.

Web Service Setup

Describes how to set up credentials for the Web Service transfer method.

After selecting *SAP Fieldglass SOAP Web Service* in the *Connectivity* step, the *Setup Web Service* step opens.

A license is required to use the web service. If you have an existing license it displays in the table; otherwise, the table displays the message: `No items found`. If no license is found, contact your SAP Fieldglass representative.

The web service uses the *SAP Fieldglass Web Service Technical Specification*, a proprietary, Web Service Description Language (WSDL) document that allows clients to download and upload data seamlessly between the application and a client system.

> **Note**
>
> To access and download the WSDL document from within the application, on the Setup Web Service page, click the blue '*here*' hyperlink. You can also access the WSDL document from https://help.sap.com/docs/SAP_FIELDGLASS_INTEGRATION/19bd369173524cacb58b6a2b0ca91bab/631753725a744d91905fff0e4e939cf1.html.

The following tasks explain how to create a new license key and how to use an existing license key.

Create a New License Key

If there are no existing licenses, the *License Key* table is empty.

1. To generate a license key, choose *Create New*.
   The page refreshes with new fields.
2. In the *Virtual Person Name (Username)* list, choose a value to generate the license key for.
   The field populates with a copy of the selected username.
3. Do either of the following:
   1. To save the license key and username details, choose *Submit*.
      The new license key displays in the table. To continue, choose *Next Step*. The *Finished* step opens. To continue, go to Finished Step [page 31].
   2. To cancel the action and return to the previous selection page, choose *Cancel*. In the *Confirmation* dialog box, choose *OK*.

Use an Existing License Key

If the system finds an existing license, the license key value displays as a hyperlink in a table on the page.

1. If the license key *Status* is Active and the details are correct, choose *Next Step*. The *Finished* step opens. To continue, go to Finished Step [page 31].
2. To edit the details of the license key, choose the license name hyperlink.
   The *Edit Details* dialog box opens.
3. Do either of the following:
   1. To choose a different username, choose a value in the *Virtual Person Name (Username)* list. To change the *Status*, choose *Enabled* or *Disabled*, as needed, and then choose *Save*. The Setup Web Service page displays. Choose *Next Step*. The *Finished* step displays. To continue, go to Finished Step [page 31].
   2. To cancel the action and return to the previous selection page, choose *Cancel*. In the *Confirmation* dialog box, choose *OK*.

3.2.8 Finished Step

The *Finished* step confirms that the connector is enabled with the minimum requirements and any optional setup, if chosen. You can begin using the connector in your company.

Proceed as follows:

- To go to the Self-Service Dashboard, choose *Go to Dashboard*.
- To view the details of the connector on the Detail page, choose *Go to Detail*. Go to Connector Integration Details [page 33].

3.3 Connectors

Describes the Connector List page and how to view and manage enabled connectors.

The *Connectors* tile on the dashboard (visible when at least one connector is enabled) opens the Connector List page. The Connector List page is a tabbed interface that provides connectors in two groups:

The *Company Connectors* tab is the default view. You can view and edit the details of enabled connectors, as well as view and enable previously enabled connectors.

The *Connector Catalog* tab is an alternate view that allows you to view, enable, and edit the details of all connectors in the following groups:

- *All* displays connectors that are enabled, never enabled, enabled and then disabled (status varies).
- *My Connectors* displays connectors that are currently enabled (status On) or previously enabled (status Off). This is the same list as in the *Company Connectors* tab noted above.
- *Available Connectors* displays connectors that are available to be enabled (status Off).

On either tab, you can choose a connector name hyperlink to open the connector on the Integration page. The Integration page displays all configuration values defined for the connector. It also displays the actions you can take to update the connector. For more information, see Connector Integration Details [page 33].

Company Connectors

The following actions are available on the *Company Connectors* tab:

- To filter the page content, enter criteria in the *Connector Name* and/or *Variant* fields, and/or select options in the drop-down lists.
- To enable a connector that is currently disabled or edit an enabled connector, choose the connector name hyperlink to open it on the Integration page, and then choose *Enable* or *Edit*, respectively. For details, see Enable Connector [page 39] and Edit Connector [page 38].
- To quickly navigate to the audit trail details of a connector's most recent run, choose the hyperlink value in the *Last Run Date* or *Run Count* column in the connector name row.
- To save the page content in a CSV file, at the bottom of the page, choose the *Save as CSV* link.

The following table describes the connector details that display on Connector List page under the *Company Connectors* tab.

Connector List – Company Connectors Field Descriptions

Connector Name	Version	Variant	Status	Activity	Last Run Date	Run Count.	Sensitive Data	Accessible To
Name of connector, formatted in a hyperlink that opens the Integration page for that connector. Displays custom connector name, if it exists.	Version number of connector.	Variant number, if connector is a variant.	On Off	Upload Download	Value is a timestamp formatted in a hyperlink that opens the Audit Trail tab of the connector, filtered to the details of the selected run.	Value is a number formatted in a hyperlink that opens Audit Trail tab of the connector, filtered to the details of the selected run.	Yes No	All Users Buyer Users Only

Connector Catalog

To enable a connector that is currently off or edit a connector that is currently on, choose the connector name hyperlink to open it on the Integration page, and then choose *Enable* or *Edit*, respectively. For details, see Connector Integration Details [page 33].

Visible connectors are based on your user type. Note that you can also open the Connector Catalog from the decision tree in the Connector Wizard by choosing *Browse Catalog*.

The following table describes the connector details that display on the Connector List page under the *Connector Catalog* tab.

Connector List – Connector Catalog Field Descriptions

Name	Description	Category	Version	Activity	Status
Name of the connector, formatted in a hyperlink that opens the connector Integration page.	Description of the connector, which can be the default description and/or the custom description, if entered, for a connector variant.	Master Data Configuration Financial Data Invoicing Job Posting Projects (buyers only) Rate Structure Services Time Expense User Worker and Work Order	Version number of connector.	Upload Download	On Off

3.3.1 Connector Integration Details

The connector Integration page allows you to view and edit the configuration specifications of your company's connectors.

The connector Integration page is a complete self-servicing tool that provides a centralized location for viewing and editing connector specifications using a tabbed interface.

To view the detailed specifications of a connector, choose the *Connectors* tile on the dashboard, and on Connector List page, choose a connector.

At the top of the page, you can view the *Connector Name*, *Status* (On or Off), and the *Activity* (Upload or Download). You can also select the *Edit* button to open the connector in the Setup Wizard and change any details, or click the *Enable*/*Disable* button to change the status of the connector.

Connector Actions

You can invoke actions on connectors using the command buttons under the *Actions* tab on the right side of the page. The available actions are visible based on the connector type (upload or download) and status (enabled or disabled).

Connector Actions

Action	Description
Edit Last Run Date	To edit the last run date for a connector download, in the *Actions* list, choose *Edit Last Run Date*. The *Edit Last Run Date (timezone)* dialog box opens. Enter a new value in the *Last Run Date* field, and then choose *Update*. You can also edit the last run date when enabling a connector download or when creating a variant of connector download. For more information, see Edit Last Run Date [page 40]
Create Variant	Allows you to create a variant (copy) of an enabled connector. All fields are populated from the original connector and you can make changes as needed in the Setup Wizard. For more information, see Create Variant [page 40].
Define Delta Compare Fields	For connector downloads only, this option displays after you enable or edit a connector download and select the *Enable Delta Compare* option. (Not all downloads support this feature.) Allows you to configure the download to pull records only when the values of the selected fields change. Select *Define Delta Compare Fields* to select the fields. When Delta Compare fields are defined, the connector's Details page displays the fields in the bottom half of the page. For more information, see Setup Connector Details [page 15].

Action	Description
Truncate Delta History Table	When a download connector has 'Enable Delta Compare' enabled, a Delta History table is created and every time the download runs, it looks at this history table to compare and only pull records for which the selected field values have changed. If needed, you can truncate the Delta History Table so there is no data history to compare and thereby pull all the records. For example, a download is configured to pull worker records only if there's a change in a particular field. If 10 workers were downloaded in the last run and there's no change in that particular field for any worker, then the next run won't have any records. However, if the Delta History table is truncated, then all records meeting the connector logic will download in the next run. And then subsequent runs will compare with the history table and pull only those that have that field value changed. Invoking this option displays a confirmation dialog box with the message, `'Truncating the Delta History Table will impact download results'`. Select *Truncate* to invoke the action or *Cancel* to exit the action. An entry is made in the Modification Log when any Delta Compare functionality is modified.

Tabbed Views

Connector specifications display on tabs that are visible based on the connector type (upload or download) and status (enabled or disabled).

The following table describes tab names, descriptions, and related actions on the page.

Tab Name	Description
Details	The *Details* tab is the default view that displays for all connectors. When viewing connector details, the tab displays all configuration information defined for the connector in the setup wizard. Some of the details include connector name, last run date/time, company code, status, activity (upload or download), custom connector name (if applicable), connector setup details, upload record limit, and pre-processors (the first processor listed is the default). When the connector is enabled, the *View Guide* hyperlink allows you to download the Connector Specification document.

Tab Name	Description
Upload Column Transform	The *Upload Column Transform* tab displays for enabled upload connectors that are configured with upload column transform details. The tab displays the transformed column name, enabled template name (if applicable), standard column name, file column name, default value (if applicable), and whether it will be skipped on subsequent updates after the initial run. To edit or add upload column transform details, choose *Edit* at the top of the page. The setup wizard opens. Navigate to the *Customize > Upload Column Transform* section, and then make the changes. For more information, see Configure Column Transforms for Connector Uploads [page 24].
Connectivity	The *Connectivity* tab allows you to monitor the file transfer methods and integration activity for connectors with SFTP or web services configured. **Subscriptions** Each subscription displays the subscription name and status. To view the processing details for a subscription, select the subscription name. Information displays on the following tabs: • The *Details* tab displays the selected subscription name, end point name, parameters, subscriber, and notification email (if defined), and delivery times. • The *Modification Log* tab displays activity related to when the subscription was created, edited, enabled, and disabled, including when disabled because of a disabled connector or end point. Each log entry includes the activity, activity time, reason, and person responsible for the modification. If the connector is enabled, the *Run Now* button allows you to trigger a one-time run to test the subscription (the subscription and end point must be enabled). To run the subscription now, choose *Run Now*. The *Confirmation* dialog box opens. Choose *Yes* to confirm the action. The subscription runs once in the background. If the subscription run is successful, a confirmation message displays. You can view the subscription details in the *Integration Audit Trail* tab on the Connector Integration page. The *Status* column displays the status of the subscription, either active or inactive. **Note** The *Run Now* button is only visible when a connector is enabled. **Web Services** For web services, the *Partner Details* section displays the virtual person name (username), license, and status, either enabled or disabled, for each web service configured. To edit or add connectivity details, choose *Edit* on the Details page to open the setup wizard. Navigate to the *Connectivity > Transfer Method* section, and then make the changes. For more information, see Connectivity Transfer Method Step [page 26].

Tab Name	Description
Enabled Fields	The *Enabled Fields* tab displays for enabled download connectors. The tab displays the column (field) name, module, type (default, new, custom field enabled by ID or custom field enabled by name), and description. To edit and customize enabled fields, choose *Edit* on the Details page to open the setup wizard. Navigate to the *Customize* > *Configure Fields* section, and then make the changes. You can add/remove native and/or custom fields, combine custom fields, rename individual field names, and apply templates to modify the data in the file. For more information, see Customize Step [page 20].
Customizations	The *Customizations* tab displays for standard download connectors. The tab displays any custom features defined for the connector. Under the *Custom Columns List* (for definitions) or *Custom Conditions List* (for clauses), choose *View* to display the full definition and clause values. Under *Enabled Feature Details*, choose *Disable* to delete the custom feature details. A confirmation dialog box displays. Choose *OK* to disable the feature. An entry is made in the modification log. You can always re-enable the custom feature from the *Available Custom Features* tab. **Note** Disabling a current feature deletes all customizations defined for the feature.
Available Custom Features	The *Available Custom Features* tab displays for enabled download connectors. The tab displays all custom features that are available for the company to configure. To enable a custom feature, select the custom feature on the Details page, and then choose *Enable Custom Feature*. Confirm the action in the *Confirmation* dialog box. To disable a custom feature, select an enabled custom feature on the Details page, and then choose *Disable Custom Feature*. Confirm the action in the *Confirmation* dialog box. You can always re-enable the custom feature. If no custom features are available, the table is empty. For information on how to configure custom features in the setup wizard, see Configure Custom Features for Connector Downloads [page 23].
Integration Audit Trail	The *Integration Audit Trail* tab displays for all enabled and disabled connector types. The tab displays combined details from the subscription, integration, and data transport, as applicable to the connector in view. You can also navigate to this tab and view real-time activity from Connector List page, by choosing the value hyperlink in the *Last Run Date* or *Run Count* column.
Modification Log	The *Modification Log* tab displays for all enabled and disabled connectors. The tab displays a log of all changes that a CM or Company Admin made to a connector. Each log entry includes the activity date and time, reason for the modification, and person responsible for the modification.

Edit Connector

Describes how to edit the details of a connector.

Context

The *Edit* action is valid for all enabled connectors. When editing a connector in the setup wizard, since the connector is already enabled, lock icons don't display next to the setup sections.

> **Note**
>
> The *Edit* button is universal for all editing functions. The available edit actions are based on the connector type and status.

Procedure

1. On the top-right side of the connector Integration page, choose *Edit*.

   The connector opens in the setup wizard.
2. Navigate to the section containing the details you want to edit, and make the necessary changes.

   You can select any available section in the left navigation page to edit – you don't have to navigate step by step as is required when enabling a connector. Edited values are committed in place. For more information on editing a connector, see Connector Wizard [page 10].

   > **Note**
   >
   > - On the Setup page of download connectors, you can configure the precision for all *Amount* and *Rate* fields at the connector level. Additionally, precision can be enabled at the field level from the **Enabled Fields** page.
   > - When editing the following download connectors, you can use the *Enable Row Count Footer Flag (optional)* field, to include the row count of records at the end of the file:
   >   - Active Worker Download version 1.0
   >   - Job Posting Buyer XML Download version 1.0
   >   - Job Posting Template Download version1.0
   >   - Job Posting Template with Rate Lookup Download version 1.0
   >   - Worker Security Single Line Download version 1.0
   >   - Worker Security Single Line Download 1.1
3. To cycle through the setup wizard, choose *Next Step*, or to return to the dashboard, choose *Exit Wizard*.

Enable Connector

Describes how to enable a connector.

Context

When a connector is disabled, the connector status is 'Off'. The connector must be enabled before any other actions are allowed. Because a disabled connector was at one time enabled, any details previously configured are available for editing.

Procedure

1. On the top-right side of the connector Integration page, choose *Enable*.

   The connector opens in the setup wizard.
2. Edit the details as needed. The changes you make are committed in place. For more information on enabling a connector, see Connector Wizard [page 10].

   > **Note**
   >
   > When enabling the following download connectors, you can use the *Enable Row Count Footer Flag (optional)* field, to include the row count of records at the end of the file:
   > - Active Worker Download version 1.0
   > - Job Posting Buyer XML Download version 1.0
   > - Job Posting Template Download version1.0
   > - Job Posting Template with Rate Lookup Download version 1.0
   > - Worker Security Single Line Download version 1.0
   > - Worker Security Single Line Download 1.1
3. To cycle through the setup wizard, choose *Next Step*, or to return to the dashboard, choose *Exit Wizard*.

Disable Connector

Context

Describes how to disable a connector.

Use this action to disable (turn off) an enabled connector. After you confirm the delete action, the connector is disabled and no longer available to use in the company. The connector details are retained, including the Transfer Method (if set up), but any SFTP or web service subscriptions stop processing. If the connector is re-enabled, the retained details are available for editing.

Procedure

1. On the Connector List page, choose the connector you want to disable.
2. On the top-right side of the connector Integration page, choose *Disable*.

   The *Disable Connector* dialog box opens.
3. To confirm the delete action, choose *OK*.

Create Variant

Describes how to create a variant (copy) of a connector.

Context

This action is available for enabled connectors that require a variation (copy) of the existing connector. All fields are populated from the original connector.

Procedure

1. On the top-right side of the connector Integration page, click in the *Actions* list, and then choose *Create Variant*.

   The connector opens in the setup wizard.
2. Enable the new connector variant. Change the connector name to a unique name that isn't already being used. For example, you could append the name with a version or four-digit code. Change other values as needed.
3. To cycle through the setup wizard, choose *Next Step*, or to return to the dashboard, choose *Exit Wizard*.

Edit Last Run Date

Describes how to edit the last run date of a download connector.

Context

Certain download connectors look at the last run date and pull data created after that date. If needed, you can edit the last run date to bypass the date and pull older data.

For example, a worker download is configured to automatically download worker records once per week. The download pulls all workers created in the week by looking at the previous run date. To troubleshoot a download issue, you change the last run date to an older date, to download data as of that date.

Procedure

1. On the top-right side of the connector Integration page, click in the *Actions* list, and then choose *Edit Last Run Date*.

   The *Edit Last Run Date* dialog box opens.
2. In the *Last Run Date* field, enter the new date in the existing date format.
3. Choose *Update*.

   The date changes to the new value.

Reset Lastrun Table

Describes how to reset the Lastrun table for a bulk full upload connector or variant.

Context

On the Connector Details page of a bulk full upload connector or variant, you can force the next upload to process all records in the upload file.

Procedure

1. On the Connector List page, choose a bulk full upload connector or variant.
2. On the top-right side of the connector Integration page, click in the *Actions* list, and then choose *Reset Lastrun Table*.

   The *Edit Batch Job* dialog box opens.
3. To process all records in the file, choose *OK*.

   > **Note**
   >
   > If you choose the ARIBA Custom Pick List Upload connector or the Pick List Value Upload connector, the *Edit Batch Job* dialog box displays the *Select a Pick List* list of values that are specific to the buyer. Choose a pick list value, and then choose the *Reset Lastrun Table* button. A confirmation dialog box opens. To continue with the table reset, choose *OK*.

   An entry is made in the modification log and the connector Integration page reopens.

3.4 Document Information Extraction (DOX)

SAP Fieldglass has a single connection instance per region for all customers. The following information is available to configuration managers for visibility only at this time.

Field Name	Field Value	Source	Comments
Instance Type	Production/Non-Production	Configuration file	SAP Fieldglass maintains the mapping file between environments.
Region	US, EMEA, KSA, etc.	Configuration file	SAP Fieldglass maintains the mapping file between environments.
SAP BTP URL	Production Value Non-Prod Vale	Configuration file	SAP Fieldglass maintains the mapping file between environments.
SAP BTP Instance ID	Production Value Non-Prod Vale	Configuration file	SAP Fieldglass maintains the mapping file between environments.
Username	Masked	Configuration file	A single username and authentication method for all connections.
Authentication	Masked	Configuration file	
Document Type	Table (below)		Only statement of work is available.

Document Type information

Document Type	This is the Fieldglass module related to the document type	Only Statement of Work is available.
DOX Document Type Name	The name of the document type in SAP DOX instance	
Version	To support development of version controls, which DOX offers.	
Activation Time	This allows customers to *switch* templates in the future, based on the start date of the upload.	
Description	Used to provide information to the administrators around version/ configuration.	

3.5 API Application Keys

The connection between SAP Fieldglass and API applications is established via the Configuration Manager dashboard.

The *API Applications Keys* tile allows you to create and manage SAP Fieldglass license keys and web service users for access to API applications. For example, you can establish connectivity between SAP Fieldglass and the Time Processing service or SAP Identity Provisioning service.

An API requires two pieces of information to access an API application and process data: an application key and an active web service (username/password).

The *API Application Key* tile on the dashboard opens the API Application Key List page. In the top section of the page under *API Application Name*, you can create and manage API application keys, as well as view, edit, enable, and disable existing API application keys. After creating an application key, the API Application Key List page opens and displays the auto-generated application key, client ID, and client secret details. You can use existing API application keys, edit the keys, or create new ones.

In the bottom section of the page under *Web Services*, you can view existing web service accounts related to your company. You can use the existing web service accounts, edit the accounts, or create new ones, and establish users who can manage your web service accounts. When editing a web service, you can select a different virtual person name and also change the web service status. The virtual person is typically a user set up specifically for integrations who is associated to a role with the appropriate rights assigned for actions to be taken.

3.5.1 Create API Application Key or Web Service

Describes how to create API application keys and web services for file transfer uploads and downloads.

Context

When you create an API application key, the system auto-generates the application key, Client ID, and Client Secret.

> **Note**
>
> You can only create a web service when creating an application key.
>
> You can't delete an API application key or web service.

Procedure

1. **To create a new API Application Key**

1. On the Self-Service Dashboard, choose the *API Application Keys* tile.
   The Create API Application Key page opens.
2. Enter the following values:
   - Application Name (must be a unique value)
   - Description
3. Choose *Create*.
   The API Application Key List details page opens and displays a success message confirming the key was created. Note that the status of the new key is `Active`.
   In the *API Application Key Details* section, the following details display:
   - *Application Name* is the name you entered on the previous page.
   - *Application Key* is auto-generated.
   - *Client ID* is auto-generated.
   - *Client Secret* is auto-generated.
   - *Description* is the description you entered on the previous page.

   To edit the API application key, on the right-side of the page, choose *Edit*. For more information, see Edit API Application Key or Web Service [page 44].

2. **To create a new Web Service**
   1. After creating an API application key, on the Application Key details page in the *Setup Web Service* section, choose *New* on the right side of the page.
      The *Edit Details* dialog box opens.
   2. Enter/ select the following values:
      - Application Name (must be a unique value)
      - Virtual Person Name (Username)
      - Status (enabled or disabled)
3. Choose *Save*.

3.5.2 Edit API Application Key or Web Service

Describes how to view and edit existing API application keys and web service accounts.

Context

The **API Application Key** tile on the dashboard allows you to view, edit, enable, and disable existing API application keys. In addition, you can manage your web service accounts and establish users who can manage the accounts.

Procedure

1. **To edit an API Application key**

1. On the dashboard, choose the *API Application Keys* tile.
   The API Application Key List page opens.
2. In the *Application Name* section, choose the application name hyperlink.
3. In the *Edit Details* dialog box, change any of the following details:
   - Enter a new Application Name.
   - Enter a new Description.
   - Change the Status to enabled or disabled (based on the current status).
4. Choose *Save*.

2. **To edit a Web Service**
   1. In the *Web Services* section, choose the application name hyperlink.
   2. In the *Edit Details* dialog box, change any of the following details:
      - Enter a new Application Name.
      - Enter a new Virtual Person Name (Username).
      - Change the Status to enabled or disabled (based on the current status).
   3. Choose *Save*.

3.6 DocuSign End Points

DocuSign end points are required to link your SAP Fieldglass instance to your DocuSign account.

ESignature workflows support the needs of buyers and their suppliers or workers to have documents electronically signed using DocuSign as the provider.

DocuSign is the global leader in electronic technology for facilitating electronic exchanges of contracts and signed documents. When the DocuSign integration is enabled, standard functionality is available that allows buyers to set up their workflows using activity items. For more information about the company and its services, visit the DocuSign website: www.docusign.com .

DocuSign is a system of record and all signatures are managed within a DocuSign envelope (a unique transaction ID within the DocuSign system). DocuSign can house multiple types of documents that require signature management between buyers, suppliers, and workers.

If your company has enabled DocuSign as your esignature provider, you can create and manage your integration end points using this tile. Be sure to review the Requirements to Get Started to ensure you have the necessary information to create the end points.

Related Information

Create and Manage DocuSign End Points [page 46]

3.6.1 Create and Manage DocuSign End Points

DocuSign end points can be managed by your company's configuration manager.

Prerequisites

If you're setting up your DocuSign integration for the first time or you're editing your end points to add a new JWT authentication token, you'll first need to generate an access token with JSON Web Token (JWT) Grant authentication here . You'll also need the DocuSign Integration Key.

Context

You can use the DocuSign End Points tile to update your existing DocuSign end points, or add new end points. To update your existtng settings, select the *ID* from the list and choose *Edit*. To add new information, choose *Add* and follow the steps below.

Procedure

1. Enter a unique *ID* for the end point. This value cannot be changed once the settings are saved.
2. Enter the *End Point* URL.
3. Enter the DocuSign *Integrator Key*.
4. Provide the *User ID* for the end point.
5. Provide the JWT you previously generated in the *Private Key* field.
6. Optionally provide your DocuSign account *Username* and *Password*.
7. If necessary, enter the *API Account ID*.

Results

If you are upgrading your DocuSign end point, the JWT entered in the Private Key field will be used to authenticate your DocuSign integration.

3.7 Encryption Keys and Certificates

Configuration Managers can create and manage the company's different types of security assets using the *Encryption Keys and Certificates* tile on the Self-Service Dashboard.

Business applications, in general, process confidential information. Software applications secure confidential information by restricting access and sometimes encrypting data. Information Security departments, auditors, customers, and other stakeholders review assets, methods, and processes used to secure confidential information. SAP Fieldglass provides a common platform that enables reusable services to store, retrieve, and use assets (encryption keys and certificates) to implement a common interface for all business applications to secure confidential data; reduce duplication of code and processes; and provide a single view to all security assets. Data marked as secure are encrypted through the keys and stored encrypted in the SAP Fieldglass database.

> **Note**
>
> Encryption keys must be rotated at a minimum of every 6 months. If not rotated, they will expire and you will experience system disruption. Options to generate and auto-rotate are available for some encryption keys, however if these options are used, action may still be required to prevent disruption. To mitigate risk, you can set up notifications to alert the appropriate users when expiration is approaching. See Manage Key Expiration Notifications.

The following table describes the different asset types supported by this feature.

Asset Type	Characteristics	Storage
Symmetric Key (DEK)	Used to encrypt/decrypt sensitive field level data, custom fields, unique ID, and security ID. Encryption converts plain text into an unintelligible form called cipher text. Decryption converts the cipher text back to plain text. The same secret key is used for encryption and decryption.	Symmetric keys are stored in the SAP Fieldglass vault.
Public Key Infrastructure (PKI)	Asymmetric key used to encrypt a symmetric key and for exchanging data with third-party customers. The keys are also used in system-to-system authentication and TLS implementation. The algorithm uses 2 encryption keys, a public key visible/available to everyone and a private key that is kept private, to encrypt/decrypt data. The public key is used to encrypt the data and the private key is used to decrypt it.	Private keys are stored in the SAP Fieldglass vault.

Asset Type	Characteristics	Storage
Pretty Good Privacy (PGP) Key	Used to encrypt files transmitted to or received from customers. **⚠ Caution** Weak encryption configurations, such as the CAST 128-bit cipher or RSA key sizes that fall below our required security standards for PGP keys, are now deprecated. Under the new automated expiration process, all newly generated PGP keys will use AES-256 encryption wrapped in a 2048-bit RSA key, ensuring a substantially higher level of cryptographic strength and long-term protection. Customer-provided keys will be required to follow the same security standard.	Private keys are stored in the SAP Fieldglass vault.
Secure Shell (SSH) Key	Provides a secure way to authenticate and establish a connection between your computer and a remote server. They're commonly used for logging into servers, especially in cloud environments, without needing to type a password.	Private keys are stored in the SAP Fieldglass vault.
X.509	Used to generate KeyStore private keys and identity certificates, and to store Truststore certificates.	Private keys and certificates are stored in KeyStore stores. Certificates from trusted CAs (Certificate Authorities) are stored in Truststore stores.

After choosing a vault to store the security assets, you can create, generate, activate, rotate, and revoke encryption keys, as well as associate keys to other keys. Key storage and retrieval are managed by the system.

3.7.1 Choose a Storage Vault

Context

The first time you choose the *Encryption Keys and Certificates* tile, the *Basic Setup* dialog box prompts you to choose a vault to store the encryption keys you create.

Procedure

1. Sign into SAP Fieldglass as configuration manager.
2. On the dashboard, choose the *Encryption Keys and Certificates* tile.

   The *Basic Setup* dialog box opens.

3. Choose the *SAP Fieldglass* vault option. This stores keys in the SAP Fieldglass vault. The system creates all necessary tokens and the URL where the private keys are stored. After selecting this option, choose *Save*.
4. The Encryption Keys and Certificates page displays the *Action*, *Asset Category*, *Asset ID*, and *Asset Version* of assets you create. You can now proceed to Create, Generate, and Activate Asset [page 49].

3.7.2 Create, Generate, and Activate Asset

Create encryption keys and certificates to secure confidential application data and file transfers.

Prerequisites

You've chosen a storage vault to store your encryption keys as described in Choose a Storage Vault [page 48].

Context

Choose the *Encryption Keys and Certificates* tile to create, generate, and activate PGP, PKI, and symmetric encryption keys, and to create X.509 certificates. When creating encryption keys, you can auto-generate the key values or create them manually. After choosing the *Encryption Keys and Certificates* tile, the Encryption Keys and Certificates List page displays a list of all existing keys and certificates with corresponding values for the *Asset Category*, *Asset ID*, *Asset Version*, and *Asset Status*.

Procedure

1. To create a new asset, choose *New*.

   The *Create Asset* dialog box opens.

   For a description of the fields, see the following table.
2. In the *Category* list, choose one of the following asset types:
   - PGP
   - PKI
   - Symmetric Key
   - SSH
   - X509
3. Choose *Create*.

   The *Create Asset* dialog box displays populated with additional fields based on the category you chose.
4. Enter an **Asset ID** for the asset.
5. If you want the key to be auto-generated, select **Generate**. (This option is not available for X509 certificates.) When you select **Generate**, the **Auto-Rotate** option becomes available. (This option is not

available for PGP keys.) Select **Auto-Rotate** to have the key automatically rotated every 6 months. If you don't choose this option you will need to manually create a new key and activate it. Note that keys that are manually provided (not system-generated) cannot be automatically rotated. Manual rotation is required at least every 6 months.

6. Define the additional fields for the asset as described in the following Add Encryption Keys and Certificates Field Descriptions table, and then choose *Create*.

   After creating the new asset, the following message displays on the Asset Configuration page:

   `Success! Asset has been Created or Updated Successfully`.

   The asset ID displays at the top of the page and the corresponding asset configuration displays on the *Details* tab.

   When managing Encryption Keys and Certificates, you can now manage PGP Encryption for end points leveraging keys stored in a secure vault in SAP Fieldglass.

7. To activate the asset, on the top-right side of the page, choose *Activate*.

   The following message displays on the Asset Configuration page: `Success! Asset has been Activated Successfully.`

Add Encryption Keys and Certificates Field Descriptions

Field	Description	Field Type	Required/ Options	Applies to PGP	Applies to PKI	Applies to Symmetric Key	Applies to X509
Namespace	Namespace is an internal hierarchy to group assets that belong to a company.	Plain text. Not editable.	Yes. Generated by the application.	Yes	Yes	Yes	Yes
Asset ID	An internal identifier to uniquely identify the asset within a namespace.	Text Box. Editable.	Yes. Generated by the application or entered by the user when adding a new asset. Maximum 100 characters. Field is read-only when editing.	Yes	Yes	Yes	Yes

Field	Description	Field Type	Required/ Options	Applies to PGP	Applies to PKI	Applies to Symmetric Key	Applies to X509
Category	Identifies the type of asset. Possible values are PGP, PKI, Symmetric Key, and X509.	Drop-down. Plain Text	Yes	Yes	Yes	Yes	Yes
Generate Key	Provides an option to allow the application to auto generate the asset. Applies to PGP, PKI, and Symmetric Key.	Check Box	Optional	Yes	Yes	Yes	No
SSH Public Key	Cryptographic asymmetric key used to encrypt plain text data and Symmetric Key. Applies to PGP and PKI.	Text Box	Optional if *Generate Key* check box is selected.	Yes	Yes	Yes	Yes
Private Key	Cryptographic asymmetric key used to decrypt data and a Symmetric Key encrypted with corresponding public key. Applies to PGP and PKI.	Text Box	Optional if *Auto Generate Key* check box is selected.	Yes	Yes	Yes	Yes
Symmetric Key	Cryptographic shareable key used to encrypt plain text data and decrypt encrypted data.	Text Box	Optional if *Auto Generate Key* check box is selected.	No	No	Yes	No

Field	Description	Field Type	Required/ Options	Applies to PGP	Applies to PKI	Applies to Symmetric Key	Applies to X509
Value External ID	Option to enter key as a value OR as external ID. External ID applies to a client that is set up to use an external vault for keys instead of the SAP Fieldglass vault. Defaults to `Value`.	Option Button	Mandatory	Yes	Yes	Yes	No
Password	Passphrase used to protect a private key.	Text Box	Optional if *Auto Generate Asset* check box is selected.	Yes	No	No	No
Key Algorithm	The standard algorithm name for the cryptographic key.	Plain text. Not Editable.	Yes. Generated by the application.	Yes	Yes	Yes	No
Key Strength	The length of the key in bits. Key Security Strength is determined by key algorithm and length of the key.	Plain Text. Not editable.	Yes. Generated by the application.	Yes	Yes	Yes	No
Use for Signing Signature Verification	An option to use the key for signing / digital signature verification.	Option Button	Yes. (Yes, No and None - Not implemented yet.)	Yes	No	No	No

Field	Description	Field Type	Required/ Options	Applies to PGP	Applies to PKI	Applies to Symmetric Key	Applies to X509
Status	Status of the asset in the application. Possible values are `New`, `Active`, `DecryptOnly`, and `Revoked`. A newly created asset has status `New`. The asset moves to `Active` status upon activation. `DecryptOnly` status applied when an asset/key is rotated. Only an `Active` asset can be used for an encryption.	Plain text. Not editable.	Yes. Generated by the application.	Yes	Yes	Yes	Yes
Notes	A field for user notes for the asset.	Text Box	Optional	Yes	Yes	Yes	Yes
Public Certificate	X509 certificate text.	Text Box	Yes	No	No	No	Yes
Encoded Form	Encoded form of the certificate.	Plain text. Not editable.	Yes. Generated by the application.	No	No	No	Yes
Valid From Date	Start date of validity period of X509 certificate.	Plain text. Not editable. Generated by the application.	Yes. Generated by the application.	No	No	No	Yes

Field	Description	Field Type	Required/ Options	Applies to PGP	Applies to PKI	Applies to Symmetric Key	Applies to X509
Valid To Date	End date of validity period of X509 certificate. Applies to X509 certificate only.	Plain text. Not editable.	Yes. Generated by the application.	No	No	No	Yes
Serial Number	Serial Number is an integer value that uniquely identifies the certificate. Applies to X509 certificate only.	Plain text. Not editable.	Yes. Generated by the application.	No	No	No	Yes
Issuer X500Principal	Distinguished name of the issuer from the given X509 certificate that signed the certificate. Applies to X509 certificate only.	Plain text. Not editable.	Yes. Generated by the application.	No	No	No	Yes
Subject X500Principal	Distinguished name of the subject from the given X509 certificate. Applies to X509 certificate only.	Plain text. Not editable.	Yes. Generated by the application.	No	No	No	Yes
Alias	Unique field that is a concatenation of company code, assetId & 'Valid To Date' from the given X509 certificate.	Plain text. Not editable.	Yes. Generated by the application.	No	No	No	Yes

Field	Description	Field Type	Required/ Options	Applies to PGP	Applies to PKI	Applies to Symmetric Key	Applies to X509
Begin Notification day(s) before asset expires	Number of days before which the email notification should be sent out to the client before X509 certificate expires. Applies to X509 asset only.	Text Box	Yes	No	No	No	Yes
Notification Email ID	Email ID for sending notifications.	Text Box	Yes	No	No	No	No
Custom Attributes	Custom values that can be associated with the certificate for the given attributes in the drop-down.	Drop-down Text Box. Editable.	Optional. Options in the drop-down box are: LinkedCompany LinkedUser Use	No	No	No	Yes
Key Usage	Specifies the cryptographic operations that may be performed using the public key contained in the certificate.	Plain Text. Not editable.	Yes. Generated by the application.	No	No	No	Yes
Subject Alternative Names	Subject alternative names from the cPlainertificate.	Text. Not editable.	Yes. Generated by the application.	No	No	No	Yes
Is CA	Identifies if the certificate is a root/intermediate certificate.	Plain Text. Not editable.	No	No	No	No	Yes

Field	Description	Field Type	Required/ Options	Applies to PGP	Applies to PKI	Applies to Symmetric Key	Applies to X509
Extended Key Usage	Indicates the purpose of the public key contained in the certificate.	Radio Button. Editable.	Optional. Options are *User Authentication*, *System Authentication*, *None*.	No	No	No	Yes
Key Encryption Key	An active PKI asset used to encrypt a symmetric key. Displays PKI asset ID with version and status in the drop-down.	Drop-down	Yes	No	No	Yes	No
Begin notification this many days before asset expires	Number of days before which the email notification is sent to the client before X509 certificate expires. Applies to X509 asset only. Valid values are 0–180 days. The value 0 automatically sends notifications at 30, 60, and 90 days.	Text Box	Yes	No	No	No	Yes
Auto Activate	Activates the asset upon successful creation of an asset. Applies to X509 certificate only.	Check Box	Optional	No	No	No	Yes

Field	Description	Field Type	Required/ Options	Applies to PGP	Applies to PKI	Applies to Symmetric Key	Applies to X509
Apply to all custom fields	Associates the Symmetric Key with all custom fields for encryption/ decryption. Only applicable to Symmetric Key after activation.	Check Box	Optional	No	No	Yes	No
Custom Attributes	Associates additional information about the certificate. For example, to specify how the certificate is being used, choose `Use` in the *Common Attributes* list, and enter `Certificate Authentication` in the next field, then choose *Add*. Or choose `Linked User` and specify an SAP Fieldglass buyer username for connectivity to the web service API.	Drop-down. Plain Text	Optional	No	No	No	Yes

3.7.3 Edit Asset

Prerequisites

You've created, generated, and activated the asset you want to edit.

Context

Choose the *Encryption Keys and Certificates* tile to edit the values of an asset based on the asset category. After choosing the *Encryption Keys and Certificates* tile, the Encryption Keys and Certificates List page displays all existing keys and certificates, and the corresponding configuration values.

Procedure

1. To edit an asset, in the *Action* column, choose *View Details* in the corresponding row of the asset you want to edit.

   The selected asset opens on the *Details* tab of the Asset Configuration page.
2. On the top-right side of the page, choose *Edit*.

   The Edit Asset page opens.
3. Change the values as needed. For a description of the fields, see Create, Generate, and Activate Asset [page 49].
4. Choose *Save*.

3.7.4 Associate Asset

Associate symmetric keys with your application data to secure the data in the database.

Prerequisites

You've created, generated, and activated the symmetric key you want to associate.

Context

Choose the *Encryption Keys and Certificates* tile to associate a symmetric key with application data. Associating an asset is applicable to symmetric keys for the purpose of storing all custom fields as encrypted data in the SAP Fieldglass database.

> ⓘ Note
>
> After associating and rotating an asset, the association stays enabled once you activate the rotated asset.

Procedure

1. To associate an asset, on the Encryption Keys and Certificates page, choose *View Details* in the corresponding row of the symmetric key you want to associate.

   The selected asset opens on the *Details* tab of the Asset Configuration page.
2. Choose the *Association* tab.
3. Select the *Apply to all custom fields* check box.
4. Choose *Save*.

3.7.5 Rotate Asset

Key rotation is supported for PGP, PKI, and SSH keys; it doesn't apply to X509 certificates.

Context

Rotating an asset is the process of generating a new version of the same asset with a different crypto value. Encryption key rotation generates a new version of the asset with a new key value. The status of the previous version (for example, version 1) is set to `DecryptOnly` when you activate the new version (for example, version 2). The old version is no longer valid for encrypting data; however, it can still be used to decrypt data that was previously encrypted with that version.

Choose the *Encryption Keys and Certificates* tile to rotate an asset based on the asset category. The Encryption Keys and Certificates List page displays a list of all existing keys and certificates, with corresponding configuration values. All new versions of generated keys need to be activated before use. The new key version is automatically associated with custom fields on activation. You can also update the key metadata, such as adding a new note.

> → Tip
>
> You can manage notifications by capturing email addresses for each category of assets, like PGP keys. Clients are sent notification alerts at regular intervals, starting at 90 days, when an encryption key/

certificate is about to expire. For more information, refer to Manage Key Expiration Notifications [page 62].

> **Note**
>
> Expiration for existing assets and any new assets created before January 2026, will begin in June of 2026. Expiration for new assets created after January will be set for six months from the date the key was created. Expiration will be reset for six months out each time a key is rotated.

Asset Type	Generate	Auto-Rotate	Expiration	Information
Symmetric Key (DEK)			6 months - expiration will begin occurring on or after June 1, 2026.	Manually created keys will be set to Decrypt once the expiration date is reached and the key will have to be manually rotated.
Public Key Infrastructure (PKI)			6 months - expiration expiration will begin occurring on or after September 1, 2026.	Manually created keys will be set to Decrypt once the expiration date is reached and the key will have to be manually rotated.
Pretty Good Privacy (PGP) Key			6 months - expiration will begin occurring on or after June 1, 2026.	PGP keys cannot be auto-rotated. Generated keys will have to be manually rotated. Customer provided keys will be set to Decrypt once the expiration date is reached and the key will have to be manually rotated. **Caution** Weak encryption configurations, such as the CAST 128-bit cipher or RSA key sizes that fall below our required security standards for PGP keys, are now deprecated. Under the new automated expiration process, all newly generated PGP keys will use AES-256 encryption wrapped in a 2048-bit RSA key, ensuring a substantially higher level of cryptographic strength and long-term protection. Customer-provided keys will be required to follow the same security standard.

Asset Type	Generate	Auto-Rotate	Expiration	Information
Secure Shell (SSH) Key			6 months - expiration will begin occurring on or after July 2026.	⚠ Caution For generated keys that are auto-rotated, a new version of the same asset will be generated on the expiration date. The new version of the key will need to be updated in your SFTP servers for integrations to continue functioning. Customer provided keys will be set to Decrypt once the expiration date is reached and the key will have to be manually rotated.
X.509	NA	NA	NA	NA

Procedure

1. To manually rotate an asset, in the *Action* column, choose *View Details* in the corresponding row of the asset you want to rotate.

   The selected asset opens on the Asset Configuration page on the *Details* tab.
2. On the top-right side of the page, choose *Edit*.

   The Asset Edit page opens.
3. In the *Public Key* field (for PKI or PGP key) or *Symmetric Key* field, replace the current value with a new valid key value, or choose the **Generate** option. Optionally choose **Auto-Rotate** if you want the key to begin automatically rotating once activated.
4. Choose *Save*.
5. Activate the new key. For task instructions, see Create, Generate, and Activate Asset [page 49].

Manage Key Expiration Notifications

Context

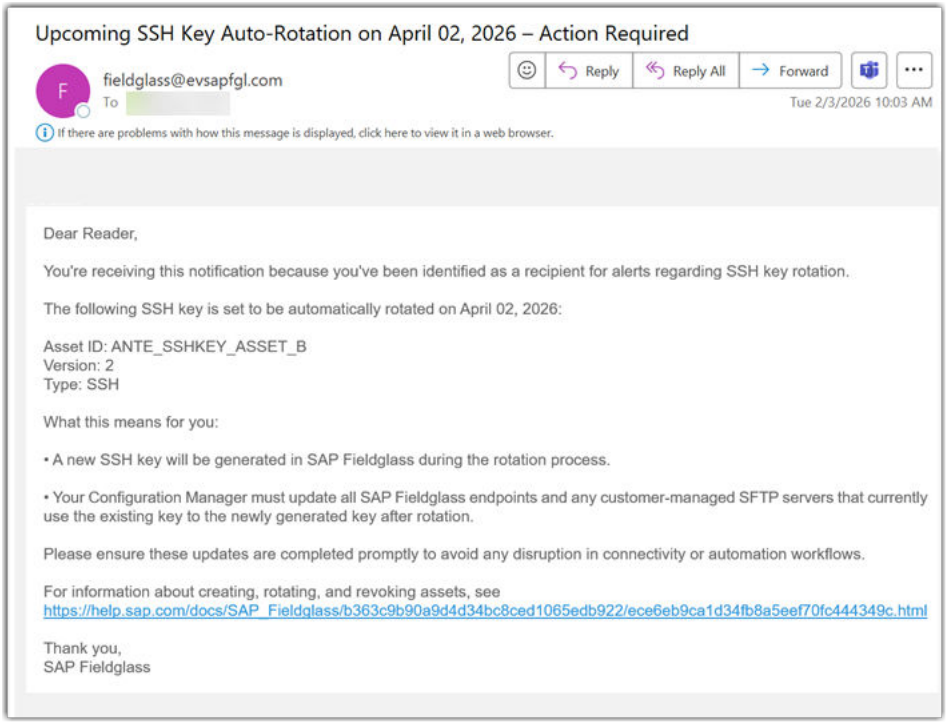
Choose *Manage Email Notifications* to capture *Email Address(es)* for each category of crypto asset, like PGP Keys or Certificates. Clients are sent notification alerts when an encryption key/certificate is about to expire.

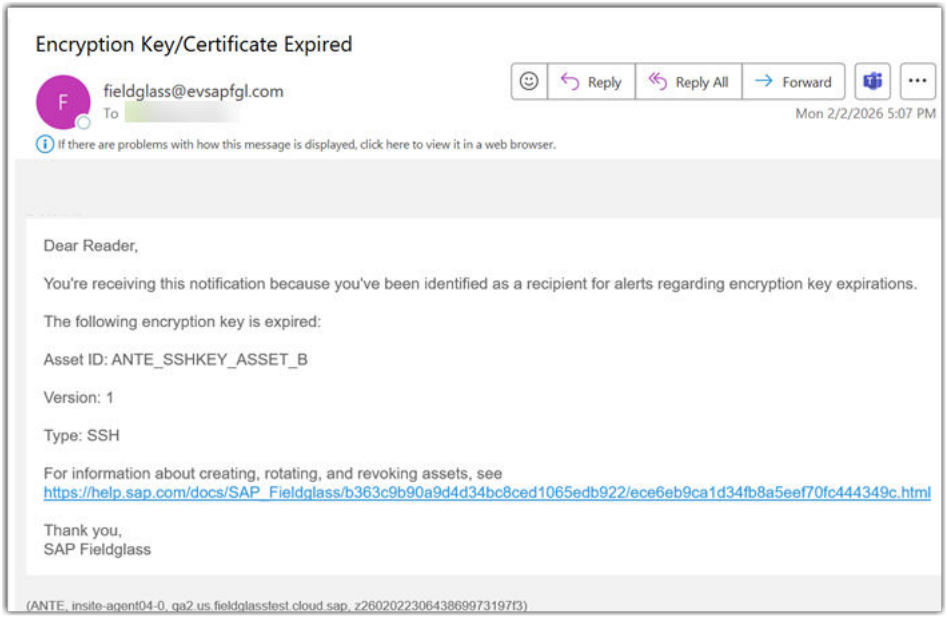
Procedure

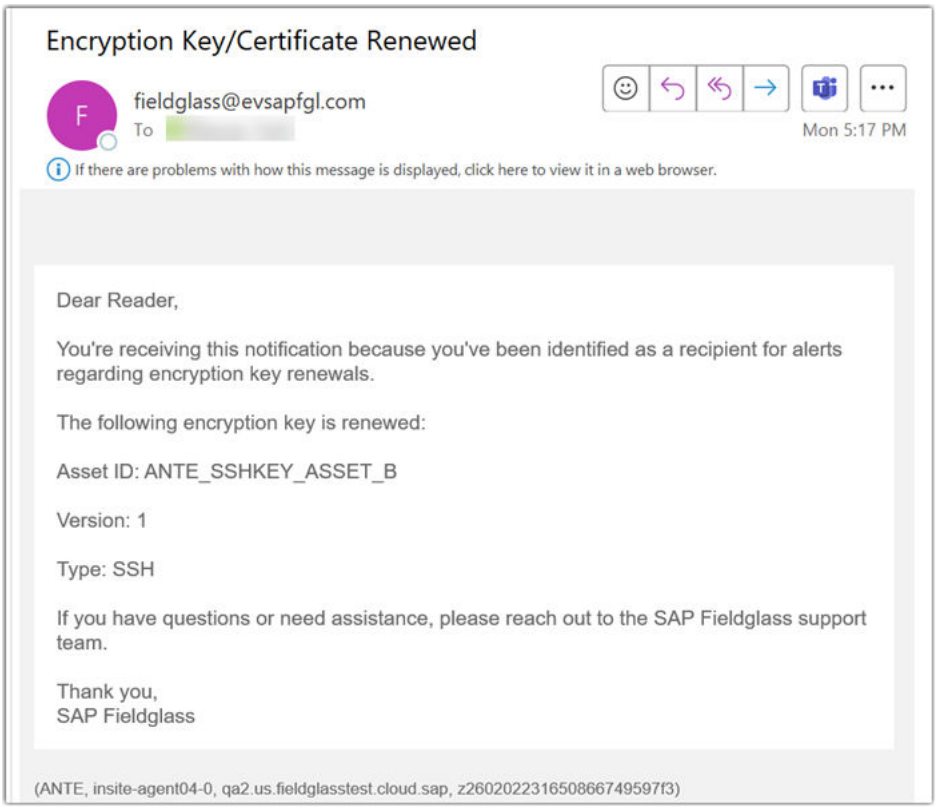
1. To manage email notifications, select *Manage Email Notifications*.
2. In the *Asset Category* list, select the asset you wish to edit.
3. On the top-right side of the page, select *Edit*.
4. Add or edit the email addresses as needed.
5. Select the *Notification Timing*. This value is set to 90 days by default and it cannot be changed. Notifications will begin at 90 days before expiration and will continue at regular intervals until expiration or until the asset is rotated.
6. Select *Update*.

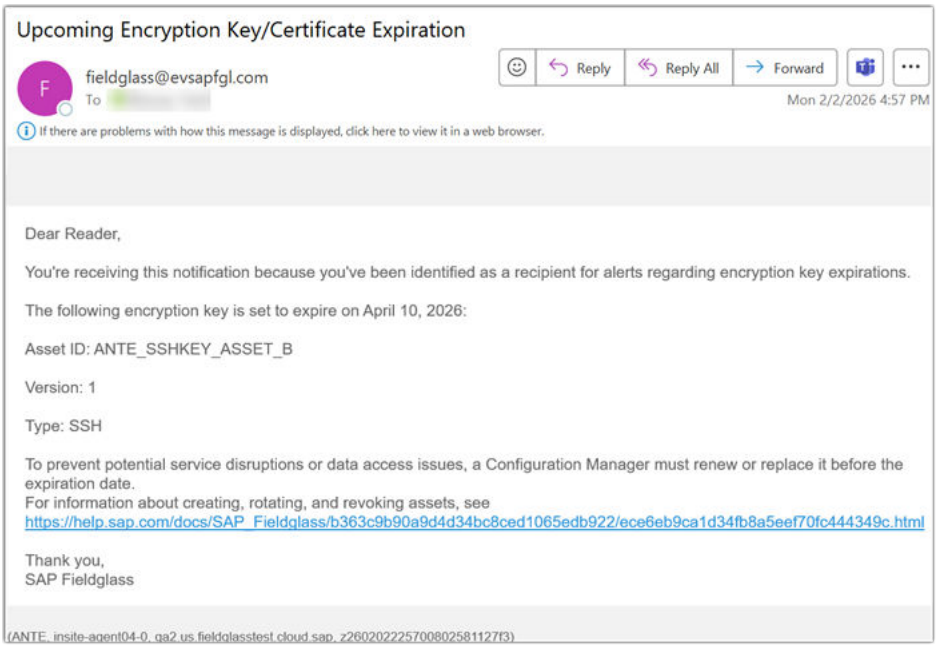
Example

System Notifications




Encryption Key/Certificate Expired
F
fieldglass@evsapfgl.com
To
Reply
Reply All
Forward
Mon 2/2/2026 5:07 PM
If there are problems with how this message is displayed, click here to view it in a web browser.
Dear Reader,
You're receiving this notification because you've been identified as a recipient for alerts regarding encryption key expirations.
The following encryption key is expired:
Asset ID: ANTE_SSHKEY_ASSET_B
Version: 1
Type: SSH
For information about creating, rotating, and revoking assets, see
https://help.sap.com/docs/SAP_Fieldglass/b363c9b90a9d4d34bc8ced1065edb922/ece6eb9ca1d34fb8a5eef70fc444349c.html
Thank you,
SAP Fieldglass
(ANTE, insite-agent04-0, qa2.us.fieldglasstest.cloud.sap, z26020223064386997319 7f3)


Encryption Key/Certificate Renewed
F
fieldglass@evsapfgl.com
To
Mon 5:17 PM
If there are problems with how this message is displayed, click here to view it in a web browser.
Dear Reader,
You're receiving this notification because you've been identified as a recipient for alerts regarding encryption key renewals.
The following encryption key is renewed:
Asset ID: ANTE_SSHKEY_ASSET_B
Version: 1
Type: SSH
If you have questions or need assistance, please reach out to the SAP Fieldglass support team.
Thank you,
SAP Fieldglass
(ANTE, insite-agent04-0, qa2.us.fieldglasstest.cloud.sap, z26020223165086674959 7f3)



3.7.6 Revoke Asset

You can revoke a certificate if you receive a new certificate or an existing certificate is compromised.

Prerequisites

You've created, generated, and activated the asset you want to edit.

Context

Choose the *Encryption Keys and Certificates* tile to revoke a certificate asset. After choosing the *Encryption Keys and Certificates* tile, the Encryption Keys and Certificates List page displays a list of all existing keys and certificates with corresponding configuration values.

> **Note**
>
> A revoked certificate can't be used for encryption or decryption. However, for field level keys the revoked key can be used, with explicit authorization, to retrieve and re-encrypt the data, which involves a manual process of decryption with the revoked key and re-encryption with the new key.

Procedure

1. To revoke a certificate, in the *Action* column, choose *View Details* in the corresponding row of the certificate you want to revoke.

   The selected certificate opens on the *Details* tab of the Asset Configuration page.
2. On the top-right side of the page, choose *Revoke*.

   The status of the certificate updates to `Revoked`.

3.8 End Points

Describes how to set up and manage you company's integration end points by using the End Points tile on the Self-Service Dashboard.

The End Points tile displays the End Point List page, which contains a list of all end points for the company, by *Activity* (All, Active, or Inactive), *ID* (unique ID), and *Category* (OData, SFTP, Publish/Subscribe, and WebService). You can filter the columns to adjust the display results, as well as add, edit, copy, activate, and remove end points.

Integration connectors that use the Subscription transfer method require one end point per connector. The end point defines the properties of the server that SAP Fieldglass must communicate with to push or pull connector files using a subscription.

An end point can have multiple subscriptions. For example, a worker upload file can be configured with two subscriptions, one puts the upload file in the SFTP server every Monday at 9:00 A.M., and the other puts the upload file in the SFTP server every Friday at 10:00 P.M. Similarly, many subscriptions can be configured for the same end point.

Considerations:

- Script values are generated in the system based on the directory and file properties selected.
- Only basic types of files uploads are supported.
- The following elements aren't supported:
  - directory uploads
  - file patterns
  - uploads that require temporary files/directories
  - encryption/decryption of files to be sent to or received from the servers
  - Non-standard ports

3.8.1 Create End Point

Describes how to create and test end points for file transfer uploads and downloads.

Context

Create end points to display in pick lists that you choose from when editing or creating connectors and publish/subscribe entries.

For any new or changed details made to a subscription, entries are made to the Modification Log.

Procedure

1. On the Self-Service Dashboard, choose the *End Points* tile. The End Point List page opens.
2. In the upper-right corner of the page, choose *New*.

   The *Create End Point* page opens.
3. Enter/select the end point properties as described in the following table of property descriptions.

   > → Tip
   >
   > You have the option to create an end point in the environment of your choice using the *Env Mode* drop-down list.
4. To work with additional fields:
   - To add additional fields to the end point, choose *+ Add Additional Fields*, and then enter values in the *Name*, *Description*, and *Value* fields.
   - To remove an additional field, choose *X Remove* above the field.
5. Before submitting the end point for creation, select the *Test Connectivity* button to test the connectivity to the target server. If the test is successful continue with the next step, if the test is unsuccessful, resolve the issue and try again.

   Note that you can also test connectivity after creating or editing an end point.
6. Choose *Submit*.
7. After creating a new end point, you need to activate the end point. For information on this process, see Activate/Deactivate End Point.

   The following table describes the required properties, optional properties, and applicable rules for creating end points.

   End Point Property Descriptions

Property	Description
Basic Setup (all end points)	

Property	Description
ID	Unique ID for the end point. The value is prefixed with `[Company Code]_[get/put]_[Connector Name]`, based on the selected *Activity* (Upload/Download). Required property.
Category	Describes how to transmit the file to the end point. Additional fields display based on the option that you select. Required property except as noted. Valid options are: OData (Open Data Protocol) SFTP (Secure File Transfer Protocol) Webservice **Note** When creating, editing, or copying an end point for the Webservice category, the URL field is optional. PublishSubscribe **Note** All end point categories support testing. For more information, see Test Subscription [page 89].
Activity	The activity of the file. Required property. Valid options are: Upload Download
SFTP Setup	**Note** To enable additional, more secure ciphers, macs, and key exchanges, you need to add an additional field after filling out SFTP information. Select *+Add Additional Fields*, and in the *Name* field, enter **`useSSHJ`**, with a *Value* of **`true`**. (Although not mandatory, you can also enter a brief description.)
Host	Internet-facing network address of the SFTP server to be accessed by the Host server address. Required property.
Port	Port to use when connecting to the host. If not specified, the default value is 22. Required property. The dropdown list includes standard ports 990, 443, and 22.

Property	Description
Authentication Type	Method used to connect to the SFTP server to ensure that the server is authentic. Valid options are: User Name / Password (requires entry of *Username* and *Password* properties). or Public Key Authentication (requires entry of *Username*, *Password*, and *Public Key* properties). Required property. **Note** For 'Authentication Type = Public Key Authentication', contact your SAP Fieldglass representative for assistance with generating and populating the Private Key (customers and partners currently don't have access).
Username	Username used for authentication to the server. Required property.
Password	Password used for authentication to the server. Allows up to 10,000 characters. Only alphanumeric characters and !@#$%A&*()_ special characters are allowed in the end point password. Required property if *Authentication Type* is 'Public Key Authentication'.
Confirm Password	Re-enter the password to confirm its authenticity. Required property.
SSH Public Key	Public key used for authentication to the server. Allows up to 10,000 characters. Only displays when **Authentication Type** is 'Public Key Authentication', and then it's a required field.
File Details	
Directory Path	Enter the full directory path of the file location. Optional property. For example, if the file path on the SFTP server is `/demo/uploads/test_upload_file.csv`, then the value to enter in this field is `/demo/uploads`. If the file path on the SFTP server is `/demo/downloads/test_download_file.csv`, then the value to enter in this field is `/demo/downloads`. **Note** The directory path can't be changed after the end point is created. If a new value is required, either copy the end point and change the copied value, or delete the end point and create a new one.

Property	Description
File Name	Name of the upload or download file to send or receive data. A file extension is required and the limit is 3–9 characters. For example, `po_upload_file.csv` or `po_xml.xml`. The file name can't be changed after the end point is created. If a new value is required, either copy the end point and change the copied value, or delete the end point and create a new one. Required property.
Suffix Time Stamp	Valid options are: Yes – Appends a time stamp value to the file name, in `yyyyMMddHHmmss` format. No – Doesn't append a time stamp. Optional property.
Date Format	When creating a new end point or copying an existing end point, you can select the Date Format from a drop-down list. The existing Date Format options can be used for Subscription download integrations because there are no naming restrictions from SAP Fieldglass. However, for Subscription upload integrations, the filename is keyed off of the time-stamp of when the integration is triggered. If the filename has a timestamp with minutes and seconds, SAP Fieldglass likely won't find a file on the client's server with that same minutes/seconds, since the client generates those files at a separate time before dropping the file and from when the file gets picked up by the integration. Otherwise, multiple files may be found. **Note** Selecting a Date Format with * (asterisk) in the Upload Date Format indicates a wildcard, meaning everything after the * in that specific Date Format pattern will be captured, and the upload file will be picked up by the integration.
Remove file after processing	Applies to uploads only. Can't be changed after the end point is created. Yes – Removes the file after processing. No – Retains the file after processing. Optional property.

Property	Description
PGP Encryption?	PGP encryption keys apply to SFTP uploads and downloads. Required property. Valid options are: Yes – Choose this option to enable PGP encryption. When selected, the following *PGP Encryption Key* property displays, allowing you to choose an encryption key. No – This is the default value. **Note** To use PGP encryption, contact your SAP Fieldglass representative to enable it in your company.
PGP Encryption Key	Allows you to select an encryption key for the end point. Only displays if *PGP Encryption?* property is set to Yes. Required property.
Advanced PGP Settings **Note** This section only displays if *PGP Encryption?* is set to Yes.	
Use PGP Signature Verification?	Allows you to designate if PGP signature verification is required. Required property. Valid options are: Yes – Choose this option to enable PGP signature verification. When selected, the *PGP Signature Verification Key* list displays (see next property), allowing you to choose a verification key. No – This is the default value.
PGP Signature Verification Key	Allows you to select a signature verification key for the end point. Only displays if the *Use PGP Signature Verification?* property is set to Yes. Required property.
Data File Name – downloads only	Displays the name of the underlying data file that's generated and then encrypted. The default format of the file name is `tmp_##########.csv`. No – This is the default value. **Note** If you choose 'No' for a download, the next three properties display.

Property	Description
Zip Compression – downloads only	Creates a zip archive of the data file. Required property. Yes – Creates a compressed zip file. No – Bypasses zip compression. Default value.
ASCII Armor – downloads only	Encases the encrypted messaging in ASCII so it can be sent in a standard messaging format such as email. Required property. Yes – Converts the binary message to text. No – Bypasses the binary to text conversion. Default value.
Integrity Check (MDC) – downloads only	Runs an MDC (Modification Detection Code) integrity check to detect message tampering. Required property. Yes – Runs the integrity check. No – Bypasses the integrity check. Default value.
OData, SFTP, Publish/Subscribe, and WebService Setup	
URL	URL where the end point receives data.
Authentication Type	Leave the default value `None`, or select one of the following options: • Basic Authentication • OAuth2 Client Credentials (client ID, client secret)
Username	Username credential to access the URL, if needed.
Password	Password credential to access the URL, if needed.
Additional Details	
Encoding	Specify the encoding of the file. Optional property.
Time Zone	Time zone in which the subscription runs. Optional property.

3.8.2 Edit End Point

Describes how to edit the details of an end point.

Context

When editing an end point, you can view the file details and underlying script, but you can't edit them.

In addition, you can't edit an existing file name, end point name, or file path. If you need to change any values that aren't editable, use the Copy End Point [page 72] function to make the changes.

Procedure

1. On the End Point List page, choose the ID hyperlink of the end point you want to edit.

   The end point opens in the *Details* tab of the End Point details page.
2. Choose *Edit*.

   The Edit End Point page opens.
3. Change the details and add custom fields as needed.

   For information on the end point properties, see the table of property descriptions in Create End Point [page 66].

   > ⓘ Note
   >
   > While you can modify existing details and custom fields, the *Env Mode* is not editable. If you need to change the environment mode, you'll have to copy the end point or create a new one.
4. To work with additional fields:
   - To add additional fields to the end point, choose *+ Add Additional Fields*, and then enter values in the *Name*, *Description*, and *Value* fields.
   - To remove an additional field, choose *X Remove* above the field.
5. Choose *Submit*.

   > ⓘ Note
   >
   > End point values can also be edited and additional properties added from Company Admin page (Maintain End Points). New properties added are retained but aren't visible to you.

3.8.3 Copy End Point

Context

Describes how to copy the properties of a selected end point to create a new end point with a unique ID. All other fields are prefilled and editable.

> → Remember
>
> You have the option to copy end points from one environment to another. This means that you can copy end points from a production environment to a test or beta environment without having to reconfigure or create them from scratch.

The End Points List page shows all the end points available in every environment mode. You have the option to select any end point from a specific environment and copy it to the other available environment modes. When running the application in the production environment, you can copy end points from production, QA, and beta modes to either beta or production environment mode.

Procedure

1. On the End Point details page, choose *Copy*.

   The Copy End Point page opens.
2. Enter the new ID.
3. Add or change the details and additional fields as needed. For a description of the properties, see Create End Point [page 66].

   > → Tip
   >
   > You have the option to copy an end point in the environment of your choice using the *Copy To* drop-down list.
4. Choose *Submit*.

3.8.4 Remove End Point

This action allows you to remove (delete) an end point from the system.

Context

Removing an end point is permanent and can't be reverted.

Procedure

1. On the dashboard, choose the *End Points* tile. The End Point List page opens.
2. On the *Details* tab, choose *Remove*.
3. To confirm the action, in the *Remove End Point* dialog box, choose *Remove*.

   The End Point List page displays and the end point is removed from the list.

3.8.5 Activate/ Deactivate End Point

This action allows you to activate and deactivate end points.

Context

An end point created as Authentication Type 'Username/Password' can be activated only using the *Edit* action and then submitting the end point. An endpoint created as Authentication Type 'Public Key Authentication' can be activated using the *Activate* button, which is available once the end point is created with SSH authentication. As such, the *Activate* button is available for end points of Authentication Type 'Public Key Authentication' only; the *Deactivate* button is available for end points of both authentication types.

> **Note**
>
> Deactivating an end point causes any subscriptions associated with the end point to fail.

Procedure

1. On the End Point List page, choose the hyperlinked end point name.

   The End Point details page opens.
2. Do either of the following to change the status:
   - To activate an inactive end point, choose *Activate*.
     The End Point details page displays the new status.
   - To deactivate an active end point, choose *Deactivate*.
     The *Deactivate End Point* dialog box displays. To confirm the action, choose *Deactivate*. To cancel the action, choose *Cancel*.
     The End Point details page displays the new status.

3.9 Event Driven Config

Describe how to set up and manage your company's real-time integrations by using the Event Driven Config tile on the Self-Service Dashboard.

The Event-Driven Configuration and Punchout Accounts functionalities are available on the Configuration Manager page of the Self-Service Dashboard. These features let you configure your integrations directly through the Self-Service Dashboard.

> **Note**
>
> The Punchout Accounts button is enabled and visible only when you create an event-driven config.

The enhancement of the Event-Driven Configuration functionalities in the Configuration Manager empowers users with self-service capabilities to configure real-time integrations in SAP Fieldglass. This enhancement brings several benefits, enabling users to configure integrations seamlessly.

Specifically, these improvements target the integration packages of SAP Ariba and SAP S/4HANA Lean Service procurement. They enhance the flexibility and efficiency of configuration processes, providing an improved user experience and streamlined integration management.

3.9.1 Create Event Driven Config

Describe how to create an Event Driven Config for the modules used in the workflows for real-time integration with SAP Ariba and SAP S/4HANA Lean Service procurement.

Context

The Event Driven Config setup process involves selecting a module, entering a configuration ID, associating activities, and configuring transport and authentication settings.

Procedure

1. On the system administration menu under *Integration Tools*, choose *Event Driven Config*. The Event Driven Config List page displays.
2. In the upper-right corner of the page, choose *New*. The *Add Event Driven Config* page opens.
3. Select the *Module* from the drop-down menu.
4. Enter the *Event Driven Config ID*.
5. Choose *+ Add Activities* to associate activities to the Event Driven Config page. The Associate Activity to Event Driven Config page displays.
   a. → Tip

      You can narrow down the results using the filter option. To filter the results, enter the *Activity Name* or *ID* and then click *Apply Filter*.

      Select the checkboxes next to one or more activities and choose *Add Selected*. Options include, but are not limited to:

      - View
      - Approve
      - Final Approval
      - Submit
      - Reject
      - Withdraw

- Complete Later
- Notify Approvers
- Approved
- Restart
- Final Rejection

> **Note**
>
> Types of activities vary based on the module selected for an Event Driven Config.

6. Select the *Transporter Class* from the drop-down menu.
7. Enter the following values (Optional):
   - Ariba Realm ID
   - Test End Point
   - Test Notification Emails
   - Prod End Point
   - Prod Notification Emails
   - Notify at Retry
   - OAuth Prod Params
   - OAuth Test Params
8. Select the *Auth Type* from the drop-down menu (Optional).
9. Select the *Custom Script* from the drop-down menu.
10. Select the *Transport Status* either *Push* or *Pull*.

> **Note**
>
> There are two options for transport status: Push and Pull. Please note that the default transport status is set to Push. There's no need to change it unless requested.

11. Choose *Add*. The new event driven config opens on the Details tab. From this page you can edit event driven config, activate/ diactivate, edit punchout account, and initiate a test run.
12. After creating a new event driven config, if you need to activate/ deactivate it. For information on this process, see Activate/ Inactivate Event Driven Config [page 80].

Event Driven Config Property

Describes the properties and applicable rules of an Event Driven Config.

The following table describes the required properties, optional properties, and applicable rules for adding Event Driven Config.

Event Driven Config Property Description

Property	Description
Module	Use the picklist from the Start Object field in the Punchout Account UI page. The code creates a second event-driven configuration with the same values entered here but includes the corresponding revision module. There are only three revision modules: Work Order Revision, SOW Revision (SOW Request), and SOW Response Revision. Required property.
Ariba Realm ID	Text field. Optional property.
Event Driven Config Id	It's pre-populated with Buyer_ModuleId_AnyUniqueIdentifier. It can allow the user to change if needed. The automatically created event-driven configuration for the Revision modules will have the ID entered plus _Rev (For example, ARBT_540_unique_Rev). Required property.
Activity	This field is a modal window. Required property.
Revision Activity	This field is required if you select Work Order, Statement of Work, or SOW Response as the module. Only show this field when one of these module values is selected. Required property.
Transporter Class	Select the transporter class from the drop-down list. Required property.
Auth Type	Select the Auth Type (for example, BASIC, oAuth, CERTIFICATE selection, or blank) from the drop-down list. Optional property.
Test End Point	This field appears only when users select all authentication types. Optional property.
Test Credential	This field appears only when users select the BASIC authentication type. Optional property.
Test Notification Emails	This field appears only when users select all authentication types. Optional property.
Prod End Point	This field appears only when users select all authentication types. Optional property.

Property	Description
Prod Credential	This field appears only when users select the BASIC authentication type. Optional property.
Prod Notification Emails	This field appears only when users select all authentication types. Optional property.
Notify At Retry	It is set to 25 retries by default. You can adjust it according to your requirements. Optional property.
oAuth Prod Params	This field appears only when users select the OAuth authentication type. Optional property.
oAuth Test Params	This field appears only when users select the OAuth authentication type. Optional property.
Custom Script	A drop-down list with an option for free-form text entry allows users to select predefined values or input custom data when necessary. Required property.
Revision Custom Script	When users select the Work Order, Statement of Work, or SOW Response modules, display this field only if they choose those module values. Required property.
Transport Status	Radio button defaulted to Push. Required property.
Punchout Account ID	This is the ID for the Punchout Account. Update both the Event Driven Config for the start and change objects. Optional property.

3.9.2 Edit Event Driven Config

Describe how to edit the Event Driven Config for the modules used in the workflows for real-time integration with SAP Ariba and SAP S/4HANA Lean Service procurement.

Prerequisites

Before you start editing, ensure you've changed the status of Event Driven Config to deactivated. For information on this process, see Activate/ Inactivate Event Driven Config [page 80].

Context

When editing an event driven config, previously entered values are displayed and can be edited where applicable. Any changes made to an event driven config are recorded in the *Modification Log*.

Procedure

1. On the *Event Driven Config List* page, choose the ID hyperlink of the event driven config you want to edit. The event driven config opens in the *Details* tab of the Event Driven Config details page.
2. Choose an *Event Driven Config ID*. The Event Driven Config Details page displays.
3. Choose *Edit Event*. The Edit Event Driven Config page opens.
4. You can change any of the following details:
    - Activity
    - Transporter Class
    - Auth Type
    - Test End Point
    - Test Notification Emails
    - Prod End Point
    - Prod Credentials
    - Prod Notification Emails
    - Notify at Retry
    - Custom Script
5. Choose *Update*.

3.9.3 Test Event Driven Config

Describe how to test the Event Driven Config for the modules used in the workflows for real-time integration with SAP Ariba and SAP S/4HANA Lean Service procurement.

Context

The Event Driven Config is enabled to trigger a test run. You can test all endpoint categories.

Procedure

1. On the *Event Driven Config List* page, choose the ID hyperlink of the Event Driven Config you want to test. The event driven config opens in the *Details* tab of the Event Driven Config details page.

2. Choose *Test*. The Test Event Driven Config page opens.
3. Enter the *Object Ref*.
4. Select the *Activity* from the drop-down menu.
5. Choose *Submit*. The system generates a transaction ID for the manual push.
6. Choose *Close*.

3.9.4 Activate/ Inactivate Event Driven Config

Describe how to activate/ inactivate the Event Driven Config for the modules used in the workflows for real-time integration with SAP Ariba and SAP S/4HANA Lean Service procurement.

Context

You can activate or inactivate Event Driven Configs at any time.

To edit an Event Driven Config, make sure to inactivate it first.

> **Note**
>
> When you activate/ inactivate an Event Driven Config, the Punchout Account also activates/ inactivates simultaneously.

Procedure

1. On the *Event Driven Config List* page, choose the ID hyperlink of the Event Driven Config you want to activate/ inactivate. The Event Driven Config opens in the *Details* tab of the Event Driven Config details page.
2. Do either of the following to change the status:
   - To activate an inactive end point, choose *Activate*. The Activate Event Driven Config dialog box displays. To confirm the action, choose *OK*. To cancel the action, choose *Cancel*. The Event Driven Config details page and Punchout Account display the new status.
   - To inactivate an active end point, choose *Inactivate*. The inactivate Event Driven Config dialog box displays. To confirm the action, choose *OK*. To cancel the action, choose *Cancel*. The Event Driven Config details page and Punchout Account display the new status.

3.9.5 Punchout Account

Punchout CXML account updates facilitate seamless integration with SAP Ariba and SAP S/4HANA Lean Service procurement. This is useful for ensuring efficient and real-time procurement processes within these platforms.

Edit Punchout Account

Describes how to edit and update the Punchout Account for an event driven config using the *Edit Punchout Account* feature.

Prerequisites

Before you start editing, ensure you've changed the status of Punchout Account to inactivated. For information on this process, see Activate/ Inactivate Event Driven Config [page 80].

Context

When editing the punchout account, you see previously entered values based on event driven config. You can edit these values where applicable.

Procedure

1. On the *Event Driven Config List* page, choose the ID hyperlink of the Event Driven Config you want to update the Punchout Account. The event driven config opens in the *Details* tab of the Event Driven Config details page.
2. Choose *Edit Punchout Account*. The Edit Punchout Account Details page opens.
3. The following details are autofilled and don't need any changes.
   - ID
   - Start Object
   - Change Object
4. You can change any of the following details:
   - Buyer ANID
   - Supplier ANID
   - Shared Secret
   - Supplier Part ID

- Supplier Auxiliary ID
- Punchout Type
- Punchout Action Class
- Start Object Lock at Status
- Change Object Lock at Status
- Default UOM
- Default Unspsc
- Work Order Post to URL
- Work Order Post at URL
- Approver ID
- Amount format Type
- Approval Level to Push
- Ariba Realm ID

5. There are two options for the following details: *Yes* and *No*. They're set to *No* by default. Don't change them unless requested.
   - Lock Start Object
   - Lock Change Object
   - Cost Allocation at SOW Line Item

     > **Note**
     >
     > This field appears only when the module is either SOW Response or SOW Revision Response.

   - Include Ship to Address to CXML

     > **Note**
     >
     > This field appears only when the module is either SOW Invoice or Invoice.

6. Choose *Update*.

Punchout Account Property

Describes the properties of the Punchout Account for an event driven config.

The following table describes the required properties, optional properties, and applicable rules for updating the Punchout Account.

Punchout Account Property Description

Property	Description
ID	Any unique identifier such as BuyerModuleUniqueid. Required property.

Property	Description
Buyer Company	Set this to the user's company code by default. Required property.
Buyer ANID	This is a text field where users can enter the required details. Required property.
Supplier ANID	This is a text field where users can enter the required details. Optional property.
Shared Secret	This is a text field where users can enter the shared secret. Optional property.
Supplier Part ID	Default as "FGLS" Required property.
Supplier Part Auxillary ID	Default as "FGLS" Required property.
Punchout Type	This is a dropdown menu. Users can select their desired option from the list. Required property.
Punchout Action Class	This is a dropdown menu. Users can select their desired option from the list. Required property.
Start Object	Use the Module ID from the Event Driven Config. Required property.
Lock Start Object?	Radio Button Optional property.
Start Object Lock at Status	This is a dropdown menu. Users can select their desired option from the list. Optional property.
Change Object	Infer the change object based on the Start Object. For example, Work Order would be Work Order Revision. Optional property.
Lock Change Object?	Radio Button Optional property.
Change Order Object Lock at Status	This is a dropdown menu. Users can select their desired option from the list. Optional property.

Property	Description
Default UOM	This is a text field where users can enter the required details. Optional property.
Default UNSPSC	This is a text field where users can enter the required details. Optional property.
Work Order Posting URL	Optional property.
Work Order Posting Status	Optional property.
Approver ID	This is a text field where users can enter the required details. Optional property.
Amount Format	This is a dropdown menu. Users can select their desired option from the list. Optional property.
Approval Level to Push	This is a text field where users can enter the required details. Optional property.
Cost Allocation at SOW Line Item?	Default No This field appears only when the module is either SOW Response or SOW Revision Response. Optional property.
Include ShipTo Address to cXML?	Default No This field appears only when the module is either SOW Invoice or Invoice. Optional property.
Ariba Realm ID	This is a text field where users can enter the required details. If users have already entered the Ariba Realm ID in EDC, this field displays as read only. Optional property.

3.10 Integration Subscriptions

Provides a holistic approach to set up and manage subscriptions to uploads and downloads.

On the Self-Service Dashboard, choose the *Integration Subscriptions* tile to open the Subscription List page. The page provides visibility to all subscriptions for the company, including details of *Status* (All, Enabled, or Disabled), *Name*, *Type* (All, Download, Upload (sftp), or webservice), *Subscriber*, and *End Point* for each subscription. You can filter the columns to adjust the display results, as well as add, edit, enable/ disable, test, and remove subscriptions.

Subscription names are in the form of a hyperlink, which you choose to open the Details page for a subscription. For more information, see Subscription Details [page 85].

3.10.1 Subscription Details

The Subscription details page is a tabbed interface that gives you all of the information about a subscription.

Context

The *Details* tab displays status, subscriber ID, company, subscription name, subscriber name, notification email, end point, delivery times, and recent activity. The *End Point* value is a hyperlink that opens the End Point Details page. For more information on end points, see End Points [page 65].

The *Modification Log* tab displays subscription activity (enabled, disabled, upload, download), activity time, reason, and the person who completed the activity.

Procedure

1. On the Self-Service Dashboard, choose the *Integration Subscriptions* tile.
2. On the Subscription List page, choose the subscription name hyperlink to open the details page for that subscription.

   The *Detail* tab is the current view.

   Depending on the subscription status, the following actions are available:
   - Enabled subscriptions allow the *Disable* and *Run Now* actions.
   - Disabled subscriptions allow the *Edit*, *Enable*, *Remove*, and *Run Now* actions.

3.10.2 Create Subscription

Create subscriptions to schedule file transfer uploads and downloads.

Context

This task requires adding an existing end point to the subscription. If there are no endpoints configured, you can create a new endpoint from the *End Points* tile on the dashboard. For information on creating end points, see Create End Point [page 66].

You can choose an existing endpoint from the list, define email addresses to receive notifications upon success or failure of the transfer, and schedule the subscription to run at a desired time.

For more information on creating subscriptions, see Subscription Setup [page 27].

Procedure

1. On the Self-Service Dashboard, choose the *Integration Subscriptions* tile.

   The Subscription List page opens.
2. In the upper-right corner of the page, choose *New*.

   The Create/Maintain Subscription page opens.
3. Define the following details:
   1. Under *Type*, choose `Upload` or `download`.
   2. In the *Connector* list, choose the connector for the subscription. All enabled connector names display.
   3. In the *End Point* list, choose an existing end point.
   4. In the *Subscription Class* field, the default value is `insite.subscription.WebserviceUploadSubscription`. You can leave the default value or enter any special subscription class value provided by your SAP Fieldglass representative.
   5. In the *Parameters* field, enter one or more parameters to pass in the subscription. If only one parameter is required, enter one value. If multiple parameters are required, enter the values separated by a comma with no space in between.
   6. In the *Subscriber* list, choose a user.
   7. In the *Notify On Missed Run*, check yes, if you want to be notified if a subscription fails to run. This is an optional field that's only visible if your company code has been added to the *FG_SUBSCRIPTION_ALERT* Feature Toggle.
   8. In the *Notification Email* field, enter an email address to send status notifications.
   9. Under *Delivery Time*, click in the *Minute*, *Hour*, *Day*, *Month*, and *Day* lists to choose values for when the subscription runs.
   10. In the *Time Zone* list, choose a value where the subscription runs.
4. Choose *Submit*.

   The new subscription opens on the Details page.

   From this page you can edit, enable/ disable, and remove the subscription, as well as initiate a test run of the subscription.

3.10.3 Edit Subscription

Change any details of an existing integration subscription.

Context

Subscriptions must be disabled for editing. For details on how to enable and disable a subscription, see Enable/ Disable Subscription [page 87].

When editing a subscription, previously entered values display and can be edited, where applicable.

For any changes made to a subscription, entries are made to the Modification Log.

Procedure

1. On the Self-Service Dashboard, choose the *Integration Subscriptions* tile.

   The Subscription List page opens.
2. To choose the subscription, click the subscription name hyperlink.

   The Subscription Details page opens.
3. In the upper-right side of the page, choose *Edit*.

   The Create/Maintain Subscription page opens.
4. You can change any of the following details:
   1. Type
   2. Connector
   3. End Point
   4. Subscription Class
   5. Parameters
   6. Subscriber
   7. Notify On Missed Run
   8. Notification Email
   9. Delivery Time
   10. Time Zone

   For a description of the fields, see Create Subscription [page 85].
5. When finished, choose *Submit*.

3.10.4 Enable/ Disable Subscription

Use this action to enable and disable subscriptions.

Context

Subscriptions can be enabled and disabled at any time.

Note that in order to edit a subscription, it must first be disabled.

Procedure

1. On the Self-Service Dashboard, choose the *Integration Subscriptions* tile.

   The Subscription List page opens.
2. To select the subscription, choose the subscription name hyperlink.

   The Subscription Details page opens.
3. In the upper-right side of the page, choose one of the following:
   - To enable a disabled subscription, choose *Enable*.
     The *Enable Subscription* dialog box opens.
     To continue, choose *Enable*. The Details page displays the new status of the subscription.
   - To disable an enabled end point, on the Details page choose *Disable*.
     The *Disable Subscription* dialog box opens. To confirm the action, choose *Disable*. The Details page displays the new status of the subscription.

3.10.5 Remove Subscription

Context

This action allows you to remove (delete) a subscription from the system. Removing a subscription can't be reverted.

Note that in order to remove a subscription, it must first be disabled.

Procedure

1. On the dashboard, select the *Integration Subscriptions* tile. The Subscription List page opens.
2. Choose the subscription name hyperlink.
3. On the *Details* tab, choose *Remove*.
4. To confirm the action, in the *Remove Subscription* dialog box, choose *Remove*.

   The Subscription List page opens. The subscription is removed from the list and system.

3.10.6 Test Subscription

Test the connectivity to a designated subscription end point.

Context

Subscriptions must be enabled to schedule or trigger a test run. All end point categories can be tested.

Procedure

1. On the Subscription List page, choose the subscription name hyperlink to open the details page for that subscription.

   The *Detail* tab is the current view.
2. On the upper-right side of the page, choose *Run Now*.

   A *Confirmation* dialog box confirms the subscription trigger event, and then you're asked to confirm to run the subscription now.
3. Choose *OK*.

   A second dialog box confirms that the subscription was scheduled. It runs based on the schedule defined for the subscription.
4. Choose *OK*.

   The subscription details page opens.

   At the bottom of the page, you can view recent subscription activity. Under *Type*, the filter displays up to the last 10 `Scheduled` subscription activities and `Manual` activities (generated by the *Run Now* trigger action).

   To view all subscription activities, choose the *See More* hyperlink to open the *Integration Audit Trail*. You can also access the activity from the *Monitor Activity* tile on the dashboard, which displays all activities for the selected subscription. For more information, see Monitor Activity [page 89].

3.11 Monitor Activity

Describes the transaction activities you can monitor and troubleshoot.

On the dashboard, the *Monitor Activity* tile opens the Monitor Activity list page. The page displays the status and activity details of connector upload and download processing, transactions for event driven integrations, and payload transport details.

The information is organized on tabs based on the integration types of *Batch*, *Real Time*, *Payload Transport*, and *Subscription*.

> **Note**
>
> - The *Activity* dropdown displays POST transactions that have been received from SAP Ariba and transferred to SAP Fieldglass.
> - The System Audit Trail captures all actions related to connectors, endpoints, and subscriptions that Configuration Manager Users perform in relation to integration.

Batch

The *Batch* tab displays batch transaction details that process through upload and download connectors. Batch transaction details also display in the *Integration Audit Trail* tab on the connector Integration page, and on Connector List page by clicking *Last Run Date* or *Run Count* hyperlink of a specific connector.

You can download the original upload file, error log, error upload file, or error log for a transaction. In the detail section, choose the file option from the list, choose a format option, and then choose *Retrieve*.

The following table provides a description of the fields in the list section on the *Batch* tab.

ID	Name	Start Time/Stop Time	Duration	Status
Zid of the transaction.	Name of the transaction.	Timestamp, based on locale.	Processing time (ss:ms).	Success Failed

Real Time

The *Real Time* tab displays transaction details that process through real-time event driven integrations. An example of an event driven transaction is when an invoice or job posting is submitted, it's pushed real time for approval.

For real-time transactions that fail because of an error, you can choose the transaction ID hyperlink to display the details and troubleshoot. When the `Status` = `Error`, the *RePush* button allows you to resend the data message associated with a real-time transaction that failed. If the repushed transaction processes through, the status updates accordingly. If the transaction fails again, the status defaults to `Error`. You can repush the data message for a transaction up to six times.

The following table provides a description of the fields in the list section on the *Real Time* tab.

ID	Object ID	Request Time	Process Time	Module	Triggering Activity	Status	Attempts
Zid of the transaction.	ID of the object in the transaction, for example, invoice or job posting number.	Timestamp (date and time).	Processing timestamp (date and time).	SAP Fieldglass module that generated the transaction, for example, invoice or job posting.	Action that triggered the event, for example, the close or reject of an invoice.	Status of the transaction. All Error In Process N/A OK Upload Data Error	Number of times the transaction was submitted or resubmitted.

Payload Transport

The *Payload Transport* tab displays transaction details that process through connector publish subscribe activity. This tab is only related to the *Publish/Subscribe Framework* tile on the dashboard. For more information, see Test Payload [page 130].

In the list section, the *RePush* button allows you to select and resubmit a transaction. In the detail section, the *Retrieve* button allows you to download the payload in the format you choose.

The following table provides a description of the fields in the list section on the *Payload Transport* tab.

ID	Company Code	Object ID	Insert Time	Process Time	Status	Attempts
Zid of the transaction.	Company code the payload was generated for.	ID of the object being tested, for example, a job seeker ID for a job seeker payload.	Insertion timestamp (date and time).	Processing timestamp (date and time).	All Retry Sent	Number of times the payload triggered.

Subscription

The *Subscription* tab displays transaction details that process through connector subscription activity. These transactions are related to activity configured in the *Integration Subscriptions* tile on the dashboard. For more information on subscriptions, see Integration Subscriptions [page 84].

For download subscription transactions that fail because of a file delivery error, you can choose the transaction in the table to display the details and troubleshoot. If the `Status` is `document:Ok;delivery:ERROR`, the *RePush* button allows you to resend the specific file from the associated connector transaction to the configured end point. This error occurs if a client's server goes down and it can't accept SFTP access at the time of the transaction. The *RePush* button provides support to repush these failed transactions.

The following table provides a description of the fields on the *Subscription* tab.

ID	Company	Name	Start Time	Duration (Seconds)	Status	Size (KB)
Zid of the transaction.	Company code associated with the subscription.	Name of the subscription.	Timestamp when the subscription triggered, based on locale.	Processing time (ss:ms).	Status of the document and the delivery. OK Error In Progress	Size of the file.

3.12 SAP Task Center

To enable the push of task updates from SAP Fieldglass to SAP Task Center, set up the authentication credentials from SAP BTP cockpit where your SAP Task Center instance was created.

Prerequisites

You've created a new service instance as described in step 1 under Connect SAP Fieldglass and SAP Task Center.

> **Note**
>
> In this step, you get the service key that contains the values required for the Integration Service Registration Center.

You've enabled SAP Task Center in SAP Fieldglass as described in Enable SAP Task Center in SAP Fieldglass [page 95].

You've imported the trust certificates into SAP Fieldglass environments as described in Establish Trust with SAP Destination Service [page 96].

Procedure

1. Sign into Configuration Manager and choose the *SAP Task Center* tile.

   The SAP Task Center page opens.

   > **Note**
   >
   > If you get an error stating the push capability is disabled, refer to the first Prerequisites for resolution. Once the capability is enabled and cache is refreshed, you can proceed.

2. Choose *Configure*.
3. In the *Setup* dialog box, enter the service key details you received when following the prerequisites for creating a new service instance.

Required Entries	Details
Destination URL	Copy the `endpoints > inbox_rest_url` attribute value from the prerequisites section. For example, https://api.one-inbox-service-sap.cfapps.sap.hana.ondemand.com/task-center-service.
Certificate Based	Defines whether authentication is certificate-based. Options are Yes and No. No is the default value.
OAuth URL	Copy the `uaa > url` attribute value from the prerequisites section. For example, https://ies-one-inbox.authentication.sap.hana.ondemand.com.
Client ID	Copy the `uaa > clientid` attribute value from the prerequisites section.
Client Secret	Copy the `uaa > clientsecret` attribute value from the prerequisites section.

4. Choose *Save*.

   The values are saved in the *Authentication* section on the SAP Task Center page. The push capability is now enabled.

Next Steps

Once the configuration is complete in SAP Fieldglass, you need to update SAP Task Center destination settings to PUSH using SAP BTP cockpit where your SAP Task Center instance was created.

SAP Task Center automatically enables the push functionality within SAP Fieldglass by using the push configuration end point (`<SAP Fieldglass Task Center Endpoint>/api/v1/task-provider/v2/configuration/push?languages=en-US,de-DE`). Entries are generated in the `data_transport` table for valid modules/activities.

Check SAP Fieldglass Push Capability Status

To check the push capability status, use the capabilities endpoint (`<SAP Fieldglass Task Center Endpoint>/api/v1/task-provider/v2/capabilities`), specifically the `tasks.push` value.

Sample Code

Capabilities

```
{
    "value": [
        {
            "name": "tasks.pull",
            "value": "true"
        },
        {
            "name": "taskDefinitions.pull",
            "value": "true"
```

```
        },
        {
            "name": "tasks.push",
            "value": "false"
        }
    ]
}
```

The push capability status is enabled when both of the following conditions are met:

> **Note**
>
> The following updates to the `CompanySysEnv` table require assistance from SAP Fieldglass support, or a user with SA admin rights who can access and update the *Maintain Table* option. In addition, update the *Company SysEnv Variables* cache in *Maintain Server Caches*.

1. SAP Task Center Setup must be completed within the SAP Fieldglass application as described in the preceding procedure.

Check Push Functionality Status

To check the push functionality status, the status is determined by the value of SAP_TASK_PUSH_ENABLED in the `CompanySysEnv` table for the company code:

Value	Status
Default	Disabled
true	Enabled
false	Disabled

To continue with the setup of SAP Task Center, see step 3 in Connect SAP Fieldglass and SAP Task Center - SAP Help Portal.

3.12.1 Supported Use Cases

An overview of the SAP Fieldglass use cases supported in SAP Task Center.

Use Case	Release Date
Job Posting	2021.05
Work Order	2021.05
Work Order Revision	2021.05
SOW	2021.05
SOW Revision	2021.05
SOW Response	2021.05
SOW Response Revision	2021.05
Project	2021.05

Use Case	Release Date
Profile Worker	2021.05
Time Sheet	2022.05
Invoice	2022.05
Misc Invoice	2022.05
SOW Invoice	2022.05
Consolidated Invoice	2022.05
SOW Event	2022.05
SOW Schedule	2022.05
SOW Fee	2022.05
SOW Worker	2022.05

3.12.2 Enable SAP Task Center in SAP Fieldglass

The SAP Task Center service provides a single entry point for users to access all their assigned tasks across various SAP applications in a central inbox.

Prerequisites

You've downloaded the SAML 2.0 metadata file from the Identity Authentication service using the URL `https://<Identity_Authentication_tenant>.accounts.ondemand.com/saml2/metadata`.

> ✤ Example
>
> `https://my-ias-tenant.accounts.ondemand.com/saml2/metadata`

For more information, see Tenant SAML 2.0 Configuration in SAP Cloud Identity Services - Identity Authentication.

Procedure

1. On the Single Sign-On Setup page, choose *Edit*.

   The SSO configuration opens in the setup wizard.
2. In the *Identity Provider Details* section, choose the *Upload* button to upload the client's metadata file using the *Identity Provider Metadata Import* tool, as described in Single Sign-On [page 114]. Alternatively, you can enter the information manually.
3. In the *SAML Identity Location* property, choose *Attribute*, and in the *Attribute Name* text box, type **`sap_uid`**.

4. In the *Service Provider Details* section, choose *Yes* for the *Enable Deep Linking In Notifications?* property.
5. Contact SAP Fieldglass Customer Support at https://www.fieldglass.com/customer-supportInformation to request assistance with enabling the custom script `sso.sapid2uname` for the company.

> **Note**
>
> If another SSO script is already enabled, in relation to an existing Identity Provider setup, this may cause some conflict and require further analysis on the overall configuration.

3.12.3 Establish Trust with SAP Destination Service

Describes how to establish trust with SAP Destination service.

Procedure

1. To export your trust certificate in the SAP BTP cockpit where your SAP Task Center instance was created, navigate to your Cloud Foundry subaccount and then select *Connectivity Destinations* from the navigation area on the left.
2. Select *Download Trust*.

> **Note**
>
> Make sure to renew your trust certificate before it expires. For the time while you are renewing the trust certificate and updating it for SAP Fieldglass, you may not be able to work on tasks, nor receive task updates. For more information, see Renew Destination Trust Certificates.

3. Save the trust certificate file locally with extension `.cer`.
4. Contact your SAP Fieldglass representative to upload this certificate in the SAP Fieldglass tenant Truststore.

   Limitations

   SAP Fieldglass currently only supports these limited modules for the SAP Task Center service:
   - Job Posting
   - Work Order
   - Work Order Revision
   - Statement of Work (SOW)
   - Project
   - Profile Worker

Next Steps

For information on enabling SAP Task Center Push in SAP Fieldglass, see SAP Task Center [page 92].

3.13 Time Processing Tenant

Companies using the Time Processing service with SAP Fieldglass can set up a Time Processing tenant and establish a connection from the SAP Fieldglass configuration manager to the Time Processing configuration manager.

Time Processing provides a simplified time management micro service that can process all time management needs, eliminating redundant investments in resources and effort. When Time Processing is enabled in SAP Fieldglass, APIs provide access to time management information via user interfaces within SAP Fieldglass. To use the service, your company must have a Time Processing tenant set up to manage the necessary time entry configuration elements, data management, and other required components.

SAP Fieldglass provides companies an option to create and manage their Time Processing tenant directly from their Configuration Manager dashboard. A connection must be established between SAP Fieldglass and your Time Processing tenant. To create the connection, your SAP Fieldglass company must have at least one Configuration Manager user with access to the Configuration Manager dashboard.

Upon tenant creation, a predefined set of configuration files is automatically uploaded to your tenant. These files are required to successfully connect and transact with SAP Fieldglass. These files do not include any company-specific configurations; however, the files do include some prepackaged options for pick list APIs to SAP Fieldglass and options to retrieve and utilize SAP Fieldglass rate categories, work schedules, and corporate calendars.

Once the connection is established from SAP Fieldglass to your Time Processing tenant, your Configuration Manager users are automatically created in the tenant with access to that system's Configuration Manager dashboard via single sign-on.

3.13.1 Tenant Connection Types

Describes the options available to manage the tenant connection.

From the SAP Fieldglass Configuration Manager dashboard, you can create your Time Processing tenant or connect to an existing tenant.

There are two setup types: SAP Fieldglass Managed and Client Managed.

- The SAP Fieldglass Managed setup allows you to use the Fieldglass system information to establish the connection to your Time Processing tenant. In this scenario, Fieldglass acts as the client and manages the required information.
- The Client Managed setup can be used if your company has already established a Time Processing tenant. With this option, you can use your time processing client information to establish the connection from your SAP Fieldglass company.

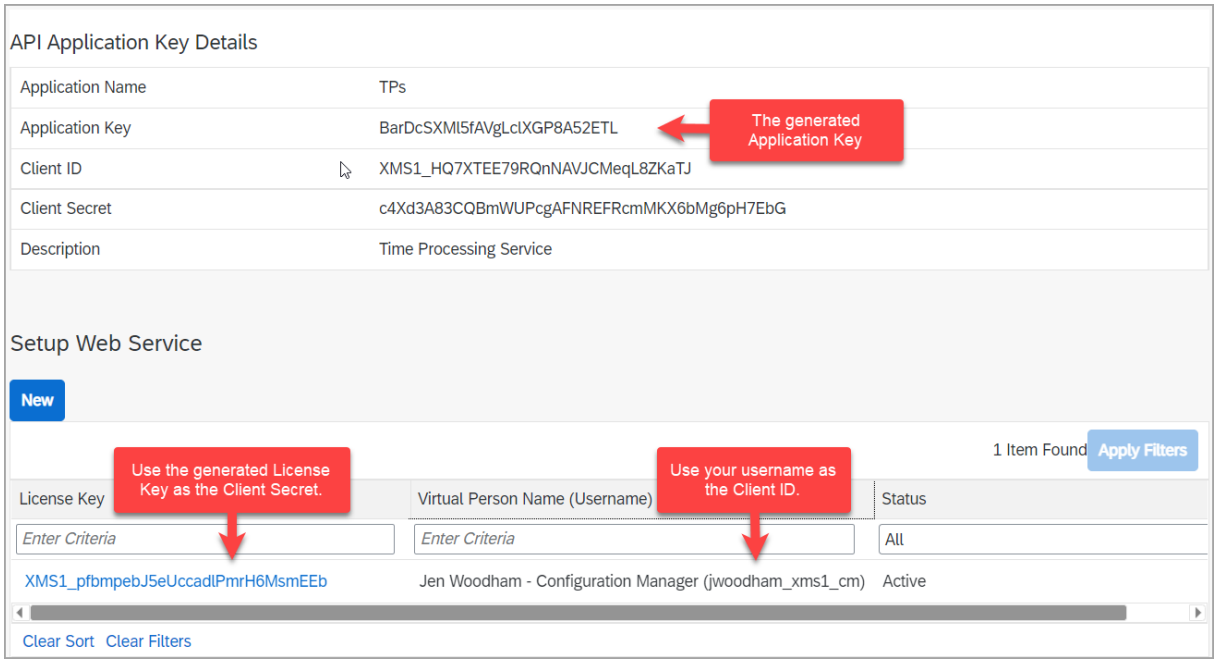
3.13.2 Tenant Creation

The connection between SAP Fieldglass and the Time Processing service is established via the Configuration Manager dashboard.

Before completing your tenant setup, your company's configuration manager will need to generate the API Application Key, Client ID, and Client Secret for the tenant. This is necessary to create sign in credentials for Configuration Manager users and allow access via SSO. Once created, the necessary values can be copied to your tenant setup.

- Create an API application key for the Time Processing application using the *API Application Key* tile on the Configuration Manager dashboard.
- You'll need to add a new user in the Web Service Setup section to generate the TP tenant Client ID and the Client secret for each user.

> **Note**
>
> For Time Processing, the Client ID and Client Secret generated when the API application key is created, are not used in the corresponding fields during your tenant setup. Instead, the Username and License Key values, generated when users are added, are used to create user access in your tenant.



If you've already created an API application key for time processing, you can use the *API Application Keys* tile to locate the necessary information. For information, see API Application Keys [page 43]

Next step: Create your Time Processing tenant.

Creating a Time Processing Tenant

Describes the steps to set up your Time Processing tenant.

Context

The *Time Processing Tenant* tile provides an option to configure and manage your Time Processing tenant by providing the information necessary to establish a connection between the two systems. Once the connection is created, configuration manager user accounts are automatically created in the Time Processing tenant so that users can seamlessly access and manage their tenant setup. In addition, the predefined setup files are automatically loaded so that you can access your tenant and complete any additional configuration.

If SAP Fieldglass is managing your company's Time Processing tenant setup, some required information is automatically populated on the Setup page. Do not change the auto-populated values.

To get started, select a *Setup Type*, then use the table below to complete your setup. The *Tenant Name* is your SAP Fieldglass company code and that value defaults and cannot be edited. Once complete, select *Create* to initiate the process of creating your Time Processing tenant. Note that you cannot edit the Time Processing tenant connection settings from SAP Fieldglass after the tenant is created.

Time Processing Tenant Field Definitions

Setup Type	When SAP Fieldglass Managed is selected, the system uses Fieldglass provided values to manage the connection and those values are auto-populated. You can review and accept the default values during tenant creation. If you've already established a Time Processing tenant, you can select Client Managed to enter your own values.
Token URL	Required to authorize users' access to the Time Processing configuration manager.
Time Processing Client ID	Required to authenticate the connection.
Time Processing Client Secret	Required to authenticate the connection.
Verification Key	Required to authenticate the connection.
Identify Zone ID	Required to authenticate the connection.
Tenant Configuration Template	SAP Fieldglass provides a generic configuration template. Once your tenant is created you can add or upload additional template configuration.
Fieldglass API URL	The URL for your company's SAP Fieldglass environment.
Fieldglass Client ID	Use your SAP Fieldglass Configuration Manager username, ending in '_cm'.
Fieldglass Client Secret	Use the License Key generated in the Setup Web Sevice section.
Fieldglass Application Key	Generated value from the API Application Key.

Results

Your Time Processing tenant is created and a set of configuration files are automatically uploaded to the tenant. The values you entered to create the connection cannot be edited. You can now use the Time Processing Tenant tile to access your tenant and complete any necessary configuration.

3.13.3 Predefined Setup Files

Describes the files that are included in the ZIP package that is uploaded automatically upon tenant creation.

Some of the files listed in the table below are required to maintain the connection between SAP Fieldglass and the Time Processing tenant, and to define the attributes needed within your Time Processing tenant.

Note that many of these files are necessary for Time Processing to be used with the SAP Fieldglass Assignment Management module. Some files create generic data elements that can be updated as needed using the Upload Tenant Configuration action.

Configuration File Name	Purpose
Type: apiConnectionDefns	
Self_Connection.json	Used to create a connection to and from Time Processing.
FG_Admin_Connection.json	Defines the connection for the admin objects between Time Processing and SAP Fieldglass
FG_Workflow_Connection.json	Defines the connection for the workflow objects between Time Processing and SAP Fieldglass
FG_TimeBundle_Connection.json	Defines the connection for the Time Bundle object between Time Processing and SAP Fieldglass
Type: attributeDefns	
Resource_detail_work_schedule.json	Attribute that defines the work schedule (if available) for a given resource and date.
Resource_corporate_calendar.json	Attribute that defines the corporate calendar (if available) for a given resource.
Rate_category.json	Rate category connection to SAP Fieldglass. Can be used within business rules to specify under what rate category to allocate time.
Res_ratelookup_picklist.json	Pick list that has an API reference to the SAP Fieldglass resource rate lookups. This pick list can be used within a time attribute to collect data on any object within Time Processing. This is required on time bundles when sending data to time journals.
Res_assignment_picklist.json	Pick list that has an API reference to the SAP Fieldglass assignments. This pick list can be used within a time attribute to collect data on any object within Time Processing. This is required on time bundles when sending data to time journals.
Res_costcenter_picklist.json	Pick list that has an API to reference to the SAP Fieldglass Cost Center list. This pick list can be used within a time attribute to collect data on any object within Time Processing.
Res_jobcode_picklist.json	Pick list that has an API to reference to the SAP Fieldglass Resource Job Code associations. This pick list can be used within a time attribute to collect data on any object within Time Processing.
Res_PO_line_item_picklist.json	Pick list that has an API reference to the SAP Fieldglass Assignment Management PO Line Item. This pick list can be used within a time attribute to collect data on any object within Time Processing. This is required on time bundles when sending data to time journals.
Type: configs	

Configuration File Name	Purpose
Enable_Bulk_Subscription.json	Configures the option to receive time bundles in batches from Time Processing to SAP Fieldglass.
Batch_Size.json	Configures the batch size for the Enable_Bulk_Subscription.json
Batch_Retry_Limit.json	Configures the number of times to retry the bulk subscription process if the target system is down.
Type: masterDataDefns	
RateCategory.json	Defines the Rate Category master data.
WorkSchedulePatternDefinition.json	Defines the Pattern for a work schedule.
Work_Schedule.json	Defines the Work Schedule.
Corporate_Calendar_Entries.json	Fetches and holds the data from the Corporate Calendar associated to the resource.
Corporate_Calendar.json	Defines the Corporate Calendar that acts as a parent table to the entries below.
Resource_Detail_Work_Schedule.json	Defines the structure of the association between resource detail and work schedule.
Resource_Detail_Corporate_Calendar.json	Defines the structure of the association between resource detail and corporate calendar.
Type: objectDefns	
Resource_Detail_Update.json	Associates master data definitions (work schedule & corp. calendar) to the resource detail.
Type: picklistDefns	
FG_Rate_Category_Picklist.json	Picklist with API to fetch Rate Categories from the SAP Fieldglass admin object.
RE_assignements_picklist.json	Picklist with API to fetch Assignments from SAP Fieldglass with a filter on resource supplier.
RE_CostCenter.json	Picklist with API to fetch Cost Centers from the SAP Fieldglass admin object.
RE_jobcode_picklist.json	Picklist with API to fetch Job Codes associated to a resource.
RE_PO_LineItems_Picklist.json	Picklist with API to fetch PO Line Items on an assignment.
RE_Rate_Lookup_Picklist.json	Picklist with API to fetch Rate Lookups from the SAP Fieldglass admin object.
Type: subscriptions	
TimeBundleCompletedSubscription.json	Defines which event the target system subscribes to.
Type: Default	
defaults.json	Mandatory file that is required to use Time Processing.

3.13.4 Tenant Management Actions

Configuration manager users can use the Time Processing Tenant tile to perform the following actions:

- Access your Time Processing configuration manager to update and manage your tenant configuration.

- Upload additional tenant configuration files.
- Synch your time data from SAP Fieldglass to Time Processing.
- Access your time templates to edit and/or create new templates.

Uploading Tenant Configuration

Describes the steps to upload new or updated company-specific Time Processing configuration files from the SAP Fieldglass Configuration Manager self-service dashboard.

Context

You can use the *Time Processing Tenant* tile to upload your company-specific tenant configuration files. Upon tenant creation, some generic company configuration options were uploaded to your tenant. These options can be updated and new options can be added in your tenant using the *Upload Tenant Configuration* action.

To perform this action, the required files must be contained in a zipped file. Select the tile and then follow the steps below to upload the necessary zipped file.

Procedure

1. From the Actions menu, select *Upload Tenant Configuration*.
2. Select *Choose File* to locate the zipped file.
3. Select the zipped file. *ZIP* is the only file format allowed.
4. Select *Upload* to complete the process.

Triggering Data Synchronization

You can use the Time Processing Tenant tile to sync data from SAP Fieldglass to Time Processing.

Context

Several APIs communicate SAP Fieldglass data to Time Processing, such as objects, work schedules, corporate calendars, etc. These APIs run on a regular schedule, however if there is an immediate need, the configuration manager can trigger the synchronization manually.

To sync data, select the *Trigger Data Synchronization to Time Processing* option from the Actions menu. The process runs automatically. No additional steps are required.

Accessing the Time Processing Configuration

You can use the Time Processing Tenant tile to access and manage your Time Processing configuration.

Context

The SAP Fieldglass provided setup files contain default files that are required for the tenant to function. In addition, some generic configuration files are also provided to populate some of the elements needed to use Time Processing with SAP Fieldglass, such as time attributes, master data definitions, and roles. You may wish to add more values or create new setup elements such as time templates, processing rules, and time event types.

From the Actions menu, select *Access Time Processing Configuration*. The Time Processing Configuration Manager dashboard opens in a new window. You can select any element to view the existing values and/or add new values.

4 Partner Management

The Partner Management tile on the Self-Service Dashboard allows you to set up and manage integrations with third-party digital partners.

Partner Management provides access to a growing network of partner integrations that are being migrated from the SAP Fieldglass application to the self-service framework on the dashboard. When a migration is completed, a tile labeled with the partner's name is added to the Partner Management section. Selecting the tile opens that partner's administrative setup pages, where you can set up and manage the integration, without having to contact SAP Fieldglass for assistance.

OpenText Corporation, an Enterprise Content Management (ECM) provider, is the first partner integration migrated to the dashboard. The integration with OpenText allows clients to store all document attachments in the OpenText ECM repository instead of in the SAP Fieldglass database, while only the attachment metadata is stored in SAP Fieldglass. All supplier uploaded attachments are stored in SAP Fieldglass and not in OpenText.

4.1 OpenText ECM

Set up and troubleshoot your OpenText ECM end point on this page. After creating an end point, new buyer and worker attachment files are stored in the OpenText repository.

Overview

The integration of SAP Fieldglass and OpenText ECM allows clients to store and retrieve all buyer and worker attachments in the OpenText ECM repository instead of in the SAP Fieldglass database, while only the attachment metadata is stored in SAP Fieldglass. All supplier uploaded attachments are stored in SAP Fieldglass and not in OpenText ECM.

The OpenText ECM environment is set up and controlled by the buyer's configuration manager. Set up includes configuring an end point in OpenText ECM to connect to the OpenText API for the ability to save and retrieve documents.

Process Workflow

In SAP Fieldglass, the configuration manager chooses the *OpenText ECM* tile on the Self-Service Dashboard to open the OpenText ECM page and create an end point. The end point enables the OpenText API to access the resources on a server. After creating an end point, additional functions are available to edit and disable the end point, as well as enable a disabled end point. You can edit the Username and Password details of the end point or disable the end point at any time.

Authorized users can upload attachments to the documents that are stored in OpenText ECM. There's no impact to old attachments; however, if you want to move old attachments to OpenText, contact your SAP Fieldglass representative.

SAP Fieldglass pushes the attachment to the repository via the OpenText API using the login details saved in the end point setup. Before sending the file to OpenText, SAP Fieldglass performs a Clam AntiVairus scan. The file header of the attachment is stored in SAP Fieldglass.

When retrieving data from OpenText to display in SAP Fieldglass, SAP Fieldglass accesses the attachment stored in the repository via the OpenText API and using the login details saved in the end point setup. A virus scan isn't performed when a file is retrieved from OpenText.

If a user can't open an attachment on the *Details* page or on a form page, and the problem is because of an issue reaching the end point, an error message displays in the *Attachment* section, and the *View* and *Download* links are unavailable. The error message states: `The attachment cannot be opened. Refresh the page and try again or contact your configuration manager for assistance`. The user can proceed as described in the message.

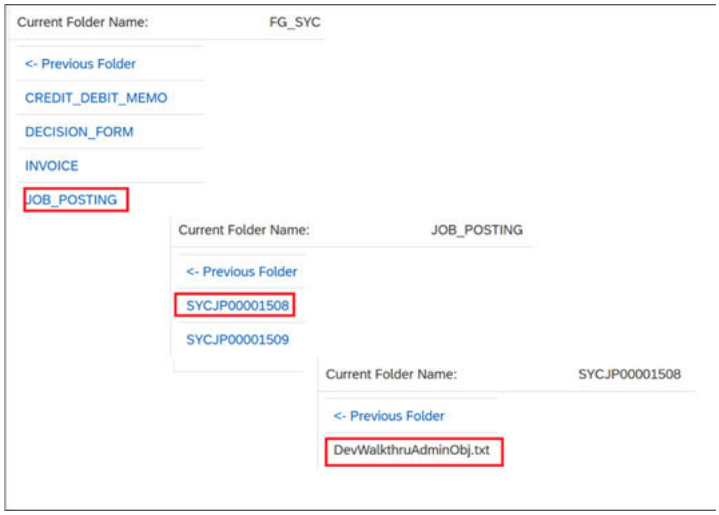
> **Note**
>
> When a field is updated via conversion, it doesn't update the revision time stored on the document. If particular downloads need to capture (or not capture) changes, then clients can work with their SAP Fieldglass representative to update the 'Last Run Time' on those downloads.

Folder Structure in OpenText ECM

SAP Fieldglass creates a folder structure in OpenText ECM with one folder per module when a module has one document with an attachment.

For example, when a job posting is created with an attachment, SAP Fieldglass creates the parent folder for the Job Posting module. Then it creates a subfolder for the job posting (with the ID as the folder name) and stores all attachments of that job posting inside that folder. A folder is only created in the OpenText ECM repository when a module has an attachment. This process applies to all SAP Fieldglass modules that support (see table below) creating documents with attachments.

In the following example, once a job posting is created with an attachment, the parent folder `JOB_POSTING` gets created under the main folder of the company `FG_SYC`. Then a folder for the job posting ID is created, and all attachments related to that job posting are stored within it.



> **Note**
>
> If all the files in a folder are deleted, either through SAP Fieldglass or by an OpenText admin who can delete files directly in the repository, SAP Fieldglass doesn't automatically delete the folder.

Additional Considerations

- **Personally Identifiable Information (PII)**
  When an attachment is stored in OpenText ECM, SAP Fieldglass handles a PII erasure request as follows:
  - SAP Fieldglass sends a delete request to the attachment in OpenText ECM, and then Opentext returns a delete confirmation response back to SAP Fieldglass.
  - The link and metadata stored in SAP Fieldglass related to the attachment are deleted.
  - SAP Fieldglass isn't responsible if a buyer has copies of the attachment and has stored it elsewhere.
- **Multi-Tenant Companies**
  No specific changes are required to implement OpenText integration for a multi-tenant company.
- **Multiple MSP Companies**
  The attachments of all MSP's in an instance are stored in one OpenText ECM end point. SAP Fieldglass doesn't control the visibility of attachments stored in OpenText ECM. However, the job posting or SOW document visibility is controlled within SAP Fieldglass, which automatically controls the visibility of its associated attachments.
- **Customers in European Union (EU)**
  SAP Fieldglass isn't responsible for validating if the OpenText ECM repository of an EU customer is located in an EU region. Since the customer configures the end point, they're responsible for complying with EU regulations regarding the storage of attachments.

Supported Modules

The following SAP Fieldglass modules support attachment uploads and storing the attachments in OpenText ECM with only the metadata stored in SAP Fieldglass.

Supported Modules
Job Posting
Job Seeker / Applicant / Candidate
Work Order / Quick Hire
Work Order / Work Order Credit / Quick Revision
Worker
Time Sheet
Invoice / Credit Memo / Debit Memo
RFX / SOW Bid
SOW / SOW Revision
SOW Line Items
SOW Worker
SOW Invoice / Credit Memo / Debit Memo
Profile Worker
Candidate Portal
Integration

Supported Documents and Attachments

The following table describes the attachments that a user can add and whether the attachment is sent to OpenText ECM or stored in the SAP Fieldglass database.

Document	Submitted By	Is Attachment Stored in OpenText?	Comments
Job Posting	Buyer	Yes	
Job Seeker Resume	Supplier	No	Stored in SAP Fieldglass to protect privacy of confidential information on a Job Seeker/Worker resume.
Work Order/WOR	Buyer	Yes	
Timesheet	Worker	Worker – Yes	
	Supplier	Supplier – No	
Expense sheet (ES) attachment and attachment to individual expense code within an ES	Worker	Worker – Yes	
	Supplier	Supplier – No	
Candidate	FCP Worker	Yes	

Document	Submitted By	Is Attachment Stored in OpenText?	Comments
Workforce	Buyer Supplier	Buyer created workforce – Yes Supplier created workforce – No	
SOW Bid	Buyer	Yes	
SOW Bid Response	Supplier	Supplier – No	
SOW	Buyer Supplier	Buyer – Yes Supplier – No	
SOW Response	Supplier	Supplier – No	
Clauses	Supplier	Supplier – No	
Event	Supplier Worker	Worker – Yes Supplier – No	
Schedule	Supplier Worker	Worker – Yes Supplier – No	
RFX	Buyer Supplier	Buyer – Yes Supplier – No	
Holdback Items	Supplier Worker	Worker – Yes Supplier – No	
SOW Worker Timesheet Expense Sheet	Supplier Worker	Worker – Yes Supplier – No	
SOW Worker Resume	Supplier SOW Worker	No	Uploaded by supplier/SOW Worker when they add a SOW Worker.
Profile Worker	Buyer Supplier	Buyer – Yes Supplier – No	
Decision Form	Buyer	Yes	
RFX	Buyer Supplier	Buyer – Yes Supplier – No	RFX is being sunset. Is supported if used and attachments are uploaded.
Project	Buyer Supplier	Buyer – Yes Supplier – No	
Invoice Revised/Reversed Invoice	Supplier	Supplier – No	

Document	Submitted By	Is Attachment Stored in OpenText?	Comments
SOW Invoice Revised/Reversed SOW Invoices	Supplier	Supplier – No	
Miscellaneous Invoice	Supplier	Supplier – No	
Consolidated Invoice	Supplier	Supplier – No	
Credit Memo Debit Memo	Supplier	Supplier – No	
Attachments uploaded to complete Activity items	Buyer Supplier Worker Profile	Yes	
Profile picture attachments	User Profile Worker Profile	Yes	
Assignment	Buyer	Yes	
Resource	Buyer Supplier	Buyer – Yes Supplier – No	

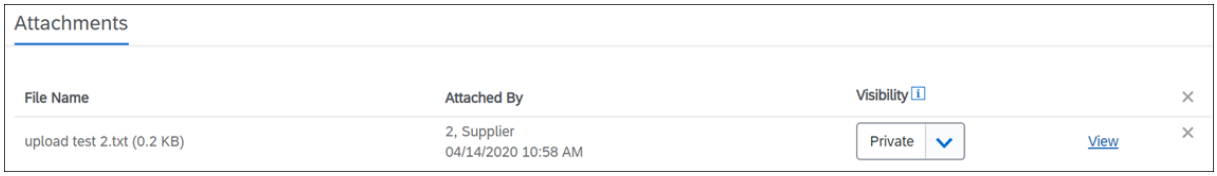
Attachment Visibility

The following table describes the visibility options for attachments.

> ⓘ Note
>
> SAP Fieldglass doesn't have control over whether a file is stored as private or restricted within OpenText ECM. SAP Fieldglass only controls the visibility when the user is in the SAP Fieldglass application.

Attachment Visibility Options	Description
Public	All buyer and supplier users can see the attachment.
Private	Only users in the buyer or supplier company can see the attachment.
Restricted	Only users in buyer or supplier company that have 'View restricted attachments' permission can select this visibility option and see the attachment. If the attachment is uploaded by a worker, then that worker can view it.

The following image illustrates that if an attachment is marked as private or restricted, then the file is only visible in the SAP Fieldglass application to the users who meet the visibility conditions. Storing the file in OpenText doesn't change this behavior inside the SAP Fieldglass application.



4.1.1 OpenText ECM Details

On the Self-Service Dashboard, the *OpenText ECM* tile opens the OpenText ECM details page where you can create an OpenText ECM end point. The page displays no data until you create the end point. After you create an end point, the page displays the end point details and end point name in a hyperlink that you can choose to edit the end point. You can also edit the username and password details of the end point, disable the end point, and re-enable a disabled end point.

4.1.2 Create End Point

Create an end point to establish where to save and retrieve documents in OpenText ECM.

Context

Once you create the end point, new attachment files are stored in the OpenText ECM repository.

Procedure

1. On the OpenText ECM details page, choose *Create End Point*. The *Create End Point* dialog box opens.
2. Complete the following mandatory fields:
   - *End Point URL*
     Enter the end point URL. The URL is validated to prohibit a malicious script.
   - *Username*
     Enter the username that has authority to access the end point URL. Specify an alphanumeric value.
   - *Password*
     Enter the password for the specified username. The value is masked while typing.
3. Choose the *Get Repository* button.

   The end point values are validated and submitted to the end point, and SAP Fieldglass populates the *Repository* list with the values returned from OpenText ECM.
   - If the end point URL is invalid or unreachable, SAP Fieldglass displays an error message.
   - If the URL is valid but the username/password are incorrect, OpenText ECM displays an error message.

> **Note**
>
> It's possible that the URL and login details are valid, but no repositories exist in the end point.

4. Select a repository in the list.
5. Choose *Create End Point* to complete the workflow.

4.1.3 Edit End Point

Context

When editing an end point, you can change the username and password but you can't change the end point URL or the repository. As such, when editing an end point, the *Get Repository* button is disabled and the *Repository* button is read-only. For any issues related to the repository, contact your system administrator.

In addition, when editing it's possible that the end point URL is invalid. In this scenario, when saving the edit an `End point unreachable or invalid` error message is returned when SAP Fieldglass tries to validate the username and password. To continue, cancel the edit and contact your system administrator.

Procedure

1. On the OpenText ECM details page, choose the *Edit End Point* button.
2. On the Edit End Point page, change the login credentials as needed. The fields are the same as described in Create End Point.
3. Choose *Save* to complete the workflow.

4.1.4 Disable End Point

Context

When you disable an end point, the end point is removed from the SAP Fieldglass database, and SAP Fieldglass continues to store attachments in the SAP Fieldglass database.

Procedure

1. On the OpenText ECM details page, choose the *Disable End Point* button.
2. In the *Confirmation* dialog box, choose *OK* to complete the workflow.

   On the OpenText ECM details page, the *Edit End Point* and *Disable End Point* buttons are replaced with the *Enable End Point* button.

4.1.5 Enable End Point

Context

You can enable an end point that was previously disabled. When you enable the end point, it's added back to the SAP Fieldglass database and attachments resume being stored in OpenText.

Procedure

1. On the OpenText ECM details page, choose the *Enable End Point* button.
2. In the *Confirmation* dialog box, choose *OK* to enable the end point and resume storing attachments in OpenText.

   On the OpenText ECM details page, the *Enable End Point* button is replaced with the *Edit End Point* and *Disable End Point* buttons.

4.1.6 Troubleshoot Push/Pull File Failures

Describes options for resolving file transmission issues.

Uploading Attachments

The following issues can prevent SAP Fieldglass from pushing data to the repository when trying to upload an attachment:

- Authentication failure because of an incorrect username/password.
- End point URL is currently unreachable.

These scenarios cause a hard stop that prevents uploading the attachment. To resolve the issue, contact your administrator.

Viewing Attachments

The following issues can prevent SAP Fieldglass from pulling data from the repository to display an attachment in SAP Fieldglass:

- Authentication failure because of incorrect username/password.
- End point URL is currently unreachable.
- File isn't accessible. The attachment was removed from OpenText ECM.

These scenarios cause a hard stop that prevents viewing the attachment. The OpenText API returns a value that confirms the instance is unreachable, the file wasn't found, or authentication failed. Based on that value, you can raise a case with OpenText ECM directly. SAP Fieldglass can't resolve these issues.

Resolving Issues

To resolve an authentication failure, correct the login details and then retry the login.

To resolve an unreachable end point URL, open a case with OpenText ECM directly. SAP Fieldglass helpdesk or 2L can't resolve this issue for end users.

5 Single Sign-On

The Single Sign-On (SSO) tile on the dashboard allows you to set up and manage your company's SSO independently, eliminating the need to open support cases with SAP Fieldglass to implement those actions in the company.

SSO is a session and user authentication service that permits a user to use a set of login credentials to access multiple applications.

The SSO configuration defines values for the following services:

- Identity Provider Details (IdP) – The primary role of the IdP is to authenticate the user and generate a SAML Response to be consumed by SAP Fieldglass.
- Service Provider Details (SP) – The primary role of the SP is to consume the authentication request sent by the IdP and grant access to the service for that user. In an SP-initiated SSO scenario, the SP also acts as the "initiating entity" that generates a SAML Request to be consumed by the IdP.

This functionality is available to stand-alone companies, multi-tenant companies at the individual buyer level, and child companies that are configured with the *Login authorization type* 'Single Sign-On' or 'Both' (Single Sign-On and Username), which enables users to sign in with Username/Password and then link to SSO.

Single Sign-On provides an intuitive wizard that allows you to set up, edit, and troubleshoot your SSO configuration. In addition, you receive notifications when your SSO certificate is close to expiration and needing to be updated.

Single Sign-On Workflow

After signing in as configuration manager, the functionality of the *Single Sign-On* tile depends on whether you're a new SSO client or an existing SSO client:

- For new SSO clients, the *Single Sign-On* tile opens the setup wizard and allows you to add new SSO details. For information on setting up SSO and using the setup wizard for editing details, see Single Sign-On Setup Wizard [page 114].
- For existing SSO clients, the *Single Sign-On* tile opens the Single Sign-On page focused on the *Details* tab. The tab displays your existing SSO setup details, which you can edit. The page also has tabs for viewing *SSO Login History* and the *Modification Log*. For more information, see Single Sign-On Details [page 116].

5.1 Single Sign-On Setup Wizard

Leveraging SAML-based Single Sign-On (SSO) functionality with SAP Fieldglass is a great way to provide your user population with simple, secure access to the application. Use the setup wizard to initially set up your company's SSO configuration and to edit the values when needed.

1. If you're setting up SSO for the first time, on the Self-Service Dashboard, choose the *Single Sign-On* tile.
   If SSO is already set up, choose the *Single Sign-On* tile to open the Single Sign-On page with the *Details* tab in view. Choose *Edit*.
   The Single Sign-On Setup Wizard opens.

2. Choose *Let's Get Started*.
   The *Identity Provider Details* setup opens.
3. Enter/select the configuration properties. You can enter the values manually or use the *Identity Provider Metadata Import* tool to populate the fields.

   > **Note**
   >
   > For detailed information on the properties in step 3 and step 4, see the property descriptions in Single Sign-On Details [page 116].

4. To save the changes and continue with SSO setup, choose *Next Step*.
   The *Service Provider Details* setup opens.
5. Enter/select the configuration properties.
6. To save the changes and update the SSO configuration, choose *Next Step*.
   The *Finished* step opens, confirming you've finished SSO setup.
   If you need to perform additional setup steps in the SAP Fieldglass application, such as configuring URLs and loading certificates, the information displays on the Finished page.
   In addition, the system checks the Expiration Dates on the Assertion Encryption Certificate and SAML Response Signing Certificate. If one or both expire in less than 6 months, the following warning message displays:
   `Your Assertion Encryption Certificate will expire on <MM/DD/YYYY> and SAML Response Signing Certificate will expire on <MM/DD/YYYY>.`
7. To continue, do either of the following:
   1. To open the Single Sign-On Setup details page, choose *Go to Single Sign-On Details*.
      The Single Sign-On Setup details page opens.
      You can take the following actions on the page: *Upload IdP Certificate*, *Download SP Metadata*, *Download Sample SAML Request*, and *Download Sample SAML Response*. For more information, see Single Sign-On Actions [page 120].
   2. To exit SSO setup and return to the Self-Service Dashboard, choose the *Home* button.

Considerations

The following information applies to the Company Configuration of the *Login authorization type* option:

- After successful configuration of a new SSO setup, the *Login authorization type* is updated to *Both* (from previous *Username/Password* only). In addition, if *Login authorization type* had the *Lock Default Values* check box selected, the configuration is overridden and the check box is now cleared.
- An existing SSO configuration that already had *Login authorization type* set to *SSO Only* or *Both* isn't affected.

The following information applies to the Company Configuration of the *Alert Threshold (SSO SAML Response Signing Certificate Expiration)*:

- When the existing *Login authorization type* is set to *Both* or *Single Signon* in the Company Admin, the field *Alert Threshold (SSO SAML Response Signing Certificate Expiration)* displays in the *Details* section of the buyer's Admin Configuration, for all users with permission to view the buyer's Thresholds - Alert page. The five *Threshold* text boxes default to *0*, and *Threshold Type* defaults to *Days* (only option). At least one nonzero value is required in one of the five text boxes. If the *Threshold* values are all set to zero and/or blanks, an error displays: `Threshold values are required.`
- When the existing *Login authorization type* is set to *Username/Password*, the *Alert Threshold* doesn't display on the Thresholds - Alert page.

5.2 Single Sign-On Details

The Single Sign-On page displays the details of your SSO configuration. You can edit the configuration values and take other related actions.

To view Single Sign-On details, choose the *Single Sign-On* tile on the dashboard.

Set up information displays on the following tabs:

- *Details* tab
- *SSO Login History* tab (for details, see SSO Login History [page 121]).
- *Modification Log* tab (for details, see Modification Log [page 122]).

The *Details* tab is the default view:

- For new SSO clients, the *Details* tab is populated with the values specified in the wizard during SSO setup.
- For existing SSO clients, the *Details* tab is populated with the latest setup details.

Single Sign-On Details Property Descriptions

The following SSO configuration properties are described below:

- Identity Provider Details
- Service Provider Details
- SAML Response Signing Certificates

Identify Provider Details

The primary role of Identity Provider (IdP) is to authenticate the user and then generate a SAML Response to be consumed by SAP Fieldglass.

The following table describes property names, descriptions, and any related rules.

Identity Provider Property Descriptions

Property	Description
Identity Provider Metadata Import	This import tool that allows you to upload a SAML-standard metadata file to prepopulate certain fields on the page (fields can be entered manually and/or imported). The following fields may be affected, depending on the corresponding field existing in the metadata file: • Identity Provider Entity ID • Identity Provider Login URL • Identity Provider Logout URL • SAML Response Signing Certificate After importing the metadata, the system auto-refreshes the page to show updated field information.

Property	Description
Identity Provider Entity ID (Issuer)	The Identity Provider's Entity ID (also known as the "Issuer"). IdP metadata mapping: `entityID` attribute of the `<EntityDescriptor>` element.
Identity Provider Login URL	The IdP URL where to send SAML requests. IdP metadata mapping: `Location` attribute of the `<SingleSignOnService>` element (defaults to the entry where the `Binding` attribute is `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`.
Identity Provider Logout URL	The URL to redirect the user to when they log out. IdP metadata mapping: `Location` attribute of the `<SingleLogoutService>` element (defaults to the entry where the `Binding` attribute is `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`.
SAML Identity Location	The location in the SAML Response where the user's identity is indicated. Options are *Attribute* and *Subject* (default value). If *Attribute* is selected, the *Attribute Name* text box displays to enter the identity location. If *Attribute Name* is specified, it displays on the details page below *SAML Identity Location*.
Encrypt Assertion in SAML Response	Define the encryption type for the SAML Response. Options are *No Encryption* (default value) and *Fieldglass Public Key*. If *Fieldglass Public Key* is selected, the next field (described below) displays dynamically.
Fieldglass Public Key	Depending on the selection of the prior field (*Encrypt Assertion in SAML Response)*, this field displays dynamically. If *No Encryption* was selected, this field doesn't display on the Details page. If *Fieldglass Public Key* was selected in the previous field, this field contains the value *Fieldglass Public Key* and a *Download* link displays. Click the link to immediately download the full file for the certificate (in `.cer` format), based on a key pair generated by SAP Fieldglass.

Property	Description
SAML Response Signing Certificate Upload	Allows you to upload the SAML Response signing certificate. The *Upload* button opens the *Upload Document* dialog box and allows uploading multiple certificates at the same time. Each certificate displays in the dialog box, with "X" next to each file to allow removing files from the upload. After each upload, a dialog box displays the *File Name*, *Date Uploaded* (date/timestamp value), a *View* link to display the Signature Header of the file (not the signature from the file), and "X" next to each file to allow removing one or more files from the Details page. For existing SSO clients, the File Alias for each file displays under the *File Name* field, along with the *Date Uploaded* (date/timestamp), and "X" to allow removing the file or files. Maximum allowed size of all files combined is 5 MB. A total of five files is allowed. The system auto-refreshes the page after uploading the certificate to show updated field information in the field below.
SAML Response Signing Certificate - Expiry Alerts	Notifications for expiry of the SAML Response signing certificate. *Alert Email Addresses* allows one or more email addresses, separated by a comma or semicolon, to notify when triggered by the values defined in the *Alert Schedule* field below. When a threshold has been met for the *SSO SAML Response Signing Certificate Expiration* specified in the *Alert Schedule* field below, the existing standard notification is triggered to the email addresses specified in this field. **Note** For existing SSO clients, no information displays here until you set up the email addresses and alert schedule.
Alert Schedule	Specifies up to 5 threshold periods (in days) to alert users of certificate expiration. At least one value must be specified. The same threshold values apply to all certificates. When a threshold has been met for the *SSO SAML Response Signing Certificate Expiration* process, the existing notification is triggered to the *Alert Email Addresses* specified in the *SAML Response Signing Certificate - Expiry Notifications* column above. The threshold values also display and can be edited in the *Details* section on the Thresholds - Alert page in the buyer's Admin Configuration. If edited in the Admin, the updated alert schedule displays in the setup wizard and on the Details page.

Service Provider Details

The primary role of the Service Provider (SP) is to consume the authentication request sent by the IdP and grant access to the service for that user.

The following table described the SP property names, descriptions, and any rules.

Service Provider Property Descriptions

Property	Description
SAP Fieldglass Username Format	The username format for users within SAP Fieldglass.
Assertion Consumer Service (ACS) URL	The Service Provider's ACS URL where SAML Response messages are received. This URL is generated dynamically by SAP Fieldglass to include the domain of the environment being used (production or otherwise) and company code for the logged in Configuration Manager user.
Service Provider Entity ID (SPID)	The Service Provider's Entity ID. The default value is https://www.fieldglass.com.
Service Provider Login URL	The login URL where an SP-initiated SSO session can be triggered. This URL is dynamically generated by SAP Fieldglass to include the domain of the environment being used (production or otherwise) and company code for the logged in Configuration Manager user.
SAML Request Protocol Binding	The binding to use for sending SAML Request messages (for SP-initiated SSO). Options are *HTTP-POST* (default value) and *HTTP-REDIRECT*.
Sign AuthnRequest?	Determines whether the AuthnRequest within the SAML Request should be signed. Options are *Yes* and *No* (default value).
AuthnRequest Signing Certificate	Download the AuthnRequest signing certificate. If *Sign AuthnRequest?* field above is set to *Yes*, this field contains the Header value for the certificate based on a key pair generated by SAP Fieldglass, and a *Download* link displays above the text area. Click the link to download the file in `.cer` format. If *Sign AuthnRequest?* is set to *No*, this field and the *Download* link are suppressed.
Enable Deep Linking In Notifications?	Enable deep linking within SAP Fieldglass notifications allows users to navigate directly to items within the application. Options are *Yes* and *No* (default value). **Note**: Enabling deep linking has an immediate impact on messaging, so only enable when fully ready.

SAML Response Signing Certificates

Certificates in SAML are used to handle the certificate signing and encryption keys.

The following table describes the property names, descriptions, and any rules.

SAML Response Signing Certificate Property Descriptions

Property	Description
Name	File name of each SAML Response Signing Certificate uploaded.

Property	Description
Date Uploaded	Date/timestamp of when each certificate was uploaded.
Expiration Date	Expiration date of each certificate uploaded.
View	Allows you to view each certificate uploaded. Click the *View* link next to a certificate to open a dialog box that displays the Signature Header from the file (doesn't display the signature from the file).

5.2.1 Single Sign-On Actions

Actions on Single Sign-On Details page allow you to manage your SSO setup.

The following actions are available:

- Edit Single Sign-On details
- Upload IdP Certificate
- Download SP Metadata
- Download SAML Request
- Download SAML Response

Edit Single Sign-On Details

This action allows you to edit the SSO property details.

1. On the *Details* tab of the Single Sign-On Setup page, choose *Edit*.
   The Single Sign-On Setup Wizard opens.
2. In the *Single Sign-on Setup* pane, choose the setup step to edit, either *Identity Provider Details* or *Service Provider Details*.
3. Make the necessary changes, and then choose *Next Step*.
4. When finished editing, choose *Next Step*.

Upload IdP Certificate

This action allows you to upload a SAML Response Signing file.

The following upload requirements apply:

- Maximum allowed size of all files uploaded and being uploaded is 5 MB.
- Required file format is `.cer` (base64), `.txt` (base64) or `.crt` (base64).
- If any information is missing from the file (for example, Expiration Date is missing or has passed), an error displays: `Invalid Certificate.`

To upload an IdP certificate:

1. On the *Details* tab, choose *More Actions > Upload IdP Certificate*.
   The *Upload Certificate* dialog box displays.
2. Select one or more files, and then choose *Attach*.

Once the files are uploaded, the page refreshes and the file details display on the bottom of the page (in the *SAML Response Signing Certificates* section).

If no file is selected, an error displays: `Must select a file to upload.`

Download SP Metadata

This action allows you to create and download a metadata file of the service provider details, including the ACS URL and Entity ID configured, and any certificates that need to be included (if using a signed Authentication Request or encrypted assertions).

To create and download the metadata file, on the *Details* tab, choose *More Actions > Download SP Metadata*.

The file downloads in XML format.

Download Sample SAML Request

This action allows you to generate and download a sample SAML Request file, based on the existing SSO configuration.

To download the sample file, on the *Details* tab, choose *More Actions > Download Sample SAML Request*.

The file downloads in XML format.

Download Sample SAML Response

This action allows you to generate and download a sample SAML Response file, based on the existing SSO configuration.

To download the sample file, on the *Details* tab, choose *More Actions > Download Sample SAML Response*.

The file downloads in XML format.

5.2.2 SSO Login History

On the Single Sign-On page, the *SSO Login History* tab displays the login history for all SSO login attempts.

The following table describes the field names, descriptions, and any rules.

Single Sign-On History Field Descriptions

Field Name	Description
Login Time	Date/time stamp of the successful SSO login. The date/time stamp displays in the Configuration Manager's local time zone.
Username	SSO username of the successful SSO login user. If the User ID isn't recognized or valid, the value `N/A` displays.

Field Name	Description
Error Message	Visible to buyer CM users only. The errors defined in Error Handling [page 123] (see column "Error Message for Config Manager") display in this field for each failed login attempt. The error is formatted as a hyperlink. Select the link to display the full error details (error description and SAML response) in a dialog box. If the SAML response isn't available for the error exception, only the error description displays. If the error message is too long to fully display in a single row, the text is truncated near the end of the column and appended with `...`. You can hover over the error message to display the full message text.
Result	Visible to buyer CM users only. Displays the result of each SSO login attempt (Error/Successful) that occurred when a user attempted an external SSO login. Click in the list to change the view to *All* (default), *Error*, or *Successful*.

5.2.3 Modification Log

On the Single Sign-On page, the *Modification Log* tab displays a log of all SSO configuration updates processed by actions taken on the *Details* tab.

The following table describes field names and descriptions in the log.

Modification Log Field Descriptions

Field Name	Description
Activity Time	Date/time stamp of when the modification occurred. The values display in the Configuration Manager's local time zone.
Reason	Value is a link with the text, `XXX Configuration modified.` Choose the link to open the *Modification Data* dialog box, which displays a table containing three columns, *Modified Field*, *Old Value*, and *New Value*, and corresponding data. (Old Value and New Value values are case-sensitive.) All field changes are tracked. For metadata file uploads, the fields and values prepopulated on the page are included, but the file details aren't included. For certificates uploaded, including certificates uploaded in the wizard and/or the *Details* tab via *Upload IdP Certificate*, a description displays: `Certificate added/deleted`, but the file details aren't included.
Person	SAP Fieldglass buyer login ID of the user who made the change.

5.2.4 Error Handling

When an SSO login error occurs, a record of the related error message is added to the SSO Login History page, when the user logging in via SSO encounters the related error message on the client-side login page.

If multiple errors occur during the login attempt, only the first error encountered displays (multiple errors don't display simultaneously on the login page or SSO Login History page).

SSO Login Error Messages

Error Message for Configuration Manager	Error Location	Error Message for User
The IdP URL is invalid or missing. Check the Service Provider Details configuration in the setup wizard.	SSO Login History page	"UnSupported SSO protocol."
No SAML Response received back in response to the SAML Request. Please check the ACS URL configured at the IdP, and that the RelayState parameter value is being returned.	SSO Login History page	"You are not authorized to use single-sign-on." (default)
Invalid SAML - No <Assertion> found in the SAML Response. Check the IdP for more details.	SSO Login History page	"UnSupported SSO protocol."
Invalid SAML - Error with the details of the <Assertion> found in the SAML Response. Check the IdP for more details.	SSO Login History page	"UnSupported SSO protocol."
Invalid SAML - Bad status value received. Check the IdP for more details.	SSO Login History page	"You are not authorized to use single-sign-on." (default)
Invalid SAML - SSO assertion expired. Check Service Provider and IdP clock values at the time of the assertion.	SSO Login History page	"You are not authorized to use single-sign-on." (default)
Invalid SAML - Signature verification failed. Check signature and/or certificate validity.	SSO Login History page	"You are not authorized to use single-sign-on." (default)
User is not authorized to use single sign-on. Please have your SAP Fieldglass administrator check the user account to confirm the Single Sign-On flag is enabled.	SSO Login History page	"You are not authorized to use single-sign-on." (default)

Error Message for Configuration Manager	Error Location	Error Message for User
User is not authorized to use single sign-on. Please have your SAP Fieldglass administrator check the user account to confirm the Single Sign-On flag is enabled.	SSO Login History page	"You are not authorized to use single-sign-on."

6 Publish/Subscribe Framework

Create payloads and subscribe to real-time application activity using the *Publish/Subscribe Framework* tiles on the Self-Service Dashboard.

The Publish/Subscribe Framework tiles allow you to create and manage payloads and subscriptions independently, as well as a setup wizard that allows you to configure all of these elements in one workflow.

Use the following Publish/Subscribe Framework tiles to create and manage your payload and subscription configurations.

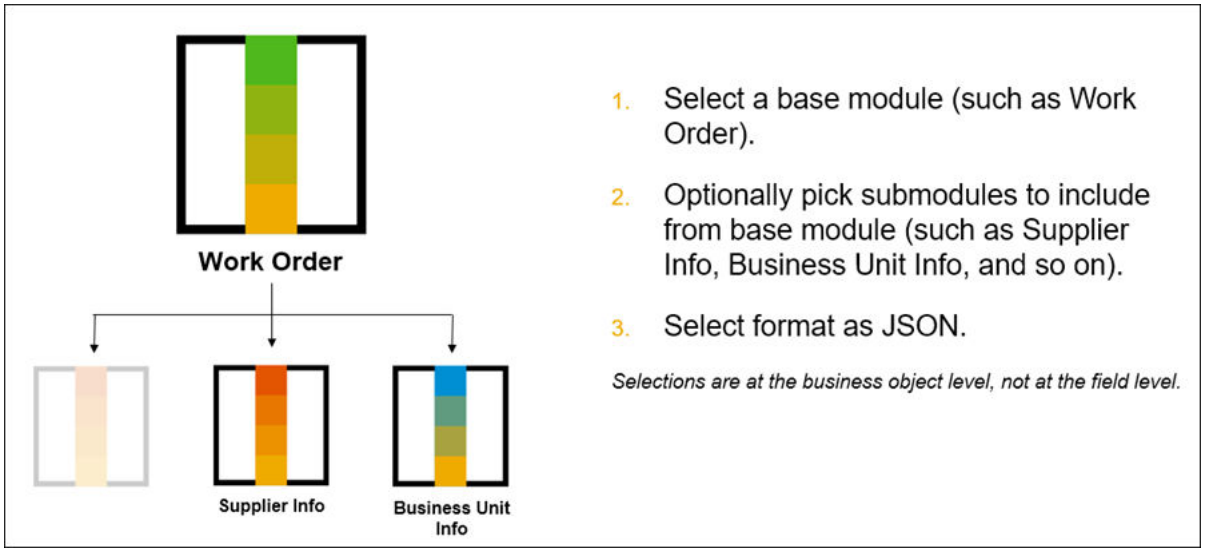
- *Pub / Sub Wizard* – Use the wizard to configure payloads and subscribe to application activities in one workflow.
- *Payloads* – Use this tile to configure the payload data elements for subscriptions to application activities (stand-alone from the wizard).
- *App Activity Subscriptions* – Use this tile to manage subscriptions to application activities (stand-alone from the wizard).

The Publish/Subscribe framework creates a new API layer that allows activity-driven payload configuration per SAP Fieldglass module, providing flexible real-time transaction data in a standard framework. The API configuration comprises three primary components, Build Payload, Event Subscribe, and Delivery Mechanism (PUSH/PULL), to get the right data at the right time. The API delivers outbound from SAP Fieldglass as a POST transaction. With the *Payload Transport* functionality, the *RePush* option allows you to resend a transaction to the end point.

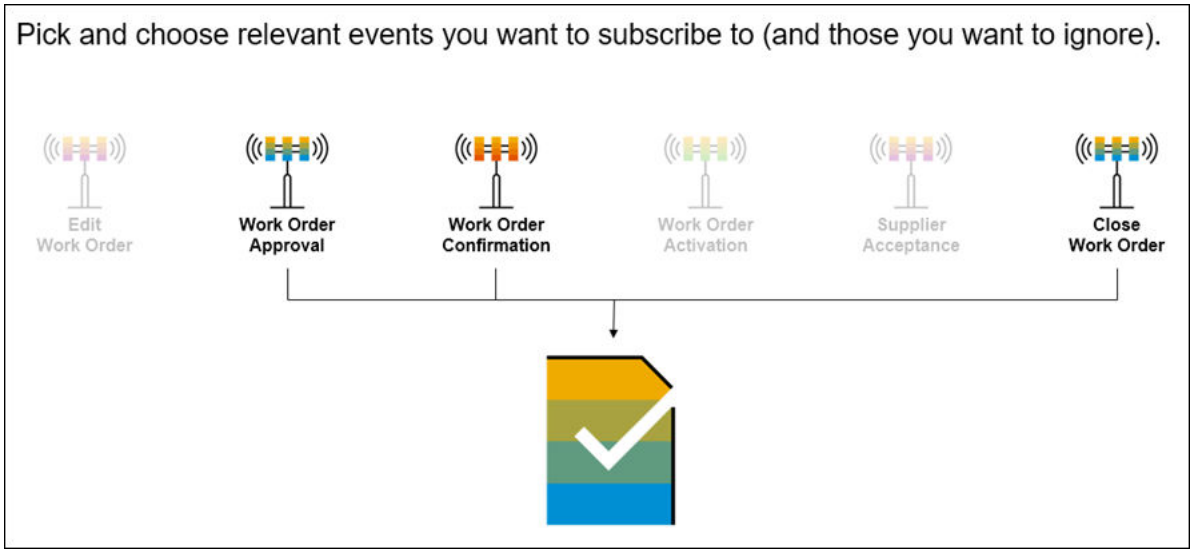
Workflow Diagrams

Configure the Payload

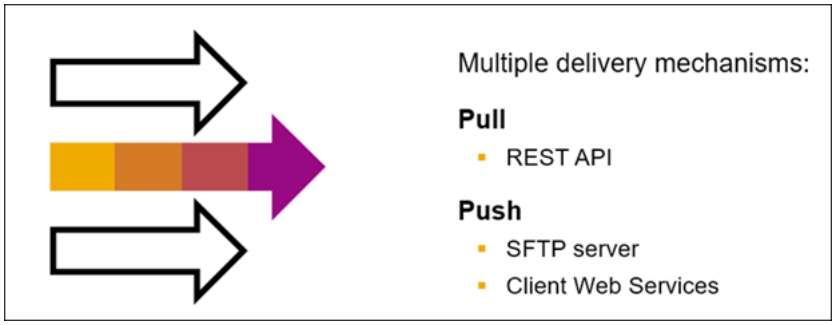
The new application API layer provides a streamlined workflow to get the right data at the right time and real-time transactional data to support quick actions.



Subscribe to Events



Deliver the Payload



6.1 Pub / Sub Wizard

Use a wizard to configure connectivity and subscribe to application activities.

Overview

The *Pub / Sub Wizard* tile on the dashboard opens the Set Up Publish/Subscribe wizard. The setup wizard provides an intuitive framework that allows you to:

- create payloads
- identify and select the data you want to receive against payloads
- subscribe to application activities that trigger payloads

The wizard guides you through the steps that you must complete in order to configure real-time integration activity. Once you've completed the wizard, you can make any configuration changes by using the other Publish/Subscribe Framework tiles.

The following setup steps are organized sequentially in the pane on the left side of the wizard page. The configuration section for each step displays in a pane on the right side of the wizard page.

1. *Welcome* – Welcomes you to the step-by-step process to configure, publish, and subscribe to real-time integration activity.
2. *Payload* – Allows you to identify and configure the data elements to receive. You can choose to create a new payload or use an existing one.
3. *Subscribe* – Allows you to select the application activity and supplier code to subscribe to in the payload.
4. *End Point* – Allows you to configure the receiving location for the payload subscription. You can choose to create a new end point or use an existing one.
5. *Finished* – Displays a message that congratulates you on completing the setup wizard and confirms that you're all set to start receiving information base on the subscribed activities.
   If at any time you need to adjust the setup, choose the *End Points* tile on the dashboard under *Configuration Tools*. For more information, see .

The following information applies to using the setup wizard:

- Fields marked with a red asterisk are required fields.
- After opening the wizard to create a new payload, you must complete the setup on a current step before you can navigate to the next step.
  - The current step displays the ○ icon after the step name.
  - Incomplete steps display the ◉ icon after the step name.
  - Completed steps display the ✔ icon after the step name.
  - To exit the wizard and return to the dashboard, choose the *Back to Dashboard* button on the upper-left side of the page.
- If you complete a page and then exit the wizard for any reason, your progress is saved and the data is retained when you return to the wizard.
- When creating or changing the end point for a payload, the payload and end point pairing must be unique and not already exist.
- After creating or editing a new payload or end point, test the payload to ensure it generates successfully and returns the expected results. For information on this process, see Test Payload [page 130].

Set Up Publish/Subscribe

Perform the following steps in the setup wizard to configure a payload and end point, and to subscribe to the application activities that generate the payload.

1. On the self-service dashboard, choose the *Pub / Sub Wizard* tile.
   The *Welcome* step opens in the Publish Subscribe Setup Wizard.
2. Choose *Let's Get Started*.
   The *Payload* step opens.
3. Select to create a new payload or use an existing payload, as follows:
   1. *Choose New*.

1. In the *Payload Name* box, enter a name for the new payload.
2. In the *Description* box, enter descriptive text.
3. In the *Base Module* list, select the base module you want to monitor.

   > **Note**
   >
   > If there are no values in the database fields for a selected base module, then those fields don't display in the generated payload.

4. In the *Linked Modules* list, select the submodule data you want to pull into the base module. The list includes custom fields, if defined for the selected module.

   > **Note**
   >
   > If there are no values in the database fields for a selected linked module, then those fields don't display in the generated payload.

5. The *Format* option defaults to JSON output.
6. Go to step 4.

2. *Choose Existing* (default value), and in the *Payload* list, select a payload to configure. Go to step 4.

4. Choose *Next Step*.
   The *Subscribe* step opens.
5. In the *Payload Name* list, choose the payload (created by SAP Fieldglass or a buyer) you want to receive. Only payloads associated to the primary module are available. The payload name isn't editable since it was selected in the previous step.

   > **Note**
   >
   > Multiple subscriptions per module are allowed.

6. In the *Activities* options, choose the application activities to subscribe to in the payload.
   You can choose the *Activity* option to select all activities or select and clear individual activities. If you select the *Approved* activity, you can use the *Approval Level (optional)* parameter to specify when the payload should be sent (for example: LAST).
7. In the *Supplier Code* options, select one or more supplier codes to generate the payload for (this is optional).
8. Choose *Next Step*.
   The *End Point* step opens.
9. Select to create a new end point or use an existing end point, as follows:
   1. *Choose New*.

      > **Note**
      >
      > The URL, Username, and Password are used to connect to whatever endpoint the user chooses. These values need to be set up in each SAP Fieldglass environment the client requires this functionality. These inputs aren't used to connect to SAP Fieldglass environments.

      1. In the *URL* box, enter the target URL where the payload is received.
      2. In the *Authentication Type* list, leave the default value `None`, or select one of the following options:
         - Basic Authentication
         - OAuth2 Client Credentials; three mandatory fields are displayed:

- Authorization Server – This is the authentication URL of the destination.
- Client ID – This is your unique identifier used to authenticate with the OAuth URL.
- Client Secret – This is the key associated with your Client ID.

> → Remember
>
> The OAuth2 Client Credentials authentication option is available only if your company's system environment variable `IS_DYNAMIC_CLIENT_ENABLED` is set to **true**. If you need to enable this for your company, then contact the Product Support Team.

> ⓘ Note
>
> If you choose `None`, the application will first try to sign you in using a valid security certificate. If it can't find one, it will then ask for your basic login credentials to continue.

3. In the *Username* box, enter the username to access the URL, if necessary.
4. In the *Password* box, enter the password for the username, if necessary. The password displays as masked text.
5. To test the end point connectivity, select *Test Connectivity*. A *Success* or *Failure* dialog box displays. Resolve any issues, if needed, and when ready, continue with the next step.
6. Go to step 10.

2. Select *Existing* (default value), and in the *End Point* list, select the end point you want to target. Go to step 10.

10. Select *Next Step*.
    The *Finished* step opens and the following message displays:
    `Congratulations, you have completed your setup. You are all set to start receiving information based on the subscribed activities. If at any time you need to adjust this setup, in the Publish/Subscribe Framework section on the Self-Service Dashboard, click the Payloads or End Points tile.`
11. Choose *Finish*.
    The Self-Service Dashboard opens.
    Use the *Payload* tile and *App Activity Subscriptions* tile on the dashboard to edit your setup. For more information, see Payloads [page 129] and App Activity Subscriptions [page 141]. For information on testing a payload, see Test Payload [page 130].

6.2 Payloads

Configure the payload data elements to receive subscriptions to application activity.

A payload is an integral part of each unit of data being transmitted. It's part of the unit data that carries the message that an app or system needs for it to act.

The *Payload* tile on the dashboard opens the Payload List page and displays a list of all existing payloads. You can display the details of existing payloads, test the payload generation, and add a new payload.

6.2.1 Create Payload

Create a new payload outside of the wizard framework. Use this when you only need a new payload, not a new publish / subscribe entry.

Context

> → Tip
>
> In pub/sub payloads, you have the option to include multiple supplier-related fields such as supplier code, supplier name, vendor ID, and supplier custom fields.

Procedure

1. On the Payload List page, choose *New*.
2. On the Add Payload page, specify the following values:
   - Payload Name (must be a unique value)
   - Description
3. Select the *Base Module* from the drop-down menu. A list of all the attributes related with this base module opens.
4. Select the appropriate attributes from the *Base Module Fields*.
5. Choose the *Linked Modules* attribute fields for each linked modules, associated with the base module.

   > → Remember
   >
   > The *Format* is always JSON by default.
6. Choose *Add*.

   The Payload List page opens with the new payload added to the list.

6.2.2 Test Payload

Test a payload to verify that the results generate successfully.

After testing a payload, you can view the payload transport details using the **Monitor Activity** tile on the dashboard. On the Monitor Activity page, the **Payload Transport** tab displays the payload details by payload transport ID for payloads generated through a publish subscribe activity.

To test a payload:

1. On the dashboard, choose the *Payload* tile.
   The Payload List page opens.

2. Choose the payload name hyperlink you want to test.
   The Payload Detail page opens.
3. On the upper-right side of the page, choose *Test*.
   The *Test Payload* dialog box opens.
4. In the *Object Ref* field, enter the document ID of the document you want to populate in the payload.
   You can specify the document ID for any document of the base module that was selected for the payload. You can copy the document ID from the corresponding Detail page in the application. For a Work Order or SOW, the latest document ID is pulled.
5. Choose *Test*.
   The process runs and the results display in the *Test Payload* dialog box.
   To view the payload transport details, see Monitor Activity.

To format the results, copy and paste the string into any JSON formatting tool, such as the JSON Viewer plugin in Notepad ++ or use a free formatting tool available online.

The following sample code shows formatted results.

Sample Code


```
{
    "payload": {
        "baseModuleData": {
            "Available Date": "07/21/2019",
            "Average Rate": "8",
            "Bu Id": "012504042014411764438082",
            "Buyer Code": "ANTE",
            "Buyer First View Time": "07/21/2019 09:47 AM",
            "Creator Id": "012504042021484215026627",
            "Currency": "USD",
            "Currency Conversion Factor": "0",
            "Display Name": "Saha, Tirthankar",
            "Email": "fg_qatest8@sap.com",
            "Exclude Pay Rate From Tax Flag": false,
            "First Name": "Tirthankar",
            "First Submit Time": "07/21/2019 09:31 AM",
            "Has Attachment Flag": true,
            "Has Comment Flag": false,
            "Job Posting Currency": "USD",
            "Job Posting Id": "z19072109085485124070901",
            "Job Seeker Ref": "AS1JS00001793",
            "Job Seeker Type": 1,
            "Last Name": "Saha",
            "Msp Calc Type": 2,
            "Msp Type": 1,
            "Number Of Shifts": 0,
            "Rate Unit": "Day",
            "Rating": "0",
            "Requisition Module Id": 40,
            "Requisition Template Id": "z19051116065824044260 90c",
            "Revision Time": "07/21/2019 09:31 AM",
            "Score From Availability": "0",
            "Score From Cost": "22.22",
            "Score From Qualification": "30",
            "Service Type": 1,
            "Site Id": "0a2904051717431101488682",
            "Status": {
                "state": 1
            },
            "Submit Time": "07/21/2019 09:31 AM",
            "Submitted To Other Requisition Flag": false,
            "Supplier Code": "AS1",
            "Tenure Policy Violated Flag": false,
            "Uploaded Flag": false,
```

```
            "Work Location Id": "z1108031207408428845 1a6d",
            "Worker Pay Type Id": "DEFAULT",
            "Workforce Id": "z18012107305917099268 83e",
            "jobPosting": {
                "Adhoc Time Sheet Flag": false,
                "Adj Amount": "0",
                "Approved Hours": "0",
                "Approved Time": "07/21/2019 09:10 AM",
                "Auto Invoice Type": 4,
                "Automatically Post Jobs To Fcp Flag": false,
                "Average Rate": "8",
                "Base Markup Pct": "0",
                "Billable Per Diem": "0",
                "Bu Id": "012504042014411764438082",
                "Buyer Code": "ANTE",
                "Complete Flag": true,
                "Coordinator Id": "012504042318065466407392",
                "Copied From Job Posting Id": "z190623093003291013009 0d",
                "Cost Weight Pct": "0",
                "CostCenterSet": [
                    {
                        "Buyer Code": "ANTE",
                        "Cost Center Id": "z160510063925076563089 18",
                        "Name": "Budget test"
                    }
                ],
                "Country": "USA",
                "Create Time": "07/21/2019 09:09 AM",
                "Creator Id": "012504042014411759438076",
                "Currency": "USD",
                "Currency Conversion Factor": "0",
                "Current Approval Level": "1",
                "Current Distribution Level": 1,
                "Days For Committed Spend": "4830",
                "Default Career Site Id": "ANTE01",
                "Description": "Site: 5.0\r\nLocation: 5.0\r\nBU: Anthem
(Mike's Test) (ANTE)",
                "Display Status": 1,
                "Distr Time": "07/21/2019 09:10 AM",
                "Distribution List Id": "z080113014059097117 91a15",
                "Distribution Pause Flag": false,
                "Distribution Type": 0,
                "DistributionList": {
                    "Active Flag": true,
                    "Always Visible Flag": false,
                    "Buyer Code": "ANTE",
                    "Code": "5.0",
                    "Create Time": "01/13/2008 01:40 AM",
                    "Display Status": 59,
                    "Name": "5.0",
                    "Revision Time": "03/13/2010 07:36 AM"
                },
                "Distributor Id": "z060901052551521059 42a1b",
                "Duration": 805,
                "Duration Unit": 0,
                "Enable Cats Time Sheet Flag": false,
                "End Date": "07/31/2020",
                "Est Expense Pct": "0",
                "Est Overtime Pct": "0",
                "Est Spend": "38640",
                "Fcp Max Submission": 0,
                "First Approval Received Time": "07/21/2019 09:09 AM",
                "For Replacement Worker Flag": false,
                "Has Attachment Flag": false,
                "Has Comment Flag": true,
                "Hire Invoice Terms Fee Pct": "0",
                "Hire Invoice Terms Type": 0,
                "Hours For Committed Spend": "38640",
```

```
                "Hours Per Day": "8",
                "Hours Per Week": "40",
                "Job Posting Id": "z1907210908548512407090l",
                "Job Posting Ref": "ANTEJP00003196",
                "Job Posting Type": 0,
                "Job Template Id": "z19051116065824044260900",
                "Job Template Type": 0,
                "Job Type": 0,
                "Labor Type Id": "2",
                "Last Approval Action Time": "07/21/2019 09:10 AM",
                "Last Approval Received Time": "07/21/2019 09:09 AM",
                "Last Approver Id": "012504042014411759438076",
                "Last Distr Time": "07/21/2019 09:10 AM",
                "Max Distribution Level": 1,
                "Max Expense": "0",
                "Max Submission": 12,
                "Msp Calc Type": 2,
                "Negotiation Started Flag": false,
                "Number Of Shifts": 0,
                "Owner Id": "012504042014411759438076",
                "Parent Company Code": "ANTE",
                "Positions Available": 6,
                "Positions Filled": 0,
                "Postal Code": "60567",
                "Primary Cost Center Id": "z160510063925076563089l8",
                "Primary Worker Pay Type Id": "DEFAULT",
                "Prorate Calculation Flag": false,
                "Qualification Weight Pct": "0",
                "Rate Uplift Pct": "0",
                "Rebillable Amount": "0",
                "Rebillable Markup Pct": "0",
                "Recruiter Supplier Code": "AS1",
                "Require Rate Change Tier Flag": false,
                "Respond By Date": "07/01/2017",
                "Revision Time": "07/21/2019 09:10 AM",
                "Service Type": 1,
                "Site Id": "0a2904051717431101488682",
                "Site Tax Pct": "0",
                "Start Date": "07/01/2017",
                "Start Day Of Week": 4,
                "State Province": "MD",
                "Status": {
                    "state": 1
                },
                "Status On Close": 0,
                "Time Sheet Freq": 15,
                "Time Sheet Type": 1,
                "Title": "Saha | 19.20 SP1 | FCP cycle test",
                "Total Duration": 0,
                "Travel Pct": "0",
                "Uploaded Flag": false,
                "Work Location Id": "z1108031207408428845la6d",
                "bu": {
                    "Active Flag": true,
                    "Bu Code": "ANTE",
                    "Company Code": "ANTE",
                    "Company Type": 1,
                    "Coordinator Id": "012504042318065466407392",
                    "Create Time": "01/12/2008 08:00 AM",
                    "Display Status": 59,
                    "Distributor Id": "z06090105255152105942a1b",
                    "Division Code Association Type": "NONE",
                    "Escalation Pref Id": "012504042014411761438078",
                    "Name": "Anthem (Mike's Test)",
                    "Parent Bu Id": "0",
                    "Require Coordinator Flag": true,
                    "Require Distributor Flag": true,
                    "Require Remit To Address Flag": false,
```

```
                    "Revision Time": "11/09/2017 11:18 PM",
                    "Uploaded Flag": false
                },
                "creator": {
                    "Access To All Bu": "ALL",
                    "Access To All Cost Center": "ALL",
                    "Access To All Site": "ALL",
                    "Access To Pmo Flag": true,
                    "Access To Visualizer Flag": false,
                    "Active Flag": true,
                    "Address1": "Pune1",
                    "Address2": "17 1/2 Nali, Hadapsar1",
                    "Allow Links To My Account Flag": true,
                    "Auth Support Contact Flag": false,
                    "Bots Type": 0,
                    "Bu Id": "012504042014411764438082",
                    "Can Electronically Sign Contract": false,
                    "Can Request Interview Flag": false,
                    "Can Set Run As User Flag": true,
                    "Can Submit Quick Jp Flag": false,
                    "Can Submit Quick Rfx Flag": false,
                    "Cc Email": "fg_qatest8@sap.com",
                    "City": "Pune",
                    "Combined List Views Flag": false,
                    "Country": "USA",
                    "Create Time": "04/20/2004 09:41 AM",
                    "Default Cost Center Id": "z160510063925076563089l8",
                    "Delete Flag": false,
                    "Device Id":
"TKf5fm57gWCh2Cnf+G5HyYI3KR77u1vHEpsf6Y7+t8M=::3074",
                    "Display Name": "Anthem, Mike",
                    "Display Status": 57,
                    "Email": "fg_qatest8@sap.com",
                    "Email Alert Flag": true,
                    "Email Broadcast Flag": true,
                    "Email Chat Flag": false,
                    "Email Chat Services Flag": false,
                    "Email Notification Flag": false,
                    "Email Question Flag": false,
                    "Email Question Services Flag": false,
                    "Email Reminder Flag": false,
                    "Email Star Flag": true,
                    "Email Work Item Flag": false,
                    "Expert Flag": false,
                    "Expert Services Flag": false,
                    "Fax Number": "x",
                    "Fg User Flag": false,
                    "First Name": "Mike1",
                    "Has Attachment Flag": true,
                    "Has Registered Thru Ui Flag": true,
                    "Last Digest Flag": false,
                    "Last Name": "Anthem1",
                    "Login Auth Type": 1,
                    "Manage Personally Identifiable Info Flag": false,
                    "Manage Site Configurations Flag": true,
                    "Msp Coordinator Flag": true,
                    "Msp User Flag": false,
                    "Parent User Role Id": 0,
                    "Phone Number": "312-279-0000",
                    "Pin Type": 0,
                    "Pmo User Flag": false,
                    "Postal Code": "411028",
                    "Prefix": "1",
                    "Primary Supervisor Id": "012504042014411759438076",
                    "Receive Notifications Before Registration Flag": true,
                    "Report On Linked Suppliers Flag": false,
                    "Revision Time": "07/24/2019 05:21 AM",
                    "Role Id": "5",
```

```
                    "Sap Data Network User Type": 0,
                    "Security Question Answer":
"aes@GIW9We5NVjWx8OmfbP8Op7bhkuCRst2MxxK/FD2xyz4=",
                    "Security Question Id": "QUESTION.FAVOURITESPORTS",
                    "Send Email Approval Flag": true,
                    "Send Notification Digest Flag": true,
                    "Send Work Item Digest Flag": true,
                    "Unregister Flag": false,
                    "Uploaded Flag": false,
                    "Use Sourcing Guidance": false,
                    "User Type": 1,
                    "Username": "Manthem",
                    "Users Have Access To All Dc Flag": false,
                    "View History Tab Flag": false,
                    "View Release Feature Admin Flag": false,
                    "View Restricted Attachment Flag": true,
                    "View Unencrypted Security Id Flag": true,
                    "View Worker Personal Details Flag": false
                },
                "jobTemplate": {
                    "Adhoc Time Sheet Flag": false,
                    "Base Markup Pct": "0",
                    "Billable Per Diem": "0",
                    "Buyer Code": "ANTE",
                    "Can Change Adj Group Flag": false,
                    "Career Site Id": "ANTE01",
                    "Cost Weight Pct": "0",
                    "Create Time": "05/11/2019 04:08 PM",
                    "Default Career Site Id": "ANTE01",
                    "Description": "Site: 5.0\r\nLocation: 5.0\r\nBU: Anthem
(Mike's Test) (ANTE)",
                    "Display Status": 59,
                    "Distribution List Id": "z08011301405909711791a15",
                    "Distribution Type": 0,
                    "Enable Rate Schedule Flag": false,
                    "Est Expense Pct": "0",
                    "Est Overtime Pct": "0",
                    "Hire Invoice Terms Fee Pct": "0",
                    "Hire Invoice Terms Type": 0,
                    "Job Template Ref": "ANTEJT00000227",
                    "Labor Type Id": "2",
                    "Msp Type": 1,
                    "Parent Job Template Id": "0",
                    "Qualification Weight Pct": "0",
                    "Rate Unit": "Day",
                    "Rebillable Flag": false,
                    "Recruiter Supplier Code": "AS1",
                    "Require Rate Change Tier Flag": false,
                    "Revision Time": "05/11/2019 04:08 PM",
                    "Service Type": 1,
                    "Shift Additional Tolerance": "0",
                    "Specify Rate Schedule Per Worker Pay Type Flag": false,
                    "Template Type": 0,
                    "Template Type Id": "1000",
                    "Time Sheet Freq": 15,
                    "Time Sheet Type": 1,
                    "Title": "SRD FCP Template",
                    "Travel Pct": "0",
                    "Ts Type Lock Value Flag": false,
                    "Uploaded Flag": false
                },
                "site": {
                    "Active Flag": true,
                    "Allow To Submit Resume Flag": true,
                    "Buyer Code": "ANTE",
                    "Calendar Id": "012504042014411761438080",
                    "Code": "Bill",
                    "Country": "AIA",
```

```
                    "Create Time": "05/17/2004 05:43 PM",
                    "Display Status": 57,
                    "Division Code Association Type": "NONE",
                    "Hours Per Day": "8",
                    "Hours Per Week": "40",
                    "Invoice Tax Info Code": "Test",
                    "Market Type": "A",
                    "Name": "Bill",
                    "Parent Site Id": "7015F4FB31EA4473AA0594AC",
                    "Revision Time": "11/18/2016 06:48 AM",
                    "Tax Pct": "0",
                    "Uploaded Flag": false
                },
                "workLocation": {
                    "Buyer Code": "ANTE",
                    "Code": "Bill1",
                    "Country": "USA",
                    "Create Time": "08/03/2011 12:07 PM",
                    "Name": "Bill1",
                    "Postal Code": "60567",
                    "Revision Time": "08/03/2011 12:07 PM",
                    "Site Id": "0a2904051717431101488682",
                    "State Province": "MD",
                    "Uploaded Flag": false
                }
            }
        }
    },
    "header": {
        "appVersion": "FieldglassAPIServer/1.0",
        "status": "OK",
        "numRecs": "1",
        "localeString": "en_US",
        "transactionId": "z191120213617803000019af"
    }
}
```


6.2.3 Payload Mapping

Describes the mapping between the base modules, associated modules, and linked modules.

The following table lists the base modules and the submodules that are associated with them. It also identifies which submodules are returned as links rather than being embedded in the response payload.

Base Module	Associated Submodules	Linked Submodules
Job Seeker	• <attachmentList> • <bu> • <creator> • <customFields> • <meetingScheduleList> • <site> • <workforce> • <workLocation>	• <attachmentList> • <bu> • <meetingScheduleList> • <site>

Base Module	Associated Submodules	Linked Submodules

Job Posting	• <adjustmentGroup>
	• <bu>
	• <costCenterSet>
	• <creator>
	• <customFields>
	• <distributionList>
	• <divisionCode>
	• <jobCode>
	• <jobTemplate>
	• <postingRateSet>
	• <purchaseUnit>
	• <rateChangeMatrix>
	• <rateSchedule>
	• <resourceWizard>
	• <shiftSchedule>
	• <site>
	• <workforce>
	• <workLocation>
		• <bu>
		• <site>
		• <attachmentList> - link for each associated attachment
		• <costCenters> - link for each associated cost center
		• <person> - link for each of the following IDs:
		  • <closedByPersonId>
		  • <CoordinatorId>
		  • <CreatorId>
		  • <DistributorId>
		  • <LastApproverId>
		  • <OwnerId>
		• reason - link for each of the following IDs:
		  • <closedReasonId>
		  • <RateUpliftReasonId>
		  • <RejectReasonId>
		  • <WithdrawReasonId>

Work Order/Work Order Extension (for the latest revision of a work order)	• <adjustmentGroup>
	• <bu>
	• <costCenterSet>
	• <creator>
	• <divisionCode>
	• <masterWorker>
	• <purchaseUnit>
	• <rateSchedule>
	• <remitToAddress>
	• <shiftSchedule>
	• <site>
	• <worker>
	• <workerPayType>
	• <workLocation>
		• <bu>
		• <site>
		• <attachmentList> - link for each associated attachment.
		• <costCenters> - link for each associated cost center.
		• <person> - link for each of the following IDs:
		  • <creatorId>
		  • <LastApproverId>
		  • <NewRequisitionOwnerId>
		• <reason> - link for each of the following IDs:
		  • <closedReasonId>
		  • <RejectReasonId>

Base Module	Associated Submodules	Linked Submodules

Worker	• <adjustmentGroup>
	• <bu>
	• <costCenterSet>
	• <customFieldSet>
	• <divisionCode>
	• <masterWorker>
	• <purchaseUnit>
	• <remitToAddress>
	• <site>
	• <workerPerson>
	• <workforce>
	• <workLocation>
	• <workOrders>
		• <bu>
		• <site>
		• <attachmentList> - link for each associated attachment
		• <costCenters> - link for each associated cost center
		• <person> - link for each of the following IDs:
		  • <personId>
		  • <ClosedByPersonId>
		• <reason> - link for each of the following IDs:
		  • <closedReasonId>

Milestone	<customFields>	
Onboarding Items	<customFields>	
Offboarding Items	<customFields>	

Timesheet	• <bu>
	• <divisionCode>
	• <site>
	• <workerPerson>
	• <purchaseUnit>
		• <bu>
		• <site>
		• <person> - link for each of the following IDs:
		  • <workOrderOwnerId>
		  • <LastApproverId>
		• <reason>- link for each of the following IDs:
		  • <reviseReasonId>
		  • <RejectReasonId>

Expense Sheet	• <bu>
	• <customFields>
	• <divisionCode>
	• <site>
	• <purchaseUnit>
		• <bu>
		• <site>
		• <person> - link for each of the following IDs:
		  • <personId>
		  • <WorkOrderOwnerId>
		  • <LastApproverId>
		• <reason> - link for each of the following IDs:
		  • <reviseReasonId>
		  • <RejectReasonId>

Base Module	Associated Submodules	Linked Submodules

Invoice	• <bu>
	• <customFields>
	• <remitToAddress>
	• <site>
	• <adjustmentGroup>
		• <bu>
		• <site>
		• <billingSchedule>
		• <buyerInvoiceTaxInfo>
		• <invoiceLocation>
		• <person> - link for each of the following IDs:
		  • <creatorId>
		  • <LastApproverId>
		• <reason> - link for each of the following IDs:
		  • <RejectReasonId>

SOW Worker	• <adjustmentGroup>
	• <bu>
	• <costCenterSet>
	• <customFields>
	• <divisionCode>
	• <masterWorker>
	• <purchaseUnit>
	• <remitToAddress>
	• <site>
	• <workerPerson>
	• <workforce>
	• <workLocation>
	• <workOrders>
		• <bu>
		• <site>
		• <attachmentList> - link for each associated attachment
		• <costCenters> - link for each associated cost center
		  • <person> - link for each of the following IDs:
		  • <personId>
		  • <ClosedByPersonId>
		• <reason> - link for each of the following IDs:
		  • <closedReasonId>

Profile Worker	• <bu>
	• <costCenterSet>
	• <customFields>
	• <divisionCode>
	• <masterWorker>
	• <purchaseUnit>
	• <resourceWizard>
	• <site>
	• <Person>
	• <workLocation>
		• <bu>
		• <site>
		• <attachmentList> - link for each associated attachment
		• <costCenters> - link for each associated cost center
		• <person> - link for each of the following IDs:
		  • <closedByPersonId>
		  • <CreatorId>
		  • <LastApproverId>
		  • <OwnerId>
		  • <PersonId>
		  • <SupervisorId>
		• <reason> - link for each of the following IDs:
		  • <closedReasonId>
		  • <RejectReasonId>

Base Module	Associated Submodules	Linked Submodules

Project	• <bu>
	• <workerPerson>
	• <reason>
	• <Person>
		• <bu>
		• <person> - link for each of the following IDs:
		  • <CreatorId>
		  • <LastApproverId>
		  • <OwnerId>
		• <reason> - link for each of the following IDs:
		  • <closedReasonId>
		  • <RejectReasonId>

Statement of Work / SOW Revision	• <attachmentList>
	• <adjustmentGroup>
	• <bu>
	• <costCenterSet>
	• <divisionCode>
	• <purchaseUnit>
	• <resourceWizard>
	• <workLocation>
	• <site>
	• <task>
	• <workerPerson>
	• <reason>
	• <payTermsTemplate>
	• <classification>
	• <template_type>
	• <project>
		• <attachementId>
		• <adjustmentGroupId>
		• <bu>
		• <primaryCostCenterId>
		• <divisionCodeId>
		• <purchaseUnitId>
		• <resourceWizardId>
		• <workLocationId>
		• <siteId>
		• <taskId>
		• <person> - link for each of the following IDs:
		  • <CreatorId>
		  • <LastApproverId>
		  • <OwnerId>
		  • <ClosedByPersonId>
		  • <RevisedBySupplierPersonId>
		• <reason> - link for each of the following IDs:
		  • <closedReasonId>
		  • <RejectReasonId>
		  • <WithdrawReasonId>
		• <payTermsTemplateId>
		• <classificationId>
		• <templateTypeId>
		• <projectId>

6.3 App Activity Subscriptions

Create and manage subscriptions to application activities.

The *App Activity Subscriptions* tile on the dashboard opens the Publish / Subscribe List page and displays a list of all existing Payload Publish/Subscribe entries. You can display the details of an existing Payload Publish/Subscribe entry, edit an entry, delete an entry that's not being used in an active configuration, and create a new entry, outside of the wizard framework.

- To create a new Publish / Subscribe, see Create Publish / Subscribe [page 141].
- To edit a Publish / Subscribe, see Edit Publish / Subscribe [page 142].
- To delete a Publish / Subscribe, see Delete Publish / Subscribe [page 142].

6.3.1 Create Publish / Subscribe

Create a new publish/subscribe entry outside of the wizard framework.

Prerequisites

The payload and end point that you use for the new publish / subscribe entry must exist before you can add it here.

Context

Procedure

1. On the Publish / Subscribe List page, choose *New*.
2. On the Add Publish / Subscribe page, specify the following values:
   - *Payload Name* – the payload must exist before you can select it.
   - *End Point* – The payload must exist before you can select it.
   - *Transporter Class* – select the Default Transporter option.
   - *Email* (to notify of status)
   - *Notify at Retry*
3. Choose *Add*. The Publish / Subscribe List page opens with the new entry added to the list.

6.3.2 Edit Publish / Subscribe

Prerequisites

When editing the payload name or end point, the values must exist to select them in the respective lists.

Context

Edit a publish/subscribe entry outside of the wizard framework.

Procedure

1. On the Publish / Subscribe List page, choose the publish / subscribe name hyperlink.
2. On the Publish / Subscribe detail page, in the upper-right corner, choose *Edit*.
3. On the Edit Payload / Publish Subscribe page, change any of the following properties:
   - *Payload Name* – the payload must exist before you can select it.
   - *End Point* – the end point must exist before you can select it.
   - *Transporter Class* – select the Default Transporter option.
   - *Email* (to notify of status)
   - *Notify at Retry*
   - *Activity* to be notified of
   - *Supplier Code*
4. Choose *Update*. The Publish / Subscribe List page opens with the changed entry in the list.

6.3.3 Delete Publish / Subscribe

Describes how to delete a publish/subscribe entry when it's no longer needed.

Context

Procedure

1. On the Publish / Subscribe List page, choose the publish / subscribe name hyperlink.
2. On the Publish / Subscribe detail page, in the upper-right corner, choose *Delete*.
3. In the *Will You Remove This Record* dialog box, choose *OK*.

   The Payload Publish / Subscribe page opens with the publish/subscribe entry removed from the list.

7 Rates

Configuration managers can maintain rate components, rate component groups, and business rules for a company.

The actions available to the configuration manager in the Rates category of the self-service dashboard are:

- Set up and manage Rate Components.
- Set up and manage Rate Component Groups and manage rate component associations.
- Maintain Business Rules that have been created by SAP Fieldglass system administrators.

7.1 Rate Component (Rates 1.0)

Rate components can be used to define an extra level of complexity in rates.

Overview

Rate components are often used to address local or national laws and governance surrounding contingent labor. They allow you to break out any markups and fees that may exist between the pay rate and the bill rate. Rate components force the inclusion of predefined fees, margins, and operating costs such as value added tax (VAT), National Insurance (NI), and fees for service into the hourly/daily rate of a contingent worker.

Available rate component types include:

- COS (percentage or flax rate)
- Margin (percentage only)
- Fee (percentage or flat rate)
- Tax (percentage only)
- MSP (percentage only)
- Parity COS (percentage or flat rate)

When individual rate components have been created, they're grouped together into rate component groups and are then associated to specific rates.

Related Information

Create and Edit Rate Components (Rates 1.0) [page 145]
Rate Component Group (Rates 1.0) [page 147]
Create and Edit Rate Component Groups (Rates 1.0) [page 149]

7.1.1 Create and Edit Rate Components (Rates 1.0)

Configuration managers can view, add new, and edit existing rate components from the self-service dashboard.

1. Select the *Rate Components* tile in the self-service dashboard.
2. Select *New* to create a new rate component. To edit an existing rate component, select it from the list and choose *Edit*.
3. Use the field definitions in the table below to complete the form.

The table below describes required fields, optional fields, and rules for rate components.

Rate Component Field Definitions

Field	Definition
Details	
Rate Structure	This field defaults to Rates 1.0. It only displays when the Coexistence rate structure is enabled. To create a Rate Component for Rates 2.0, refer to .
Code*	A unique code for the rate component.
Name*	The name of the rate component. If desired, the rate component Code and Name may be the same.
Description	A description of the rate component.
MSP Company	The MSP Company with which this rate component is associated. This field is displayed when multiple MSP functionality is used.
Type	The type for the rate component: • COS: Cost of Services • Parity COS: Pay Parity Cost of Services • Margin: The supplier's profit • Fee: Fee • Tax: Tax • MSP Fee: Fee charged by the MSP
Unit	The unit that applies to this rate component: • Percentage: This option is available for all rate component types. Enter the percentage that should be used to calculate the rate component. • Flat Rate: This option is available for the COS and Fee rate component types. Enter the fee amount.
Pre-Parity Percentage	The percentage that should be used to calculate the rate component when a worker has not yet achieved pay parity. If there are no costs during the pre-parity period, the value should be zero. This field displays when Parity COS is selected in the Type field and Percentage is selected in the Unit field.
Parity Percentage	The percentage that should be used to calculate the rate component when a worker has achieved pay parity. This field displays when Parity COS is selected in the Type field and Percentage is selected in the Unit field.

Field	Definition
Pre-Parity Fee	The flat rate that should be used to calculate the rate component when a worker has not yet achieved pay parity. If there are no costs during the pre-parity period, the value should be zero. This field displays when Parity COS is selected in the Type field and Flat Rate is selected in the Unit field.
Parity Fee	The flat rate that should be used to calculate the rate component when a worker has achieved pay parity. This field displays when Parity COS is selected in the Type field and Flat Rate is selected in the Unit field.
Rules	
Include in Level Subtotal	This rule displays for all rate component types except MSP Fee. Set this flag to No to exclude this component from the subtotal calculation for this rate component group level which excludes it from the next level calculation. If this flag is set to No a rate component group that includes this component cannot be added to a Bill Rate Based rate. This functionality can only be used with Pay Rate Based rates. Once set, it cannot be changed.
MSP Fee Calculation	For companies using MSP, this rule displays for all rate component types except MSP Fee. Set this flag to No to exclude this component when calculating the MSP fee. If the customer uses flat fee type MSP fees and this rule is set to No, the rule is disregarded and the configured flat fee is included without any modification. If this flag is set to Noa rate component group that includes this component cannot be added to a Bill Rate Based rate. This functionality can only be used with Pay Rate Based rates.
Use Admin Value	If selected for a component, the value of the component on a work order, work order revision, and SOW revision is replaced with the current admin value when the document is created. This replaces the value of the parent document (job posting, work order, or SOW). This field displays when COS, Margin, Fee or Tax is selected in the Type field. See Considerations.
Edit Value	Select the Edit Value check box if this rate component should be editable when it is part of a rate during the creation of a work order, work order revision or SOW revision. This field displays when COS, Fee, or Tax is selected in the Type field. See Considerations.
Supplier Can Increase Margin	When this flag is enabled, the supplier is able to increase the margin when submitting a job seeker. This field displays when Margin is selected in the Type field.

Considerations

- When a work order, work order revision, or SOW is saved as a draft and later edited/submitted, the rates will not change from the rates saved on the draft, regardless of the Use Admin Value or Edit Value flags.
- When a work order or work order revision is Rejected or Declined and then edited, the application will review the rules set on the rates and either make changes to the rates, or not, based on the rule settings.

7.2 Rate Component Group (Rates 1.0)

A rate component group is a collection of rate components that together drive a calculated bill rate or pay rate.

Overview

Rate component groups are required to use rate components.

- All rate component groups must contain a "margin" rate component.
- All rate component groups apply to a rate. For example, rate component groups can apply to ST (standard time), but not to OT (overtime).

Rate Component Group Field Definitions

Field	Definition
Details	
Rate Structure	Select *Rates 1.0* or *Rates 2.0* depending on which rate structure this group applies. This field only displays when the Coexistence rate structure is enabled.
Code*	A unique code for the rate component group.
Name*	The name for the rate component group. If desired, the rate component Code and Name may be the same.
Description	A description of the rate component.
MSP Company	The MSP Company with which this rate component group is associated. This field is displayed when multiple MSP functionalities are used.
Rate Components	

Field	Definition
Level*	The level is used to control the order of operation of rate components in the rate component group. Enter the level for each rate component in the rate component group. • Multiple rate components can be assigned to a single level. • If a level contains multiple rate components, any flat fee components are applied first. • If a rate component has a level of 1, then that rate component is applied to the base pay rate or base bill rate first. • If a rate component has a level of 2, all level 1 calculations are done first and then the resulting rate is used as the base for computing level 2. • A rate component group must contain only one component of the Margin type. This is the actual profit that the supplier makes on the worker. • Levels should be created from the pay rate perspective, even if it's bill-rate based rate. For example, a rate component group could include rate components for lunch, insurance, and margin. If lunch is assigned to level 1, insurance is assigned to level 2, and margin is assigned to level 3, and the rate is pay-rate based, then the calculation will be pay rate plus lunch plus insurance, with the margin applied to the total. If the rate is bill-rate based with the same level assignments, the calculation will be bill rate less margin, and then minus insurance and lunch. • The MSP % component doesn't have a level selection and is always applied last.
Non-Taxable	For each rate component in the group, select the *Non-taxable* check box, if necessary. If the *Non-taxable* check box is selected, that rate component won't be included in the calculation of tax when tax adjustments are applied to the invoice amount. The nontaxable flag is applicable at all levels.
Code	The *Code* of the selected rate component is displayed.
Name	The *Name* of the selected rate component is displayed.
Use Admin Value	The value from the rate component is displayed.
Edit Value	The value from the rate component is displayed.
Include in MSP Fee Calculation	The value from the rate component is displayed.
Include in Level Subtotal	The value from the rate component is displayed.
Type	The *Type* of the selected rate component, such as Margin or COS (Cost of Service).
Value	The *Value* of the selected rate component, such as a Percentage or a Flat Fee.
Component Limit	When a *Component Limit* is added and the calculated component value exceeds this limit, the value is capped automatically at the amount entered in this column. This column doesn't display when the rate component type is MSP Fee, or if the unit type is Flat Rate. If the *Component Limit* entered is zero or the field is left blank, there's no limit imposed. When the component group includes a *Component Limit*, it can't be added to a *Bill Rate Based* rate. This functionality can only be used with *Pay Rate Based* rates. The amount entered is translated to the currency of the rate that the rate component group is associated.

Field	Definition
Rules	
Use Admin Structure	This flag impacts work orders, work order revisions, and SOW revisions. It has no effect on job postings or SOWs. If *Use Admin Structure* is selected, the structure and components from the admin object will be copied when a work order, work order revision, or a statement of work revision or SOW worker is created. This replaces the structure that was used on the parent document (job posting, work order, or SOW). If *Use Admin Structure* is selected for individual rate components in the rate component group and the value is increased between the time a job posting is approved and work order is approved, the buyer won't be able to submit the work order if the committed spend is greater than the estimated spend amount.

7.2.1 Create and Edit Rate Component Groups (Rates 1.0)

Configuration managers can view, add new, and edit existing rate component groups from the self-service dashboard.

1. Select the *Rate Component Group* tile in the self-service dashboard.
2. Select *New* to create a new rate component group. To edit a rate component group, select it from the list and choose *Edit*.
3. To view the associated rates, click *Rates* in the associations tree view.
4. Use the field definitions in the table below to complete the form.
5. If desired, click *+ Add Component* to associate additional rate components, or click *Re-Order* to change the order of the rate components in the group.

The table below describes required fields, optional fields, and rules for rate component groups.

Rate Component Group Field Definitions

Field	Definition
Details	
Code*	A unique code for the rate component group.
Name*	The name for the rate component group. If desired, the rate component Code and Name may be the same.
Description	A description of the rate component.
MSP Company	The MSP Company with which this rate component group is associated. This field is displayed when multiple MSP functionality is used.
Rate Components	

Field	Definition
Level*	The level is used to control the order of operation of rate components in the rate component group. Enter the level for each rate component in the rate component group. • Multiple rate components can be assigned to a single level. • If a level contains multiple rate components, any flat fee components are applied first. • If a rate component has a level of 1, then that rate component is applied to the base pay rate or base bill rate first. • If a rate component has a level of 2, all level 1 calculations are done first and then the resulting rate is used as the base for computing level 2. • A rate component group must contain only one component of the Margin type. This is the actual profit that the supplier makes on the worker. • Levels should be created from the pay rate perspective, even if it is bill-rate based rate. For example, a rate component group could include rate components for lunch, insurance, and margin. If lunch is assigned to level 1, insurance is assigned to level 2, and margin is assigned to level 3, and the rate is pay-rate based, then the calculation will be pay rate plus lunch plus insurance, with the margin applied to the total. If the rate is bill-rate based with the same level assignments, the calculation will be bill rate less margin, and then minus insurance and lunch. • The MSP % component does not have a level selection and is always applied last.
Non-Taxable	For each rate component in the group, select the *Non-taxable* check box, if necessary. If the *Non-taxable* check box is selected, that rate component will not be included in the calculation of tax when tax adjustments are applied to the invoice amount. The non-taxable flag is applicable at all levels.
Code	The *Code* of the selected rate component is displayed.
Name	The *Name* of the selected rate component is displayed.
Use Admin Value	The value from the rate component is displayed.
Edit Value	The value from the rate component is displayed.
Include in MSP Fee Calculation	The value from the rate component is displayed.
Include in Level Subtotal	The value from the rate component is displayed.
Type	The *Type* of the selected rate component, such as Margin or COS (Cost of Service).
Value	The *Value* of the selected rate component, such as a Percentage or a Flat Fee.

Field	Definition
Component Limit	When a *Component Limit* is added and the calculated component value exceeds this limit, the value will be capped automatically at the amount entered in this column. This column does not display when the rate component type is MSP Fee, or if the unit type is Flat Rate. If the *Component Limit* entered is zero or the field is left blank, there is no limit imposed. When the component group includes a *Component Limit*, it cannot be added to a *Bill Rate Based* rate. This functionality can only be used with *Pay Rate Based* rates. The amount entered is translated to the currency of the rate that the rate component group is associated.
Rules	
Use Admin Structure	This flag impacts work orders, work order revisions, and SOW revisions. It has no effect on job postings or SOWs. If *Use Admin Structure* is selected, the structure and components from the admin object will be copied when a work order, work order revision, or a statement of work revision or SOW worker is created. This replaces the structure that was used on the parent document (job posting, work order, or SOW). If *Use Admin Structure* is selected for individual rate components in the rate component group and the value is increased between the time a job posting is approved and work order is approved, the buyer will not be able to submit the work order if the committed spend is greater than the estimated spend amount.

7.3 Business Rules

A business rule can be associated to a rate schedule, a rate change matrix, or a rate.

Overview

Business rules are created by SAP Fieldglass and can be enabled for companies by an SAP Fieldglass representative. Business rules are available for use with rates, time sheets, and rate change matrices.

- Business rules can be used with rate schedules to execute logic for rates when time is entered on time sheets.
- Business rules can be used with buyer-defined rate change matrices to automate rate change conditions for workers.
- Business rules can be used to create formula-based rules for calculated rates.

7.3.1 Edit Business Rules

Business rules are configured by an SAP Fieldglass representative and enabled for a company.

From the self-service dashboard, configuration managers can edit a business rule to add or update the Custom Description, and test business rules by entering values for the variables used in the rule script.

To view a business rule, select the *Business Rules* tile in the self-service dashboard and then select a rule in the list. The following information displays for business rules:

- SAP Fieldglass defined Description
- Customer defined Custom Description
- Rule Script
- Functions, Internal References, Rate Categories, and Classifications used with the business rule

Custom descriptions can assist buyers when selecting business rules on rates, rate schedules and rate changes matrices. To add or edit a custom description, select the business rule from the list and click *Edit*.

7.3.2 Test Business Rules

Business rules can be tested to ensure they are working as expected.

To test business rules:

1. Select the *Business Rule* tile in the self-service dashboard.
2. Select a business rule from the list and click *Test*. The Test Business Rules modal displays.
3. Enter values for the variables that are used in the business rule and click *Show Test Result*.
4. When testing is complete, click *OK* to close the modal.

8 Analytics

The Analytics category contains actions that the configuration manager can perform related to reports.

The actions available to the configuration manager in the Analytics category of the self-service dashboard are:

- Schedule reports for SFTP delivery.

8.1 API Monitor

Configuration managers can use the API Monitor tile in the Analytics category to view API requests made during a specified time period.

Configuration managers can also filter the API requests made by using the *URI*, *HTTP Method*, *Duration*, and *Source* filters on the API Monitor tile.

8.2 Report Schedule

This tile allows you to schedule reports and set up delivery via SFTP.

SFTP is a secure file transfer protocol that uses secure shell encryption to provide a high level of security for sending and receiving file transfers. The SFTP reports option allows you to schedule the execution, runtime, and location of your reports automatically.

An end point must be created to establish an SFTP address. You can use the *Maintain End Points* tile in the Self-Service dashboard to create the end point.

Once an end point is created, you can add a new report schedule or edit an existing report schedule to select SFTP as the Delivery Type. To edit an existing report schedule, select it from the list. To add a new report schedule, select *New* and then choose a report from the *Report Name* list.

Use the table below to complete the report schedule.

Field Name	Definition
Turn on Schedule?	Select *Yes* to create a schedule for which the report will run automatically.
Schedule Name	Name the schedule. This name will display when viewing previously scheduled reports.

Field Name	Definition
Frequency	Select how often the report should be run. Options include *Daily*, *Weekly*, *Bi-Weekly*, *Monthly*, *By Day*, *Quarterly*, and *Annually*. If the *By Day* option is selected, each day of the week displays. Select the check box(es) next to the day(s) on which you want to run the report. If the *Run Once* option is selected, the report will run once and then the schedule will be deactivated.
Delivery Type	Choose whether the report should be emailed as a *URL*, *Attachment*, or sent via *SFTP*. Companies can send up to 25 scheduled attachment reports within a 24-hour period (standard or consolidated). Once the limit of 25 is reached, the 26th report is sent as URL and the email message notifies the user that the daily limit for attachment reports has been reached.
Encrypt Data/Public Key	These fields display if you chose *SFTP* or *Attachment* as the Delivery Type. To encrypt the resulting report, set this field to *Yes* and enter the encryption key in the *Public Key* field.
Email Addresses	Enter the email addresses for users who should receive a notification and a link/attachment when the report has run. Email addresses are optional. When no email addresses are entered, the report will still run and appear in the Report Outputs list view, but no email will be sent. If email addresses are entered, domains of these email addresses much match those set up in the *Email Domains* field in *Admin* > *Company Details*. Each email address, along with the report schedule creator, will receive a notification email if the latest scheduled report fails. For SFTP reports, the recipients in the email list will also receive a notification if the SFTP transport fails.
Start Date/Time	Enter a start date or select a date from the calendar. The start date indicates the date on which you want the schedule to begin. A future date can be selected to allow the schedule to begin later. Select the time at which the report should be run.
End Date	Enter the end date or select a date from the calendar. The end date indicates the date on which you want the schedule to terminate. Based on the schedule's frequency, the end date is limited in time from the start date as follows: • Daily (3 months) • Weekly (6 months) • Bi-Weekly (6 months) • Monthly (6 months) • By Day (6 months) • Quarterly (8 months) • Annually (8 months)
PGP Encryption Key	Choose a PGP encryption key from the dropdown menu when the *Delivery Type* is set to *Attachment* and the *Encrypt Data* field is set to *Yes*.
Filters	Choose the filtering options for the report.

Field Name	Definition
Run As User	This field is required. Select a user to view the report data as if the person selected for Run as User had executed the report themselves. The ability to use this feature is based on a user's permissions.
Data Source	Determines the database from which the report data is being pulled. • *Latest* displays only data that has not been moved to the archive database for the reporting tool. • *Archive* displays only data that has been moved to the archive database for the reporting tool.
Show Data For	Determines the set of data that displays in the report. • *All* displays all report data that a user has access to, based on user permissions. • *My Group* displays report data included in the user's My Own view plus data that the user has been given My Group access to. • *My Own* displays report data where the user is linked to the data in some way, such as the creator, owner, supervisor, coordinator, or distributor. • The *My Hierarchy* option displays if the user is in a role that has the *Hierarchy Visibility* flag enabled. When selected, the report includes data for the user and the user's subordinates. • The *Owner* option displays if the user is in a role that has the *Hierarchy Visibility* flag enabled. When selected, another drop-down displays with a list of the users that report to the logged in user. Choose a user to view report data for the specific user.
Output Format	Determine the file type of the report. Standard output options include: • *XLS*. Microsoft Excel spreadsheet. • *XLSX*. Microsoft Excel spreadsheet. • *CSV*. Comma separated values. • *CSV Data Only*. Report does not include header information, only the data. • *PDF*. Adobe Acrobat PDF format. When a report has been generated in the selected output, the file can be saved or opened.
Font Name/Size	Sets font options.
Orientation	Sets page layout options.

9 Actions

The Actions category includes other actions that the configuration manager can perform.

The actions available to the configuration manager in the Actions category of the self-service dashboard are:

- Enable the pre-defined SAP Fieldglass Qualification Dictionary for the buyer company.
- Create a list of allowed IP addresses to restrict access to your company's SAP Fieldglass tenant.

9.1 Allowed IP Addresses

Restrict access to the application by setting up a list of allowed IP addresses.

The Allowed IP Addresses tile allows configuration managers to restrict access to a buyer company's SAP Fieldglass tenant by setting up a list of allowed IP addresses.

This functionality allows you to enter both IPV4 (32 bit) IP addresses and the latest internet protocol address technology, IPV6 (128 bit) IP addresses. For each type you can enter static, ranges, and wildcard values.

To set up your list, select *Edit* and enter the information. For both IPV4 and IPV6, you can enter the following:

- Static - allows you to enter IP addresses that correspond to each device that's allowed to access the application. Entries must be complete IP addresses entered in the proper format.
- Range - allows you to enter a range of IP addresses, where all IP addresses that fall within the range are allowed to access the application. Entries must be complete IP addresses separated by a dash (-).
- Wildcard - allows you to enter a partial IP address following by an asterisk (*), which indicates that it's a wildcard value. Any IP addresses that match the partial value are allowed to access the application.

9.2 Qualification Dictionary

The Qualification Dictionary contains a SAP Fieldglass defined default list of qualifications that can be used when defining qualifications on job postings.

Qualifications are the characteristics or skills needed or requested for specific positions. They can be added to job posting templates for use with related job postings. Qualifications may include an assessment scale that is used to measure required or requested skill sets, such as years of experience, level of expertise, or specific licensing requirements. Qualifications are used to help standardize job postings across a company and streamline the job posting creation process. Qualifications help buyers specify the competency, duration, and level of experience desired and thus help suppliers submit the most appropriate candidates.

Configuration managers can enable the SAP Fieldglass Qualification Dictionary so that buyers can select from the predefined list when adding qualifications to job posting templates.

To enable the qualification dictionary, select the *Qualification Dictionary* tile in the self-service dashboard. This action will permanently load the qualification dictionary for the buyer company. Once enabled, the tile can be used by configuration managers to view the list of qualifications and to add new qualifications.

Once the dictionary is enabled, qualifications are available in the *Qualifications* admin object where buyer administrators can view and add new qualifications.

You can generate qualifications for the qualification library using artificial intelligence, based on job posting descriptions and job posting templates. On the Qualification Dictionary page, use the *Generate Qualification* option to analyze this content, review the suggested qualifications, and add the relevant ones to the library, reducing manual effort and improving consistency.

To create a new qualification, from the Qualification List, select *New*. Enter the *Name* and an optional *Description* and complete the remainder of the fields.

Field	Definition
Assessment Scale	Select the option for how this qualification is assessed on the job posting. • *Duration*: A text field displays which is used to indicate the number of years that the job seeker has met the qualification. • *Yes/No*: A Yes/No field displays. • *True/False*: A True/False field displays. • *Points*: A points bar displays which is used to rate job seekers on a five-point scale. • *Points & Duration (Yrs)*: A points bar and text field displays. If a response is mandatory, both values must be entered. • *Certification*: A certification label, start date label, and end date label displays. For example, the labels could be License Number, Issue Date, and Expiration Date. If a response is mandatory, all values must be entered. • *Flexible*: A pair of radio buttons are displayed if the assessment scale has two or less levels defined. If the assessment scale has more than two levels defined, up to ten bubbles are displayed. An informational message is shown when hovering your cursor over each level that displays the level name and description.
	When *Certification* is selected in *Assessment Scale*, the following additional fields display:
Require Attachment	Select *Yes* to require a certification attachment.
Verification Required	Select *Yes* to require the certification to be verified.
Verification Role	If verification is required, this field is used to designate the user role that must be assigned to a user in order for the user to verify the certification. User roles that have the *Verify Certification* permission enabled for the Workforce modules display in the drop-down list. Users must also have the Workforce *View* and *Manage* user role permissions in order to view and validate or reject certification qualifications.
Certification Label	Select *Yes* if you want to include a name for the certification. A blank field displays where the name must be entered.
Start Date Label	Select *Yes* if you want to include a name for the start date of the certification. A blank field displays where the name must be entered.
End Date Label	Select *Yes* if you want to include a name for the end date of the certification. A blank field displays where the name must be entered.

In addition to the list of qualifications, a list of categories is also available to buyer administrators in the *Qualification Category* admin object. Predefined qualifications are automatically associated to categories. These associations can be edited by buyer administrators.

Buyer administrators can add new qualifications and categories as needed from their respective admin objects. Buyer defined qualifications can be edited by administrators and configuration managers, and they can be associated to buyer-defined categories or the SAP Fieldglass predefined categories.

> **Note**
>
> Predefined qualifications in the SAP Fieldglass Qualification Dictionary cannot be edited by buyer administrators or configuration managers. However, buyers administrators can edit the associations to categories.

9.3 Internal References

Configuration managers can set internal references for custom fields and pick lists.

Internal references allow you to tag custom and user-defined fields with a standard label. This is used for extending SAP Fieldglass application content to specific customer content for use in cross product integrations.

Using the Internal Reference tile on the Configuration Manager Self-Service Dashboard, you can define tags for custom fields and pick lists to ensure that changes to those user-defined fields do not interrupt your integrations with other systems.

To set up an internal reference, select the tile and choose the Custom Field tab or the Pick List tab. Select a field from the list and enter the tag in the *Internal Reference* field. Select *Update* to save the information.

Internal references cannot contain:

- Spaces (underscores can be used)
- Lower case letters
- Special characters

10 Implementation Tools

Describes tools available to the Configuration Manager in the Implementation Tools section of the Self-Service Dashboard.

The following implementation tools are available:

- Company Configurations – enable and disable configurations at the company level.
- Comparison Tool – compare source and target tenants to identify differences in company configurations and site configurations.
- Configuration Mover – move configurations between SAP Fieldglass environments..

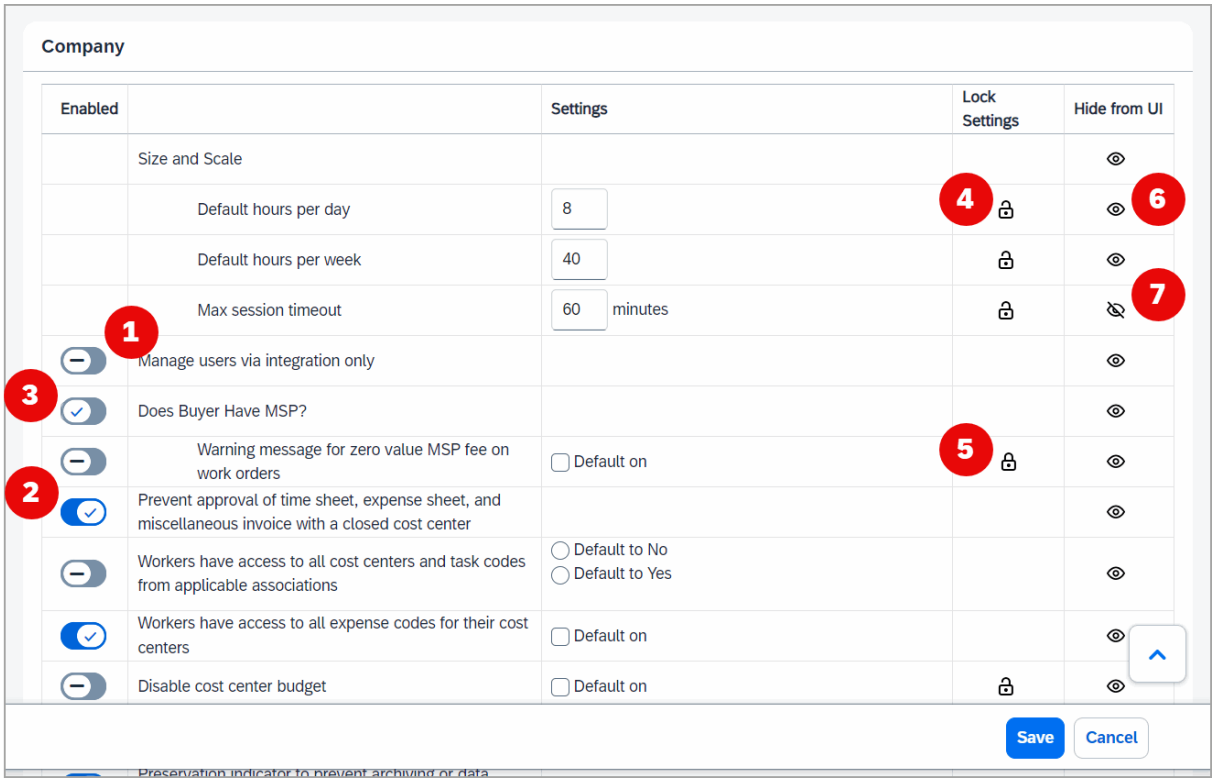
10.1 Company Configurations

Use this tile to enable and disable configurations at the company level.

The Company Configurations tile on the Self-Service Dashboard provides you with options to enable, disable, lock, and hide company configurations as needed.

Select *Edit* at the top of the page to make changes. You can hover over a configuration to learn more about the functionality it provides when enabled. Some configurations may appear that cannot be enabled or disabled by the configuration manager. Those configurations can only be managed by SAP Fieldglass, however they appear because they have child configurations that can be managed by your configuration manager.

Configurations that can be managed by the configuration manager are considered low and medium risk to your company's current setup. This means that enabling or disabling the settings poses little to no impact to your current company setup. In addition to low and medium risk configurations, you can also change some settings that are considered a higher risk. In these cases, it is recommended that you test the settings in a test environment prior to enabling or disabling them in your production environment. Configurations that appear grayed out are available for visibility only. These settings are considered very high risk and can only be enabled or disabled by SAP Fieldglass.



Icon definitions:

1. Disabled - click or tap to enable this option for your company.
2. Enabled - click or tap to disable this option for your company.
3. Not available - this option is managed by SAP Fieldglass. It appears grayed out. Contact Product Support to change this setting.
4. Unlocked - If an option is enabled and unlocked, it can be managed on templates or documents.
5. Locked - if an option is enabled and locked, it cannot be changed on templates or documents.
6. Visible - if an option is visible, it appears on the Company Details page.
7. Hidden - if an option is hidden, it does not appear on Company Details page.

10.2 Comparison Tool

The Comparison Tool for Configuration Manager users enables comparison of source and target tenants to identify differences in company configurations and site configurations. You can choose to compare configurations from either an SAP Fieldglass Leading Practice Solution, also known as gold environments, or a source environment.

Instead of displaying all configurations, the tool specifically highlights the differences between the two tenants. Additionally, users have the option to download the comparison results in a .csv format for further analysis.

Related Information

Adding Environment Details [page 161]
Comparing Company and Site Configurations [page 162]

10.2.1 Adding Environment Details

Context

You can pull configurations from either an SAP Fieldglass Leading Practice Solution, or a source environment, and then set up the target system to retrieve configurations for comparison.

Procedure

1. Select *Comparison Tool* tile on the Configuration Manager dashboard.
2. Select *Yes* or *No*, in the *Do you want to pull configuration from an SAP Fieldglass Leading Practice Solution?* field.
3. If you choose *Yes*, proceed with the following steps:
   a. Choose a solution from the *SAP Fieldglass Leading Practice Solution* dropdown list.
   b. Review the *Target URL* and *Target Buyer Code*.

      The target system is the environment where you've logged on. These fields are auto filled by the app.
4. If you select *No*, proceed with the following steps:
   a. Enter the *Source URL*, *Source Buyer Code*, *Source Username*, and *Source Password*.

      These are the details of the source system from which the configurations are retrieved for comparison.
   b. Review the *Target URL* and *Target Buyer Code*.

      The target system is the environment where you've logged on. These fields are auto filled by the app.
5. Choose *Validate*.

   The app takes you to the *Configurations* page.

10.2.2 Comparing Company and Site Configurations

Context

You can review the company configurations and site configurations in both the source and target tenants. Additionally, you have the option to download all the details in a .csv format for your reference.

Procedure

1. In the Comparison table, you can toggle between *Company Configuration* and *Site Configuration* to review the available configurations between source and target tenants.
2. Expand the available configurations to view the difference in source and target tenants.
3. Choose *Download Comparison Table* to download a .csv format file.
4. Choose *Close* to go back to the Configuration Manager dashboard.

10.3 Configuration Mover

> ⓘ Note
>
> Starting with the 2025.11.0.0 release, the Configuration Mover help documentation will be consolidated into the SAP Fieldglass Configuration Manager guide. This will provide a unified experience for managing implementation tools.

Configuration Mover is a tool that enables buyers to move configurations between tenants, for example, copying a test configuration to a production environment. Users can select the source environment from which they want to pull configurations and move them to the target environment. It's important to note that the environment in which users are logged in to use this tool is considered the target environment.

The Configuration Mover tile uses the SAP Fieldglass connector framework to download and upload configuration data between companies and environments, reducing the implementation time. You can use the Configuration Mover to pull company and admin configurations from a preconfigured Leading Practice setup to a test environment. You can also use it to move configurations from other defined companies to a test or production environment.

The Configuration Mover tile is in the *Implementation Tools* section on the Self-Service dashboard.

> → Remember
>
> - A tenant must be set up in the target environment to be used as the target company.
> - Both Target and Source environments must be on the same release version. To check the release version, go to ▶ ⓘ ▶ *About...* ▶.

- The user running the Configuration Mover must have the same language preference in both the Source and Target environments.
  - If copying from a custom environment: The user's language preference in the target must match the Source. For instance, if the source is set to English (United States), the target must also be set to English (United States).
  - If copying from one of the SAP Fieldglass Leading Practice environment: The user's language preference in the target must be English (United States), as this is the default language for Leading Practices.
  - Configuration Mover currently supports English (United States) only.

The Configuration Mover tool enables copying of any configuration to the target environment, such as custom fields, custom text, and contextual help, provided a connector pair exists for the object. When the job runs, all connectors associated with the selected items are automatically enabled and subsequently disabled upon job completion. To minimize data errors, you can refer to the *Prerequisite Connectors* column when selecting connector pairs. Additionally, any configuration already enabled on the target environment will not be overwritten if it is disabled on the source environment.

Limitations

You cannot use the Configuration Mover to copy transactional data such as Job Postings, Work Orders, and Statements of Work.

10.3.1 Accessing Configuration Mover

Context

Use Configuration Mover to transfer company configurations and admin configurations to the target system. It provides a detailed overview audit along with configuration details.

Procedure

1. Select *Configuration Mover* tile, on the Self-Service dashboard.

   The *End User Acknowledgment* dialog box opens.
2. Read the acknowledgment, and then select the checkbox.

   > ⓘ Note
   >
   > To hide the *End User Acknowledgment* dialog box from appearing each time you access Configuration Mover, select the checkbox labeled *Do not display this message again*.
3. To continue, choose *Accept*, or to exit Configuration Mover and return to the dashboard, choose *Decline*.

You can always return to the dialog box by following steps 1 and 2

After accepting the acknowledgment, the Configuration Mover page opens.

Environment and Configuration Details in Configuration Mover

You can add environment and configuration details in Configuration Mover. These details are displayed in the following tabs:

Environment and Configuration Details in Configuration Mover

Audit Trail	Environment Details	Configurations	Review and Submit
Displays an audit trail of all transactions moved within a specified date range, including: • Company Copy • Source Environment • Source Company • Source Username • Target Environment • Target Company • Target Username Select the *Audit Trail* option to return to the *Upload Status* view.	Allows you to select where to pull configurations from, either an SAP Fieldglass Leading Practice Solution or a Source URL. Select Yes and specify: **Available Leading Practice Solution** and *Source Buyer Code*. → Remember You can choose a leading practice solution in test environments. However, this option is not available in production environments. Select No and specify: *Source URL*, *Source Buyer Code*, *Source Username*, and *Source Password*.	After selecting *Validate* on the Environment Details page, the Configurations page opens. You can choose objects to transfer to the target system from the following categories: • Company Configurations • Company Structure • Configuration • Financial Data • Integration • Rate Structure • Services • Worker • Workflow	Before submitting, you have the choice to review and modify the environment details or configurations. After making the changes and submitting them, the Audit Trail page opens, allowing you to view the status and details of all transactions moved within a specified date range.

⚠ Caution

Selecting individual data elements can create errors with data integrity and prerequisite connector requirements. To maintain consistency and avoid potential issues with existing data relationships, SAP advises following the outlined prerequisites for data integration. In addition, any data not included as a Configuration Mover option needs to be created manually or via standard connector uploads. Not creating this data may cause integrity issues.

10.3.2 Viewing Configuration Mover Audit Trail

Context

Using Audit Trail, you can view all transactions, download error logs, and check the status of transactions.

> ⓘ Note
>
> To go to *Environment Details*, choose *New* on the *Audit Trail* list view page.

Procedure

1. Select *Configuration Mover* tile, on the Self-Service dashboard.

   The *End User Acknowledgment* dialog box opens.
2. Read the acknowledgment, and then select the first checkbox.

   > ⓘ Note
   >
   > To hide the *End User Acknowledgment* dialog box each time you access Configuration Mover, select the second checkbox.
3. To continue, choose *Accept*, or to exit Configuration Mover and return to the dashboard, choose *Decline*.

   You can always return to the dialog box by following steps 1 and 2

   After accepting the acknowledgment, the Configuration Mover page opens.
4. Choose *Audit Trail*.
5. Choose a *Start Date* and an *End Date*, to view all transactions moved within a date range.
6. After choosing the date range, select *Apply Filters*.

   A list of all available transactions is displayed.
7. Choose a **Job ID** to view the details of the transaction.
   The app displays a list of all objects uploaded in the transaction along with their status.
8. Choose an object to view transaction details.

   > → Remember
   >
   > You can view transaction details in the *Upload ID* flyout. The detail flyout is only available for items that have a transaction ID.
9. In the first dropdown list, select the file you want to download. You can choose to download the *Error Log*, *Error Upload File*, and *Original Upload File*.
10. In the second dropdown list, select the format in which you want to download the file. You can choose between *CSV Format*, *CSV Format-UTF8*, and *Text Format*.

11. Choose *Retrieve*.
    The file is downloaded to your system.

10.3.3 Adding Environment Details to Configuration Mover

Context

You can choose to pull configurations from either an SAP Fieldglass Leading Practice Solution, also known as gold environments, or a Source environment, and then set up the target system for replicating configurations.

> ⓘ Note
>
> SAP Fieldglass Leading Practice Environments represent structured templates tailored to your requirements. These environments include predefined Company Configurations, Admin Configurations, and Company Structure Objects. The Leading Practice Environments serve as the source. From here, Configuration Mover replicates these configurations to establish your target test environments.

Procedure

1. Select *Configuration Mover* tile, on the Self-Service dashboard.

   The *End User Acknowledgment* dialog box opens.
2. Read the acknowledgment, and then select the first checkbox.

   > ⓘ Note
   >
   > To hide the *End User Acknowledgment* dialog box each time you access Configuration Mover, select the second checkbox.
3. To continue, choose *Accept*, or to exit Configuration Mover and return to the dashboard, choose *Decline*.

   You can always return to the dialog box by following steps 1 and 2

   After accepting the acknowledgment, the Configuration Mover page opens.
4. Select *Yes* or *No*, in the *Do you want to pull configuration from an SAP Fieldglass Leading Practice Solution?* field.

   > → Remember
   >
   > You can choose a leading practice solution only in test environments. This option is not available in production environments.
5. If you choose *Yes*, proceed with the following steps:
   a. Choose a solution from the *SAP Fieldglass Leading Practice Solution* dropdown list.

b. Review the *Target URL* and *Target Buyer Code*.

The target system is the environment where you've logged on. These fields are auto filled by the app.

6. If you select *No*, proceed with the following steps:
   a. Enter the *Source URL*, *Source Buyer Code*, *Source Username*, and *Source Password*.

   These are the details of the source system from which your data will be transferred.
   b. Review the *Target URL* and *Target Buyer Code*.

   The target system is the environment where you've logged on. These fields are auto filled by the app.
7. Choose *Validate*.

   The app takes you to the **Configurations** page.

Related Information

Setting up Company and Admin Configurations [page 167]
Reviewing and Submitting Configurations [page 168]

Setting up Company and Admin Configurations

Context

You can choose the required company configurations, admin configurations, and company structure objects for the target environment.

Procedure

1. Choose the objects to transfer to the target system from the following categories:
   - Company Configurations
   - Company Structure
   - Configuration
   - Financial Data
   - Integration
   - Rate Structure
   - Services
   - Worker
   - Workflow

You can choose *Select All* to include all the available configurations.

> **Note**
>
> If both Rates 1.0 and Rates 2.0 are enabled in the source company, the *Compatible with Rates 1.0* configuration will not be automatically copied to the target company.

2. Select *Continue*.

   The app takes you to the *Review and Submit* page.

Reviewing and Submitting Configurations

Context

You can review the source environment details and the selected configuration before submitting your changes in Configuration Mover.

Procedure

1. Choose *Edit* to modify the selected configurations or environment details.
2. Select *Submit* and *Accept* the End User Acknowledgement.

   The app takes you to the *Audit Trail* tab that displays all transactions moved within a specified date range.

> **Note**
>
> If you've selected any configuration that is dependent on prerequisite connector pairs, then the app displays a message to avoid any data integrity issues.

Related Information

Viewing Configuration Mover Audit Trail [page 165]

11 Frequently Asked Questions

Getting Started

How do I become a Configuration Manager in SAP Fieldglass?	A company administrator must assign you a Configuration Manager role via the main SAP Fieldglass user account. You'll receive a separate Sign-In ID for accessing the Self-Service Dashboard.
Can multiple Configuration Managers be assigned in a company?	Yes, multiple Configuration Managers can be created. Each is linked to their original user account and inherits its preferences and settings.

Buyer Configuration Manager

What tools are available to me as a Buyer Configuration Manager?	You can access all Configuration Tools, including Connector Wizard, API Keys, Encryption, End Points, Subscriptions, and more. You can also manage Partner Integrations, SSO, and Event Driven Configurations.
Can I create and manage connectors?	Yes, Buyer Configuration Managers can create, enable, and edit connectors using the Connector Wizard. Supplier Configuration Managers do not have this access.
How do I test a connector or subscription?	Use the *Run Now* or *Test Connectivity* options in the Integration or Subscription setup pages.
Can I manage OpenText ECM integration?	Yes, Buyer Configuration Managers can configure and manage OpenText ECM endpoints for document storage.

Supplier Configuration Manager

What tools are visible to Supplier Configuration Managers?	Supplier Configuration Managers have limited access. The Connector Wizard is not visible. They can view and manage only the connectors and tools assigned to their supplier company.
Can I customize connector fields?	Yes, but only for connectors enabled for your supplier. You can add custom fields, rename columns, and apply templates.

Can I view worker data across suppliers?	If you're an MSP supplier, you can view native field data across associated suppliers. However, custom fields are only visible to the supplier who created them.

Configuration Tools

What's the difference between Upload and Download connectors?	Upload connectors bring data into SAP Fieldglass; Download connectors export data from SAP Fieldglass to external systems.
How do I enable a connector using the Connector Wizard?	Use the decision tree in the wizard to select a connector category, answer guided questions, and enable the connector or browse the catalog if no match is found.
What should I do if a connector fails during data transfer?	Use the Monitor Activity tile to view errors. You can filter by status and access detailed logs to troubleshoot.
What are API Application Keys used for?	They authenticate external applications to interact with SAP Fieldglass through APIs. You'll need both an application key and a web service user.

Encryption Keys & Certificates

What types of encryption assets can I manage?	You can manage PGP, PKI, Symmetric Keys, and X.509 certificates.
How do I rotate an encryption key?	Open the asset, edit the key value or auto-generate a new one, save, and activate the new version. The old version becomes decrypt-only.
What happens if a certificate is revoked?	It can no longer be used for encryption/decryption. Manual re-encryption may be required for affected data.
How are expired certificates handled?	You'll receive alerts based on configured thresholds. You can rotate or revoke certificates as needed.
Can I audit changes made in the system?	Yes, use the Modification Log tabs in SSO, Connectors, and Subscriptions to view who made changes and when.

End Points & Subscriptions

What is an End Point in SAP Fieldglass?	It defines the server details for file transfers (SFTP, WebService, etc.) used by connectors and subscriptions.
How do I test an End Point or Subscription?	Use the *Test Connectivity* or *Run Now* options in the respective setup pages to validate the configuration.
What should I do if a subscription fails?	Check the Monitor Activity tab for error details. Use the *RePush* option to retry failed transactions.

Event Driven Config & Punchout

What is Event Driven Config used for?	It enables real-time integration with SAP Ariba and SAP S/4HANA Lean Services by triggering payloads based on user activities.
Can I test an Event Driven Config before activating it?	Yes, use the *Test* option to simulate a transaction and validate the setup

Partner Management (OpenText ECM)

What happens to attachments when OpenText ECM is enabled?	Buyer and worker attachments are stored in OpenText ECM; metadata remains in SAP Fieldglass. Supplier attachments stay in SAP Fieldglass.
How do I troubleshoot attachment issues?	Check end point credentials and connectivity. If files are missing or inaccessible, contact OpenText support.

Single Sign-On (SSO)

How do I set up SSO for my company?	Use the SSO Setup Wizard to configure Identity Provider and Service Provider details, upload certificates, and enable deep linking.
What if users face login issues via SSO?	Check the SSO Login History tab for error messages and troubleshoot based on the error type, such as expired certificate or invalid SAML response.

Publish/Subscribe Framework

What is a Payload in SAP Fieldglass?	It's the structured data sent during a publish/subscribe event. You can configure payloads to include specific modules and fields.
How do I subscribe to application activities?	Use the Pub/Sub Wizard or App Activity Subscriptions tile to link payloads with activities and define delivery endpoints.

Rates & Business Rules

What are Rate Components and Groups?	Rate Components define fees, margins, and taxes. Rate Component Groups combine these into structured rate calculations.
Can I test business rules before applying them?	Yes, use the *Test Business Rules* option to validate logic with sample inputs.

Analytics & Reporting

How do I schedule reports for SFTP delivery?	Use the Report Schedule tile to define frequency, delivery type (SFTP, email), encryption, and filters.

Implementation Tools

What is Configuration Mover used for?	It transfers configurations between environments using connector pairs.
Can I move transactional data like Work Orders?	No, Configuration Mover only supports configuration data, not transactional records.

Actions & Security

How do I restrict access to SAP Fieldglass?	Use the Allowed IP Addresses tile to define static, range, or wildcard IPs for access control.

What is the Qualification Dictionary?	A predefined list of qualifications used in job postings. Once enabled, it can be extended but not edited.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap