CONFIDENTIAL

Document Version: SHIP – 2025-02-05

Administration Guide for SAP Ariba Buying, Base Edition

THE BEST RUN **SAP**

Content

1 Administration Guide for SAP Ariba Buying, Base Edition

This guide is for administrators responsible for setting up and managing SAP Ariba Buying, base edition. The guide includes configuration steps and information about security and data protection and privacy.

This documentation applies to SAP Ariba Buying, base edition, which is integrated with SAP S/4HANA Cloud. If you're looking for information about the SAP Ariba Buying solution package that's part of SAP Ariba Procurement solutions, see the Related Information section below.

> ⓘ Note
>
> The features described in this document require a 3-system landscape.

Related Guides

Getting Started with SAP Ariba Buying, base edition

Setting Up SAP Ariba Buying, base edition

User Guide for SAP Ariba Buying, base edition

Related Information

SAP Ariba Procurement solutions - Buyer Help Roadmap

2 Overview

This guide describes the prerequisites, roles, authorizations, and configurations you require to set up SAP Ariba Buying, base edition for SAP S/4HANA Cloud.

As an administrator, you set up SAP Ariba Buying, base edition for buyers to transact with suppliers.

> ⓘ Note
>
> Setup involves working with roles for each of the following: SAP BTP, SAP Ariba Buying, base edition, and SAP S/4HANA Cloud. SAP Ariba Buying, base edition apps are visible only to users who are assigned the required roles.

To learn more about setting up SAP Ariba Buying, base edition, see About Setting Up SAP Ariba Buying, Base Edition.

As an administrator with the role `Procurement_Configuration_Admin`, you can perform the following configuration tasks:

- Edit document ID information for the documents that will be used in the request process
- Manage user information
- Manage organization-wide information for company codes, plants, purchasing groups and purchasing organizations
- Manage recommendations that are displayed to users on the *Create Purchase Request* app
- Manage announcements that are displayed to users on the *Create Purchase Request* app
- Configure shopping site content providers
- Manage the mapping of product classification codes to SAP S/4HANA Cloud material groups
- Manage the mapping of supplier IDs to SAP S/4HANA Cloud vendor IDs
- Manage the mapping of units of measure between various content sources and SAP S/4HANA Cloud
- Manage approval workflows

3 Configuring SAP Ariba Buying, Base Edition

This section helps you set up and manage the configuration for SAP Ariba Buying, base edition.

3.1   Configuring SAP Business Technology Platform

The topics in this list cover the concepts and procedures involved in configuring and setting up SAP Business Technology Platform (SAP BTP) to integrate with SAP Ariba Buying.

Ensure that you have the necessary business roles and requirements to set up SAP BTP. For more information, see Assign Roles in the SAP BTP Cockpit.

3.1.1 Assign Users to Role Collections in the SAP BTP Cockpit

Administrators of SAP Ariba Buying, base edition require specific administrator role collections and roles on SAP BTP. Assign the required role collections to the administrator user.

Do the following to set up the role collections and roles for the administrator:

- Before you set up the role collections and roles, ensure that you have a user on SAP BTP cockpit. For more information, see Create Users.
- Set up the required role collections and roles for the SAP Ariba Buying, base edition administrator in the SAP BTP cockpit.
  Ensure that you assign the *Global Account Administrator* role collection to the administrator user of the global account. This role collection contains the following roles:

Role Name	This Role Allows You to....
Global Account Admin	Manage the read-write authorizations for updating the global account, setting entitlements, and creating, updating, and deleting subaccounts.
Global Account Usage Reporting Viewer	Manage the read-only authorizations for viewing global account usage information.
System Landscape Administrator	Manage read-write authorizations for registering SAP systems and assigning SAP systems to formations.
User and Role Administrator	Manage read-write authorizations for trusted identity providers, role collections, roles and users.

After you create a subaccount, ensure that the administrator has the required roles for the sub account. Use the role collection *Subaccount Administrator* to assign the following roles to the administrator user. For more information about creating subaccounts, see Create Subaccounts in Your Global AccountCreate Subaccounts in Your Global Account.
Subaccount Administrator Role Collection

Role Name	This Role Allows You to....
User and Role Administrator	Manage read-write authorizations for trusted identity providers, role collections, roles and users.
Subaccount Admin	Manage read-write authorizations for trusted identity providers, role collections, roles and users.
Subaccount Viewer	Manage read authorizations for viewing subaccount entitlements and for creating and deleting environment instances.
Subaccount Service Administrator	Get the administrative access to service brokers and environments for subaccounts. You also require this role to subscribe to applications.
Destination Administrator	Manage the configuration for destinations, certificates, and trust for subaccounts.

For more information, see the following:

- Role Collections and Roles

- Assigning Role Collections to Users or User Groups.

3.1.2 Subscribe to SAP Ariba Buying

You need an active license for SAP Ariba Buying to subscribe to the subscription plans.

You can choose one of the following options to subscribe to SAP Ariba Buying, base edition.

- Use the booster to get an active subscription to SAP Ariba Buying, base edition.
  For more information about the using the booster, see Subscription to SAP Ariba Buying, Base Edition Using the Booster.
- Perform the steps in the section Subscribing to SAP Ariba Buying, base edition to get an active subscription.

Use the booster to set up some of the required steps for setting up SAP Ariba Buying, base edition that is available in the SAP BTP cockpit. You must also use the Cloud Integration Automation Service to complete the remaining configuration.

When you configure SAP Ariba Buying using the booster and Cloud Integration Automation Service, the process to configure is simpler without many manual procedures. The guided process helps you to complete the configuration tasks step by step.

Subscribing to SAP Ariba Buying, Base Edition [page 8]
> You need an active license to subscribe to a subscription plan for SAP Ariba Buying.

3.1.2.1   Subscribing to SAP Ariba Buying, Base Edition

You need an active license to subscribe to a subscription plan for SAP Ariba Buying.

You can choose one of the following options to subscribe to SAP Ariba Buying, base edition:

Subscription to SAP Ariba Buying, Base Edition Using the Booster [page 9]
> Use the booster to guide you through some steps in setting up a subscription and configuring SAP Ariba Buying with SAP S/4HANA Cloud on SAP Business Technology Platform (SAP BTP). Follow this procedure to subscribe to a service and a plan for SAP Ariba Buying, base edition from the SAP BTP cockpit.

Subscribing to SAP Ariba Buying, Base Edition Without the Booster [page 11]
> This section contains information about setting up manually without using the booster.

3.1.2.1.1 Subscription to SAP Ariba Buying, Base Edition Using the Booster

Use the booster to guide you through some steps in setting up a subscription and configuring SAP Ariba Buying with SAP S/4HANA Cloud on SAP Business Technology Platform (SAP BTP). Follow this procedure to subscribe to a service and a plan for SAP Ariba Buying, base edition from the SAP BTP cockpit.

Prerequisites

You must have the following before you run the booster to get a subscription for SAP Ariba Buying, base edition.

- A license for SAP Ariba Buying, base edition.
- A global account on SAP BTP. For more information, see Getting Started with the Universe of SAP S/4HANA Cloud, public edition.
- Register the SAP S/4HANA Cloud system with the global account in the SAP BTP cockpit. When you register your system, ensure that you choose the formation type *Integration with SAP Ariba Buying* from the *Communication Scenario Groups* dropdown menu.
  For more information, see Register an SAP S/4HANA Cloud System in a Global Account and Enabling SAP Ariba Buying.
- (Optional) If you use directories, ensure you assign entitlements to directories by adding service plans and distribute the quotas available in your global account to your directories. For more information, see Configure Entitlements and Quotas for Directories [Feature Set B].
- Required roles on SAP BTP. For more information, see Assign Users to Role Collections in the SAP BTP Cockpit.
- Ensure that you've activated the required scope items. For more information about activating the scope item, see Activating Scope Items.
- You must have a license to set up a 3-system landscape on your SAP S/4HANA Cloud system.

Context

Perform the steps to subscribe to SAP Ariba Buying and get an active subscription.

> ⓘ Note
>
> The booster allows you to complete the following steps. If you run the *booster*, you can skip these steps in the guide:
>
> - Create Subaccounts in Your Global Account
> - Create a Tenant in the Identity Authentication Service
> - Get a Subscription to SAP Ariba Buying
> - Subscribe to Services Required for SAP Ariba Buying
> - Configure the OAuth 2.0 Client Authentication

- Configure the Communication Management
- Create the Destinations in Your Tenant
- After you run the booster, a trust between the SAP Business Technology Platform (SAP BTP cockpit) and Identity Authentication service administration is established for you. For more information, see Setting Up Trust Between Identity Authentication and SAP BTP.

  → Remember

  - If you have set up the trust manually, ensure that you select the domain that is also used by the tenant of the Identity Authentication service associated with the SAP S/4HANA Cloud Public Edition. The domain you choose must end with "cloud.sap".
  - When you establish trust with the Identity Authentication Service, ensure that the corresponding application created in the Identity Authentication Service contains the Global User ID as the subject name identifier.

  For more information about identity management, see Identity Management for SAP S/4HANA Cloud and Integrated Products.

- You can subscribe and sign in to SAP Ariba Buying only after you've established a trust between the SAP BTP cockpit and Identity Authentication service administration.

Procedure

1. Open the SAP BTP cockpit and go to your global account.
2. In the navigation menu, choose *Boosters*.
3. Choose the booster *Set Up SAP Ariba Buying*.
4. Choose *Start*. After the booster completes checking for the prerequisites, choose *Next*.
5. Choose to create a new subaccount or use an existing one. If you use an existing subaccount, choose a subaccount from the list. Specify the name, provider, and region for the subaccount.
6. Choose a service plan.
7. Choose *Next*.
8. In the *Create Formation step*, ensure that you have the formation type *Integration with SAP Ariba Buying* already specified for you. For more information, see Enabling SAP Ariba Buying.
9. In the *Include System* section, a system of type *SAP Ariba Buying* is automatically selected for you. This system is added when you create a subaccount in your global account for SAP Ariba Buying in the SAP BTP cockpit.
10. Choose the systems for the Identity Authentication service and SAP S/4HANA Cloud.
11. Choose *Next*.
12. Review your changes and choose *Finish*.

    ⓘ Note

    - In some cases, if you encounter an error while running the booster, you can run the booster again. However, you must ensure that you remove the configurations that the booster created in the earlier run. If you need further assistance, you can also raise an incident using the component `S2P-P2O-SET`.

- Although you can use the booster for some initial setup, you must also manually set up the required configuration using the steps described in this guide.

Next Steps

For more information about the steps to configure, see Steps for Setting Up SAP Ariba Buying, base edition.

3.1.2.1.2 Subscribing to SAP Ariba Buying, Base Edition Without the Booster

This section contains information about setting up manually without using the booster.

Overview [page 11]
    Set up SAP Ariba Buying manually without using the booster to get a subscription.

Create Subaccounts in Your Global Account [page 12]
    Create a new subaccount or use an existing subaccount in your global account in the SAP BTP cockpit.

Create a Tenant in the Identity Authentication Service [page 12]
    Create a tenant in the Identity Authentication service and establish a trust between the identity authentication service and SAP BTP. You must have the administrator permissions.

Subscribing to SAP Ariba Buying, Base Edition Without Using the Booster [page 13]
    Follow this procedure to manually subscribe to a service and a plan without the booster for SAP Ariba Buying, base edition from the SAP BTP cockpit.

Subscribe to Services Required for SAP Ariba Buying [page 14]
    You need additional subscriptions to some services for your subaccount to use certain functionalities in SAP Ariba Buying, base edition.

3.1.2.1.2.1 Overview

Set up SAP Ariba Buying manually without using the booster to get a subscription.

You can also use the booster to guide you through some steps in setting up a subscription and configuring SAP Ariba Buying with SAP S⁄4HANA Cloud on SAP Business Technology Platform (SAP BTP).

The booster helps you to configure SAP Ariba Buying, base edition easily without many manual procedures.

For more information about the using the booster, see Subscription to SAP Ariba Buying, Base Edition Using the Booster.

.

3.1.2.1.2.2 Create Subaccounts in Your Global Account

Create a new subaccount or use an existing subaccount in your global account in the SAP BTP cockpit.

Choose one of the following options to create the subaccounts:

- Use the following steps to create a subaccount for your global account:
  - Create the required subaccounts for your global account in the SAP BTP cockpit. When you create a subaccount, you also get the role of the administrator.
    For more information about creating the subaccount, see Create Subaccount.
  - Assign the required roles to the administrator. For more information, see Assign Roles in the SAP BTP Cockpit.

  If you have an existing subaccount, you can continue to use it. Ensure that you have the required roles for your subaccount.
- You can also use the booster to create a new subaccount.
  For more information about the using the booster, see Subscription to SAP Ariba Buying, Base Edition Using the Booster.

3.1.2.1.2.3 Create a Tenant in the Identity Authentication Service

Create a tenant in the Identity Authentication service and establish a trust between the identity authentication service and SAP BTP. You must have the administrator permissions.

Choose one of the following options to create a tenant in the Identity Authentication service:

- Do the following:
  - Establish a trust for the tenant between the identity authentication service and SAP BTP.
  - You can also use an existing tenant in the Identity Authentication service.
    For more information, see Establish Trust and Federation Between UAA and Identity Authentication.
- You can also use the booster to create a tenant in the Identity Authentication service and establish a trust between the identity authentication service and SAP BTP. If you have run the booster, you can skip this step.
  For more information about the using the booster, see Subscription to SAP Ariba Buying, Base Edition Using the Booster.

3.1.2.1.2.4 Subscribing to SAP Ariba Buying, Base Edition Without Using the Booster

Follow this procedure to manually subscribe to a service and a plan without the booster for SAP Ariba Buying, base edition from the SAP BTP cockpit.

Prerequisites

- You must have the following before you request a subscription for SAP Ariba Buying, base edition.
    - A license for SAP Ariba Buying, base edition.
    - A global account on SAP BTP. For more information, see Getting Started with the Universe of SAP S/4HANA Cloud, public edition.
    - Register the SAP S/4HANA Cloud system with the global account in the SAP BTP cockpit. When you register your system, ensure that you choose the formation type *Integration with SAP Ariba Buying* from the *Communication Scenario Groups* dropdown menu.
      For more information, see Register an SAP S/4HANA Cloud System in a Global Account and Enabling SAP Ariba Buying.
    - Required roles on SAP BTP. For more information, see Assign Users to Role Collections in the SAP BTP Cockpit.
    - A subaccount in your global account. For more information, see Create Subaccounts in Your Global Account.
    - You've established a trust between the SAP Business Technology Platform (SAP BTP cockpit) and Identity Authentication service administration. If you run the booster, the trust is established between the SAP Business Technology Platform (SAP BTP cockpit) and Identity Authentication service administration. For more information, see Setting Up Trust Between Identity Authentication and SAP BTP.

      > ⓘ Note
      >
      > - When you set up the trust, ensure that you select the domain that is also used by the tenant of the Identity Authentication service associated with the SAP S/4HANA Cloud Public Edition The domain you choose must end with "cloud.sap".
      > - When you establish trust with the Identity Authentication Service, ensure that the corresponding application created in the Identity Authentication Service contains the Global User ID as the subject name identifier.

      For more information about identity management, see Identity Management for SAP S/4HANA Cloud and Integrated Products.
    - You can subscribe and sign into SAP Ariba Buying only after you've established a trust between the SAP BTP cockpit and Identity Authentication service administration.
    - You must have a license to set up a 3-system landscape on your SAP S/4HANA Cloud system.
    - Ensure that you've activated the required scope items. For more information about activating the scope item, see Activating Scope Items.

Context

Perform the following steps to manually subscribe to a service and a plan without the booster.

Procedure

1. Open the SAP BTP cockpit.
2. Go to *Instances and Subscriptions* and choose *Create*.
3. Choose SAP Ariba Buying in the *Service* field.
4. Choose one of the following options in the *Plan* field:
   - *production*: Creates an instance for the production environment
   - *test*: Creates an instance for the test environment

   > ⓘ Note
   >
   > The test plan is for non-productive purposes only.

5. Choose *Create*. You can see the SAP Ariba Buying application in the *Subscription* section.
6. Choose *Subscribe*. You can see that the status of your subscription changes to *Subscribed*.
7. Choose *Go to Application*.

Next Steps

For more information about the steps to configure, see Steps for Setting Up SAP Ariba Buying, base edition.

3.1.2.1.2.5 Subscribe to Services Required for SAP Ariba Buying

You need additional subscriptions to some services for your subaccount to use certain functionalities in SAP Ariba Buying, base edition.

The SAP Ariba Buying, base edition license you buy also includes the Identity Authentication service. The Identity Authentication service provides you a simplified integration to managing user information.

To use the additional functionalities, SAP Ariba Buying, base edition requires the following cloud services. All the cloud services run on SAP Business Technology Platform. Technically it runs on capabilities that are now available in SAP Integration Suite and SAP Extension Suite.

You can view these services listed as applications in the *Instances and Subscription* page:

Do one of the following to subscribe to the additional services for SAP Ariba Buying:

- Use the booster to get an active subscription to the additional services for SAP Ariba Buying. If you have run the booster, you can skip this step.

For more information about the using the booster, see Subscription to SAP Ariba Buying, Base Edition Using the Booster.

- Perform the following steps:
  - Ensure you have a subscription to the following services in your subaccount:
    - SAP Audit Log Viewer for the Cloud Foundry Environment: Displays audit logs for your Cloud Foundry account. You must have the "free" plan for this service.
      We recommend that you enable audit logging to see detailed audit logs produced by SAP applications and services you've subscribed to.
      For more information on subscription, see SAP Audit Log Viewer for the Cloud Foundry Environment.
    - SAP Personal Data Manager service: Allows you to view the personal data information used by SAP Ariba Buying. You must have the "standard" plan for this service.
      For more information on subscription, see SAP Personal Data Manager service.
    - If you are using the SAP Data Retention Manager service: Allows you to set rules for managing the retention and deletion of data. You must have the "standard" plan for this service.
      For more information on subscription, see SAP Data Retention Manager service.

> ⓘ Note
>
> If you already have an existing subscription to any of the listed services for SAP Ariba Buying, you don't need another subscription for the same service.

3.1.3 Create New Users in Identity Authentication Service

Create new users in the administration console of the Identity Authentication Service.

For more information, see Manage Users.

> ⓘ Note
>
> Before you create users in the Identity Authentication Service, read about the workflow and prerequisites for maintaining the profile information for users. For more information, see About Managing User Information.

After you create users in Identity Authentication service, you must assign the users to user groups. For more information, see Assign Users to User Groups.

The users you create in Identity Authentication service must be assigned to a user group.

3.1.3.1   Assign Users to User Groups

The users you create in Identity Authentication service must be assigned to a user group.

Add one or more users created for a specific tenant to a group using the administration console for SAP Cloud Identity Services.

To add users to a group, do the following:

- Using the administration console for SAP Cloud Identity Services, create users. For more information, see Create Users.
- Create groups using the administration console for SAP Cloud Identity Services. For more information, see Managing Groups.
- Add the users created for a specific tenant to user group. For more information, see Add Users to a Group.
- Go to SAP BTP and assign the following role collections to the user group for a specific tenant:
  - Procurement Configuration Admin
  - Procurement User
  - Procurement Approver

  For more information on the role collections required, see Authorization [page 103].
- Create the mapping for the role collection as follows:
  - Log in to SAP BTP.
  - Go to ▶ *Security* ❭ *Trust Configuration* ❭.
  - Choose the SAP Cloud Identity Services tenant and go to the *Role Collection Mapping* page.
  - Map each of the following role collections to the associated user groups created in the SAP Cloud Identity Services:
    - Procurement Configuration Admin
    - Procurement User
    - Procurement Approver

For more information about user groups, see the section User Groups.

3.1.4 Configure OAuth 2.0 Client Authentication

Set up the OAuth 2.0 client credentials to connect SAP S/4HANA Cloud with SAP Ariba Buying, base edition on Business Technology Platform (SAP BTP).

You must configure the OAuth client credentials in the communication arrangement for the communication scenario *SAP_COM_0545 - SAP Ariba Buying Integration*.

Choose one of the following options to configure the OAuth client credentials:

1. Use the booster to configure the OAuth client credentials. If you have run the booster, you can skip this step.
   For more information about the using the booster, see Subscription to SAP Ariba Buying, Base Edition Using the Booster.
2. Use the steps in the following sections:
   - Creating Service Instances
   - Creating Service Bindings

Prerequisites

To create the OAuth 2.0 client credentials, you need to do the following:

- Create the following service instances for other environments on SAP BTP:
  - SAP Ariba Buying
  - Cloud Identity Service
- Create a service binding for the service instance.
- View the OAuth 2.0 client credentials for the service instances. Maintain the client credentials in the Communication Arrangement 0545.

  Creating Service Instances [page 17]
  > Follow this procedure to create a service instance to connect SAP Ariba Buying, base edition on SAP BTP with the SAP S/4HANA Cloud.

  Creating Service Bindings [page 19]
  > Follow this procedure to create a business service binding. A service binding enables you to get the client credentials for accessing SAP Ariba Buying, base edition.

3.1.4.1 Creating Service Instances

Follow this procedure to create a service instance to connect SAP Ariba Buying, base edition on SAP BTP with the SAP S/4HANA Cloud.

Prerequisites

You need the following to create the service instances on SAP Business Technology Platform (SAP BTP):

- Subscription to SAP Ariba Buying, base edition
- Subaccount on SAP BTP
- Role collection, Subaccount Service Administrator
  For more information about the role collection, see Assign the Subaccount Service Administrator Collection on the SAP Help Portal.

Context

Create the service instance for other environments and then create a binding for the service instance to connect to the SAP Ariba Buying, base edition application.

For more information on service instances, see Consuming Services in Other Environments Using the SAP Service Manager Instances on the SAP Help Portal.

Choose one of the following options to create the service instance:

- Use the booster to create the service instance. If you have run the booster, you can skip this step.
  For more information about the using the booster, see Subscription to SAP Ariba Buying, Base Edition Using the Booster.
- Use the following steps to create the service instance:

Procedure

1. Open the SAP BTP cockpit and choose the subaccount that you need to create a service instance.
2. Choose *Instances and Subscriptions*. You can view the service instances available for your environment.
3. Create the following service instances for SAP Ariba Buying, base edition:
   - SAP Ariba Buying
   - *Cloud Identity Service*
4. Choose *Create*. The *New Instance* wizard opens.
   1. Choose the service, SAP Ariba Buying from the *Service* dropdown list.
   2. Choose *apiaccess* as the service plan in the *Plan* field.
   3. Choose *Other* as the runtime environment.
   4. Enter a name for your service instance, then choose *Create*. For example, SAP Ariba Buying service.
      It takes a couple of minutes to see your newly created service instance. The *Status* column displays the status for the service instance.
5. Choose *Create* to create another service instance.
   1. Choose the service, *Cloud Identity Service* from the *Service* dropdown list.
   2. Choose *application* as the service plans.
   3. Choose *Other* as the runtime environment.
   4. Enter a name for your service instance, then choose *Next*. For example, SAP Ariba Buying client identity service.
   5. Enter the configuration in the JSON format for the service instance. Also specify the name of the service instance that you newly created in Step 4.
      For example:

      ⟨·⟩ Sample Code

      ```
      {
          "consumed-services": [
      {
          "service-instance-name": "<Instance-Name-of-the-SAP Ariba Buying-
      Service >"
          }
          ],
          "xsuaa-cross-consumption": true
      }
      ```

   6. Review and verify the details for the service instance. Use the preview to verify the instance details, then choose *Create*.
      It takes a couple of minutes to see your newly created service instance. The *Status* column displays the status for the service instance.

3.1.4.2 Creating Service Bindings

Follow this procedure to create a business service binding. A service binding enables you to get the client credentials for accessing SAP Ariba Buying, base edition.

Context

After you bind the service instance, you can view the client ID credentials.

Choose one of the following options to bind the service instance:

- Use the booster to bind the service instance. If you have run the booster, you can skip this step.
  For more information about the using the booster, see Subscription to SAP Ariba Buying, Base Edition Using the Booster.
- Use the following steps to bind the service instance:

Procedure

1. Open the SAP Business Technology Platform (SAP BTP) cockpit and choose the subaccount that contains the service instance that you need to create a service binding.

   For more information, see Creating Service Instances.

2. Choose *Instances and Subscriptions*. You can view the service instances available for your environment.

3. Choose the service instance, `Cloud Identity Service` that you newly created from the *Instances* table to create a service binding.

4. Choose the *Actions* menu then choose *Create Service Binding* from the dropdown list. The *New Binding* dialog box appears.

5. Enter a name for the binding in the *Binding Name* field. For example, SAP Ariba Buying.

   > ⓘ Note
   >
   > You don't need to specify any binding parameters for the basic authentication that the service instance requires.

6. Choose *Create*. It takes a couple of minutes to see the binding for the service instance. The *Status* column displays the status for the service instance.

7. Choose the *Actions* menu and then select *View* from the dropdown list. You can view the client ID and client secret for the service instance in the JSON file.

   Specify the client ID and client secret as the OAuth client credentials when you configure the Communication Arrangement 0545.

   > ⓘ Note
   >
   > - For more information about configuring the Communication Arrangement 0545, see Configure the Communication Management.

> To know more about service instances and service bindings in other environments, see Consuming Services in Other Environments Using the SAP Service Manager Instances on the SAP Help Portal.

3.1.5 Setting Up Roles for SAP Ariba Buying, Base Edition

You need certain roles to configure the business configuration and access the integrated services.

Ensure that you have the following roles set up in SAP Business Technology Platform (SAP BTP) for SAP Ariba Buying, base edition.

Buyer users need both the `Procurement_User` and `Procurement_Approver` roles to perform their tasks.

Role Name	This Role Allows You to....
`Procurement_Configuration_Admin`	Sign in as an administrator and configure the settings for SAP Ariba Buying, base edition. This role allows you to configure SAP Ariba Buying with SAP Business Technology Platform (SAP BTP) to connect with SAP S/4HANA Cloud.
`Procurement_User`	Add or edit line items in a request and submit the request. This role also allows you to add, update, or delete the comments you add in a request. You can also view the comments from your approvers.
`Procurement_Approver`	Approve items in a request. This role also allows you to add comments for line items in a request from the *My Inbox* app. To approve items, you also additionally need the role `WorkflowParticipant` in SAP BTP.
`ResponsibilityManagement`	Access the app *Manage Responsibility Rules*. For information about the roles for the SAP Responsibility Management service, see Defining and Bundling Roles.
`PDM_CustomerServiceRepresentativex`	View the personal data information for users. You can process and manage personal data requests for users using the app *Manage Personal Data*. For more information, see Assigning Roles.
`PDM_Administrator`	Export the personal data using the following: • If you are using the SAP Data Retention Manager service, use the app `Data Export` in the app *Personal Data Manager*. For more information, see Configuring Personal Data Manager. • If you are using the SAP Data Privacy Integration service, use the app *Manage Personal Data*. For more information, see - Assigning Roles.
`Subaccount_Service_Admin`	Get the administrative access to service brokers and environments for subaccounts. You also require this role to subscribe to applications.
`Destination Administrator`	Manage the configuration for destinations, certificates, and trust for subaccounts.
`Auditlog_Auditor`	Retrieve the audit logs for your subaccount using the SAP Audit Log Viewer service.
Roles for SAP Data Retention Manager	For information about roles see the following:

Role Name	This Role Allows You to....
	• If you are using the SAP Data Retention Manager service, see Managing Roles and Role Collections .
	• If you are using the SAP Data Privacy Integration service, see Assigning Roles to Users.
Roles for SAP Workflow Management	For more information about the roles in SAP Workflow Management, see Assigning Roles for Managing Approval Processes.

3.1.6 Configuring Destinations

Destinations contain the connection details for the remote services or systems you need to connect your application to.

Create and set up the destinations for your subaccount in the SAP BTP cockpit. Configure the destination using HTTP or mail destination type.

Use the destinations to connect to SAP S/4HANA Cloud.

Configure the mail destination to send and receive email notifications for email-related tasks in a workflow.

Configure Destinations for the Customer Tenant [page 21]
> The topics in this list cover the procedures for configuring various types of destinations for use with SAP Ariba Buying, base edition.

3.1.6.1   Configure Destinations for the Customer Tenant

The topics in this list cover the procedures for configuring various types of destinations for use with SAP Ariba Buying, base edition.

To configure destinations, you must have the role, `Destination Administrator` for you subaccount.

Creating the Destination for SAP Ariba Buying, Base Edition [page 22]
> Follow this procedure to create the destination that establishes a connection between SAP Ariba Buying, base edition and the connected system.

Creating the Destination for a Shopping Site [page 23]
> Follow this procedure to create the destinations for connecting to shopping sites of type *Ariba* or *Seller*.

Creating the Destination to Shop from a Supplier's Website [page 25]
> Follow this procedure to create a destination that enables shopping from a supplier's website from SAP Ariba Buying. Suppliers manage the catalogs hosted on their website, and buyers can buy items directly from the supplier's website.

Creating a Mail Destination [page 26]
> Follow this procedure to configure the mail destination for sending and receiving email notifications for email-related tasks in approval workflows.

Creating the Destination for Identity Authentication Service [page 27]

Follow this procedure to create a destination in SAP Business Technology Platform (SAP BTP) for SAP Ariba Buying, base edition. SAP Ariba Buying requires this destination to connect to the identity directory of Identity Authentication service.

3.1.6.1.1 Creating the Destination for SAP Ariba Buying, Base Edition

Follow this procedure to create the destination that establishes a connection between SAP Ariba Buying, base edition and the connected system.

Prerequisites

To use the client certificate authentication, you need an X.509 client certificate signed by a trusted certificate authority (CA). For more information about the list of all root CAs approved by SAP Global Security, see SAP Note 2801396 (SAP Global Trust List). The certificate must be in the .p12 or in .pfx format.

Context

SAP Ariba Buying, base edition uses the destination to retrieve the data while setting up users or creating requests.

Choose one of the following options to create the destination:

1. Use the booster to create a new destination for SAP Ariba Buying. If you have run the booster, you can skip this step.
   For more information about the using the booster, see Subscription to SAP Ariba Buying, Base Edition Using the Booster.
2. Use the following steps to create a destination.

Procedure

1. Open the SAP BTP cockpit.
2. Choose your subaccount available in your global account.
3. Choose *Connectivity* and then click *Destinations*.
4. Click *New Destination*.
5. Enter `ngproc-consys` as a name for the destination. Ensure that you enter the destination name accurately.
6. Choose the type `HTTP` in the *Type* field.
7. (Optional) Enter a description for the destination.

8. Enter the API URL for the communication arrangement SAP_COM_0545 as the destination in the *URL* field. For example, https://<API URL>. For more information about the SAP_COM_0545 communication arrangement for SAP Ariba Buying, see Creating Communication Arrangement.

9. Choose *Internet* in the *Proxy Type* field.

10. Choose the authentication type **ClientCertificateAuthentication** in the *Authentication* field.

11. Choose *Upload and Delete Certificate* to upload the client certificate for your SAP S/4HANA Cloud tenant. The Certificate dialog box appears.

12. Select the certificate from the file location and click *Upload*. Ensure that the certificate you upload is signed by a trusted certificate authority (CA). The client certificate must be in the .p12 or in .pfx format.

13. On the *Destinations* page, choose the client certificate you uploaded from the *Key Store Location* drop-down menu.

14. Enter a password in the *Key Store Password* field to validate your client certificate.

15. Choose the *Use default JDK truststore* checkbox.

16. Save the changes.

3.1.6.1.2   Creating the Destination for a Shopping Site

Follow this procedure to create the destinations for connecting to shopping sites of type *Ariba* or *Seller*.

Prerequisites

Ensure that your organization is registered on the SAP Ariba developer portal and that you've obtained credentials to access the following APIs:

- Internal Catalogs Shop API
- Public Catalogs Shop API

For more information, see Help for the SAP Ariba Developer Portal and Configure SAP Ariba APIs.

Context

> ⚠ Caution
>
> Please note that setting up a connection to a supplier's website excludes EU access compliance.

Procedure

1. Open the SAP BTP cockpit.

2. Choose your subaccount available in your global account.

3. Choose *Connectivity* and then click *Destinations*.

4. Choose *New Destination*.

5. Do one of the following:

    - To shop from internal catalogs in your SAP Ariba solution, enter `ARIBA_CATALOG_PROVIDER` in the *Name* field.

    - To shop from public catalogs from suppliers on SAP Business Network, enter `MX_SELLER_CATALOG_PROVIDER` in the *Name* field.

6. Choose the type `HTTP` in the *Type* field.

7. (Optional) Enter a description for the destination.

8. In the *URL* field, enter the runtime URL of the corresponding SAP Ariba API:

    You can get the URL from the *Environment details* section of the API's discovery page on the SAP Ariba developer portal.

9. Choose *Internet* in the *Proxy Type* field.

10. Choose the authentication type `OAuth2ClientCredentials` in the *Authentication* field.

11. You don't have to choose the *Use mTLS for token retrieval* checkbox.

12. In the *Client ID* field, enter the *OAuth Client ID* value generated for your application in the SAP Ariba developer portal.

13. In the *Client Secret* field, enter the *OAuth Secret* value generated for your application in the SAP Ariba developer portal.

14. Choose *Dedicated* as the URL type for the token service in the *Token Service URL Type* field.

15. Enter the URL for the token service in the *Token Service URL* field.

    Example: `{{oauth_server_url_prefix}}/v2/oauth/token`

    `{{oauth_server_url_prefix}}` represents the OAuth server URL prefix value available in the *Environment details* section of the API's discovery page on the SAP Ariba developer portal.

16. Go to the *Additional Properties* section and choose *New Property*. Specify the following property:

Property Name	Value
apiKey	Application key of your application on the SAP Ariba developer portal.

17. Make sure *Use default JDK truststore* is checked.

18. Choose *Save*.

3.1.6.1.3 Creating the Destination to Shop from a Supplier's Website

Follow this procedure to create a destination that enables shopping from a supplier's website from SAP Ariba Buying. Suppliers manage the catalogs hosted on their website, and buyers can buy items directly from the supplier's website.

Prerequisites

Ensure that the supplier is registered on SAP Business Network and a valid Ariba Network ID (*ANID*) is available for the SAP Business Network account.

Context

> ⚠ Caution
>
> Please note that setting up a connection to a supplier's website excludes EU access compliance.

Procedure

1. Open the SAP BTP cockpit.
2. Choose your subaccount available in your global account.
3. Choose *Connectivity* and then click *Destinations*.
4. Click *New Destination*.
5. Enter `Catalog_Punchout_Service` in the *Name* field.
6. Choose the type `HTTP` in the *Type* field:
7. (Optional) Enter a description for the destination.
8. Enter the URL for the destination in the *URL* field.

   Specify the URL from your cXML setup on SAP Business Network.
9. Choose *Internet* in the *Proxy Type* field.
10. Choose the authentication type `NoAuthentication` in the *Authentication* field.
11. You can specify additional properties. Click *New Property* and specify the following properties:
    * `tenantAnId`: Enter the *ANID* (Ariba Network ID) of your buyer account.
    * `tenantSharedSecret`: Enter the shared secret password to connect to the supplier's website.
12. Make sure *Use default JDK truststore* is checked.
13. Choose *Save*.

3.1.6.1.4   Creating a Mail Destination

Follow this procedure to configure the mail destination for sending and receiving email notifications for email-related tasks in approval workflows.

Context

Set up the mail destination with the SMTP server information in the provider tenant.

> → Remember
>
> You must configure the mail destination for approval workflows. If you don't configure the mail destination, you can encounter errors during approvals.

Procedure

1. Open the SAP BTP cockpit.
2. Choose your subaccount available in your global account.
3. Choose *Connectivity* and then click *Destinations*.
4. Click *New Destination*.
5. Enter `bpmworkflowruntime_mail` as the name of the mail destination.
6. Choose `MAIL` in the *Type* field.
7. (Optional) Enter a description for the destination.
8. Choose *Internet* in the *Proxy Type* field to access an external mail server.
9. Choose the authentication based on your requirement and specify its related values.
10. To specify additional properties, click *New Property* and specify the property and the required value.
    - Specify the following properties:

Property	Value
mail.transport.protocol	smtp
mail.smtp.auth	true
mail.smtp.starttls.required	true
mail.smtp.host	Host name of your mail server

Property	Value
`mail.smtp.port`	Port of your mail server that monitors the connections. Enter **587**. In some cases, you may need to enter **465**.
`mail.smtp.from`	Mail address of the "From" address for mails sent by the workflow capability. For example, **cpworkflow@example.com**.
	Enter the email address of an existing mailbox to receive the replies to emails from the workflow capability.
`mail.smtp.ssl.checkserve ridentity`	(Optional) **true** or **false**.
	The default value is **true**.
`mail.smtp.ssl.trust`	***** or a space-separated list of acceptable host names.
	If you don't provide a value, trust is based on the certificate provided by the server, which must be part of the SAP JVM default truststore. For more information, see Determine the Trusted CAs of SAP JVM Truststore.
`mail.bpm.send.disabled`	• **true**: When you set the value to **true**, emails are not sent from the mail server. You can set this value to block emails from the server when you're working on the workflow temporarily. • **false**

For more information about the properties, see Configure the Workflow Capability Mail Destination.

11. Save the changes.

3.1.6.1.5 Creating the Destination for Identity Authentication Service

Follow this procedure to create a destination in SAP Business Technology Platform (SAP BTP) for SAP Ariba Buying, base edition. SAP Ariba Buying requires this destination to connect to the identity directory of Identity Authentication service.

Prerequisites

• Ensure that you maintain the trust store and the key store certificate in the **Destinations** editor of SAP Business Technology Platform (SAP BTP).

Context

Configure this destination for SAP Ariba Buying, base edition to set up users from Identity Authentication service. You also need this destination for the SAP Responsibility Management service to use the standard rules and team functions. For more information, see Identity Authentication Service.

Procedure

1. Go to the SAP Business Technology Platform (SAP BTP) and navigate to your subaccount.
2. In the navigation pane, click ▶ *Connectivity* ❯ *Destination* ▶.
3. Click *New Destination*.
4. Enter the following information:

Parameter	Value
Name	**Identity_Authentication_Connectivity_IDS**
Type	**HTTP**
Description	Enter a description.
URL	Enter the URL containing the tenant ID of your Identify Authentication service. The URL displays in the following format: `https://<tenant ID>.accounts.ondemand.com/scim/Users` ⓘ Note Ensure that you add the URL of the Custom Identity Provider for Applications. For more information, see Establish Trust and Federation Between SAP Authorization and Trust Management Service and SAP Cloud Identity Services
Proxy Type	**Internet**
Authentication	**BasicAuthentication**
User	Add a new technical user as an administrator in the administration console for Identity Authentication. To add a new tenant administrator, you must have the Manage Tenant Configuration role. For more information, see the section Add System as Administrator.
Password	Specify the password of the administrator user in the Identity Authentication service.

5. Choose *Save*.

3.2 Configuring SAP S/4HANA Cloud

You configure and set up SAP S/4HANA Cloud to integrate with SAP Ariba Buying.

Ensure that you have the necessary business roles and requirements. For more information, see Assign Business Catalogs and Role Templates on SAP S/4HANA Cloud for SAP Ariba Buying, Base Edition [page 29].

Set up the communication user, communication system, and communication arrangement for SAP Ariba Buying.

> ⓘ Note
>
> Before you set up the communication management, ensure that you download the signing certificate from SAP BTP.

Assign Business Catalogs and Role Templates on SAP S/4HANA Cloud for SAP Ariba Buying, Base Edition [page 29]
    Assign business catalogs to the role templates that administrators, buyers and approvers require on SAP S/4HANA Cloud.

Configure Communication Management [page 30]
    The Communication Management apps allow you to establish secure communication in the exchange of data between SAP Ariba Buying, base edition and the SAP S/4HANA Cloud system.

Setting the Indicator for Goods-Receipt-Based Invoice Verification [page 35]
    You must set this indicator if you want to see the status flow for invoices in SAP Ariba Buying.

3.2.1 Assign Business Catalogs and Role Templates on SAP S/4HANA Cloud for SAP Ariba Buying, Base Edition

Assign business catalogs to the role templates that administrators, buyers and approvers require on SAP S/4HANA Cloud.

You assign business catalogs to business roles that are assigned to business users. Business catalogs contain authorizations that define the actions that a business user with a corresponding business role can do.

Administrators, buyers, and approvers need the following role templates and respective business catalogs assigned to their business user on SAP S/4HANA Cloud for SAP Ariba Buying, base edition:

For more information, see How to Create a Business Role for the Administrator.

Role Template	Business Catalog	This Role Template Allows You to....
SAP_BR_ADMINISTRATOR	SAP_CORE_BC_COM	Configure the communication scenario on SAP S/4HANA Cloud.
SAP_BR_EMPLOYEE_PROCUREMENT	1. SAP_MM_BC_REQUEST_PROCESS_PC 2. SAP_MM_BC_BUYING_MY_REQ_PC	Access the following applications: 1. *Create Purchase Request*

Role Template	Business Catalog	This Role Template Allows You to....
		2. *My Requests*
`SAP_BR_BPC_EXPERT`	`SAP_MM_BC_BUYING_CONFIG_PC`	Access the *Configure Buying* application from the SAP S/4HANA Cloud launchpad.
`SAP_BR_MANAGER_PROCUREMENT`	`SAP_MM_BC_BUYING_INBOX_PC`	Access the *My Inbox - Buying* application.

> ⓘ Note
>
> We recommend to unassign the business catalog `SAP_MM_BC_SSPPR_MANAGE_PC` when assigning the business catalog `SAP_MM_BC_REQUEST_PROCESS_PC`, and refrain from assigning both business catalogs to ensure a smooth user experience.

3.2.2 Configure Communication Management

The Communication Management apps allow you to establish secure communication in the exchange of data between SAP Ariba Buying, base edition and the SAP S/4HANA Cloud system.

You must have the role `SAP_BR_ADMINISTRATOR` to set up the communication arrangement. Ensure that you set up the communication user, communication system, and the following communication arrangements:

Communication Arrangement ID	Name of Communication Arrangement
SAP_COM_0545	SAP Ariba Buying Integration
SAP_COM_0A00	Integration with SAP Ariba Buying UI

Before you set up the communication user, communication system, and communication arrangement to use the client certification authentication method, ensure that you have an X.509 client certificate signed by a trusted certificate authority (CA). For more information about the list of all root CAs approved by SAP Global Security, see SAP Note 2801396 (SAP Global Trust List). The certificate you upload must be in the .p12 or in .pfx format.

Choose one of the following options to set up the communication user, communication system, and communication arrangement:

1. Use the booster to set up the communication user, communication system, and communication arrangement. If you have run the booster, you can skip this step.
   For more information about the using the booster, see Subscription to SAP Ariba Buying, Base Edition Using the Booster.
2. Use the steps in the following sections:
   * Creating a Communication User
   * Creating Communication Systems
   * Creating Communication Arrangement

   Creating a Communication User [page 31]

Use the app *Maintain Communication Users* app to create the communication user for inbound communication.

Use the app *Communication Systems* to create the communication system that represents the system for inbound and outbound services.

Use the app *Communication Arrangements* to create a communication arrangement.

3.2.2.1 Creating a Communication User

Use the app *Maintain Communication Users* app to create the communication user for inbound communication.

Prerequisites

To use the client certificate authentication, you need an X.509 client certificate signed by a trusted certificate authority (CA). For more information about the list of all root CAs approved by SAP Global Security, see SAP Note 2801396 (SAP Global Trust List).

Context

You can either create a new communication user or use an existing user. If you're using an existing communication user, skip this procedure. Ensure that the existing communication user has an X.509 client certificate signed by a trusted certificate authority (CA).

Choose one of the following options to set up the communication user:

1. Use the booster to set up the communication user. If you have run the booster, you can skip this step. For more information about the using the booster, see Subscription to SAP Ariba Buying, Base Edition Using the Booster.
2. Use the following steps:

Procedure

1. As an administrator, sign in the SAP Fiori launchpad of your SAP S/4HANA Cloud system.
2. Go to the app *Maintain Communication Users* (F1338). The *Create Communication User* screen appears.
3. Choose *New* to create a new communication user.
4. Enter a user name and description. For example, you can specify `4AI_INBOUND` as the user name.
5. Go to the section *Certificate* and then choose *Upload*.

6. Choose the X.509 client certificate signed by a trusted certificate authority (CA) and then click *Upload*.

7. Choose *Create*.

3.2.2.2 Creating Communication Systems

Use the app *Communication Systems* to create the communication system that represents the system for inbound and outbound services.

Prerequisites

- You must have a communication user using the client certificate authentication for the communication system. For more information, see Creating a Communication User.

Context

Create the communication system for SAP Ariba Buying, base edition. The the communication system enables the data exchange between SAP BTP and SAP S/4HANA Cloud system.

Choose one of the following options to set up the communication system:

1. Use the booster to set up the communication system. If you have run the booster, you can skip this step. For more information about the using the booster, see Subscription to SAP Ariba Buying, Base Edition Using the Booster.
2. Use the following steps:

Procedure

1. As an administrator, sign in the SAP Fiori launchpad of your SAP S/4HANA Cloud system.
2. Go to the app *Communication Systems* `(F1762)`.
3. Choose *New*. The *New Communication System* dialog box appears.
4. Enter the following information:
- *System ID*: `<Your Communication System ID>`, for example, `4AI_System`
- *System Name*: `<Your Communication System Name>`, for example, `4AI_System`
5. Choose *Create*.
6. On the *Communication System* page, go to the *General* tab. Enter the following information:
    - *Host Name*: Get the host name for SAP Ariba Buying from the SAP BTP application. Enter the host name after removing "https://" from the Host URL available for SAP Ariba Buying. Ensure that you also remove the backslash at the end of the Host URL.

- *UI Host Name*: Get the host name for SAP Ariba Buying from the SAP BTP application. Enter the host name after removing "https://" from the Host URL available for SAP Ariba Buying. Ensure that you also remove the backslash at the end of the Host URL.
- *Logical System*: Leave this field blank.
- *Business System*: Enter the tenant ID. You can view the information for the tenant ID in the *General* section of your subaccount.
- *Port*: Enter **443**.

7. In the *OAuth 2.0 Settings*, enter the following:

- *Auth. Endpoint*: **<Host name of the Identity Authentication Service tenant>/oauth2/ authorize**
- *Token Endpoint*: **<Host name of the Identity Authentication Service tenant>/oauth2/ token**
- *Audience*: Leave this field blank.
- *mTLS Endpoint*: Leave this field blank.

8. In the section *Users for Inbound Communication*, choose *Add*. The *New Inbound Communication User* dialog box appears.

9. In the *New Inbound Communication User* dialog box, enter the following information:

- *Authentication Method*: From the dropdown list, choose *SSL Client Certificate*.
- *User Name/Client ID*: Use the `F4` function key to view and choose the communication user with the SSL client certificate from the dropdown list. You can also search for a user.
- Choose *OK*.

10. In the *Users for Outbound Communication*, choose *Add*. The *New Outbound Communication User* dialog box appears.

11. Maintain the following information in the *New Outbound Communication User* dialog box:

- *Authentication Method*: Choose OAuth 2.0.
- *OAuth 2.0 Client ID*: Enter the client ID.
- *Client Secret*: Enter the client secret.

> ⓘ Note
>
> For more information on how to configure the OAuth 2.0 client authentication, see Configure OAuth 2.0 Client Authentication.

12. Choose *Save*.

3.2.2.3 Creating Communication Arrangements

Use the app *Communication Arrangements* to create a communication arrangement.

Context

- You must have a communication user using the client certificate authentication for the communication system. For more information, see Creating a Communication User.

- To use the client certificate authentication, you need an X.509 client certificate signed by a trusted certificate authority (CA). For more information about the list of all root CAs approved by SAP Global Security, see SAP Note 2801396 (SAP Global Trust List).

Set up the communication arrangements for the following:

Communication Arrangement ID	Name of Communication Arrangement
SAP_COM_0545	SAP Ariba Buying Integration
SAP_COM_0A00	Integration with SAP Ariba Buying UI

Choose one of the following options to set up the communication arrangement:

1. Use the booster to set up the communication arrangement. If you have run the booster, you can skip this step.
   For more information about the using the booster, see Subscription to SAP Ariba Buying, Base Edition Using the Booster.
2. Use the following steps:

Procedure

1. As an administrator, sign in the SAP Fiori launchpad of your SAP S/4HANA Cloud system.
2. Go to the app *Communication Arrangements* `(F1763)`.
3. Choose *New*.
4. Enter the following information:
   - *Scenario*: Choose `SAP_COM_0545` SAP Ariba Buying Integration.
   - *Arrangement Name*: `<Arrangement Name>`
   - Choose *Create*.
5. On the *Communication Arrangements* page, go to the *Common Data* section and enter the following information as per your business requirements:
   - *Communication System*: Select the communication system you created in Creating Communication Systems.
     The value you select for the communication system also appears for the following:
     - Inbound communication
     - Inbound services
     - Outbound communication
6. In the *Inbound Communication* section, choose the user name of the communication user in the *User Name* field. Choose the user that you have assigned to the SSL client certificate for the communication system.
7. You can view the following inbound services and their related values available for the communication arrangement:
   - *Value help service*
   - *Purchase Requisition*

8. In the *Outbound Communication* section, maintain the following values:
    - *OAuth 2.0 Client ID*: Choose the user you newly created as the Communication User.
    - *Authentication Method*: OAuth 2.0. This value is auto populated for you.

9. In the *Outbound Services* section, maintain the following values:
    - Service: *Purchase Order – Notify about Update of Item History*
        - *Service Status*: Select the *Active* checkbox.
        - *Application Protocol*: `SOAP`. This value is auto populated for you.
        - *Port*: Enter `443`.
        - *Path*: Enter the following value:
          `/api/s4-connectedsystem-soap-adapter-service-srv-api/v1/`
          `S4ConnectedSystemSoapAdapterService/updateStatus`
        - *Service URL*: This value is auto populated for you:
          `https://<Host name of the communication system>:<port>/<path value>`

10. Choose *Save*. The communication arrangement for SAP_COM_0545 is now active.

11. Perform the following steps to create the communication arrangement for SAP_COM_0A00:
    1. Go back to the *Communication Arrangements* page and choose *New*.
    2. Enter the following information:
        - *Scenario*: Choose `SAP_COM_0A00 SAP Ariba UI Integration`.
        - *Arrangement Name*: `<Arrangement Name>`
        - Choose *Create*.
    3. On the *Communication Arrangements* page, go to the *Common Data* section and choose the following information:
        - *Communication System*: Select the communication system you created in Creating Communication Systems.
    4. In the *Outbound Services* section, choose *Use embedded*.
    5. Choose *Save*. The communication arrangement for SAP_COM_0A00 is now active.

12. Your changes to the communication arrangements are now active with the required configurations.

3.2.3 Setting the Indicator for Goods-Receipt-Based Invoice Verification

You must set this indicator if you want to see the status flow for invoices in SAP Ariba Buying.

Context

To allow procurement users to see the status flow for invoices when they track the line items in the requests, we recommend that you set the indicator `GR-Based IV` for goods-receipt-based invoice verification for business partners (suppliers). When you define the field group for the business partner, all purchase orders created in SAP S/4HANA Cloud have the setting `GR-Based IV (Goods-Receipt-Based Invoice Verification)` enabled.

For more information about the status flow in requests, see Viewing the Approval Workflow and Status Flow for an Item in a Request .

Procedure

1. In your configuration environment, use the search function to open the following activity: *Define Account Groups with Screen Layout (Vendors)*. For more information, see Configuration Environment of SAP S/4HANA Cloud.
2. In the configuration step, select *Supplier*, and go to *Details*.
3. Double-click *Purchasing Data* under *Field Status*, and do the same on the next screen under *Select Group*.
4. In the *Purchasing Data* section, set the field *Req. Entry* for `GR-Based IV (Goods-Receipt-Based Invoice Verification)` to mark the good receipt mandatory.

> ⓘ Note
>
> SAP Ariba Buying supports processing purchase orders with only a single line item from purchase requisitions created on the connected system.

3.3 Configuring SAP Ariba Buying, Base Edition

Find the concepts and steps involved in configuring the SAP Ariba Buying, base edition application.

> ⚠ Caution
>
> Please note that configuring the service Procurement Search excludes EU access compliance.

Master Data in SAP Ariba Buying, Base Edition [page 37]
   Master data in SAP Ariba Buying, base edition is sourced from the customer's ERP system.

Managing Authorizations for Users [page 38]
   The topics in this list cover the concepts and procedures involved in granting users the permission to perform their tasks.

Managing User Information [page 44]
   The topics in this list cover the concepts and procedures involved in managing profile and default accounting information for users.

Editing Document IDs [page 53]
   Administrators can define a first document ID for a series of business documents to ensure that unique IDs are consecutively assigned to newly created documents.

Mapping Classification Codes with Material Groups [page 53]
   The topics in this list cover the concepts and procedures involved in mapping UNSPSC classifications in the catalog to material groups in the connected system so item requests can be processed correctly.

Managing Units of Measure [page 56]
   The topics in this list cover the concepts and procedures involved in mapping the units of measure used in supplier catalogs to the units of measure defined in the connected system.

3.3.1 Master Data in SAP Ariba Buying, Base Edition

Master data in SAP Ariba Buying, base edition is sourced from the customer's ERP system.

This master data is necessary for configuring SAP Ariba Buying, base edition. It is used to ensure accurate processing of purchase requests in terms of performing budget checks, ensuring costs are assigned to the correct cost center, ensuring that items are shipped to the correct location, and so forth.

The SAP Ariba Buying data model is harmonized with that of all other SAP products that have SAP S/4HANA Cloud at their core.

The following master data is sourced from the customer's ERP system:

- Plant
- Purchase groups
- Company codes
- Cost centers
- Purchasing organizations
- General Ledger accounts
- Material groups
- Unit of measure
- Currency
- Suppliers(Business Partners)

In SAP Ariba Buying, base edition, this data is used for the following purposes:

- Creating the user's profile

- Configuring the application
- Tailoring the buying experience in general

For information about the relationship between Company Code , Plant, and Purchasing Org in SAP S/4HANA Cloud, see About Configuring the Organizational Structure.

3.3.2 Managing Authorizations for Users

The topics in this list cover the concepts and procedures involved in granting users the permission to perform their tasks.

SAP Ariba Buying administrators define authorization policies that allow users to use certain company codes and plants based on the authorization defined for them.

SAP Ariba Buying has basic authorization policies for all users. You can create new policies for specific company codes and plants. Assign users to the basic authorization policies or custom policies.

Follow this procedure to create an authorization policy that authorizes certain company codes and plants for assigned users.

Follow this procedure to grant users the permissions they need to perform their tasks in SAP Ariba Buying, base edition.

3.3.2.1 About Managing Authorizations for Users

SAP Ariba Buying administrators define authorization policies that allow users to use certain company codes and plants based on the authorization defined for them.

As an administrator, you can create policies to allow or restrict users to specific company codes and plants.

SAP Ariba Buying provides the following basic authorization policies that are available for you:

- **Procurement_User**
- **Procurement_Items**

The basic authorization policies allow you to view items and create requests related to all company codes and plants in your organization.

You can choose to use the basic authorization policies that are available for you. You don't need to make any changes to the basic authorization policy. Alternatively, you can also create a new authorization policy using the basic authorization policy and modify it based on your requirements.

As an administrator, you can create new authorization policies and grant users the required permissions as follows:

- When you choose the Procurement_User basic authorization policy, you grant users the permission to:
  - Submit requests based on all the company codes and plants available in the organization

However, you can customize the Procurement_User basic authorization policy to do the following:
- Restrict access to view or add items to a request related to specific company codes
- Restrict access to view or add items to a request related to specific company codes and plants

> ⓘ Note
>
> To add items and create a request, you must always have either the Procurement_User basic authorization policy or a customized Procurement_User authorization policy.

- The basic authorization policy, Procurement_Items allow users to add unlisted items to a request.
  When you choose the Procurement_Items basic authorization policy, you grant users the permission to:
  - Add unlisted items to a request and submit the request
  You can customize the Procurement_ Items basic authorization policy to do the following:
  - Restrict access to add unlisted items in a request related to specific company codes
  - Restrict access to add unlisted items to a request related to specific company codes and plants
  - Restrict access to submit a request with unlisted items related to specific company codes
  - Restrict access to submit a request with unlisted items related to specific company codes and plants

> ⓘ Note
>
> When you assign the Procurement_Items or a customized Procurement_Items authorization policy, you must additionally assign users to the Procurement_User basic authorization policy.

Ensure that you have the required roles to enable you to administer the authorization policies. For more information on the roles, see Configuring Authorization Policies. For more information on creating new authorization policies for SAP Ariba Buying, see Creating a New Authorization Policy [page 42].

For additional information, see the following:

- To know more about assigning authorization policies for users, see Assign Authorization Policies.
- To know more about configuring authorization policies for users, see Configuring Authorization Policies.
- For more information about editing the administrators' authorizations, see (Optional) View and Edit a Privacy Policy Document.

3.3.2.2 Authorization Policy for SAP Ariba Buying

SAP Ariba Buying has basic authorization policies for all users. You can create new policies for specific company codes and plants. Assign users to the basic authorization policies or custom policies.

You can assign users to any of the following basic authorization policies that are available for you in SAP Ariba Buying:

Basic Authorization Policy	Allows users to.....
Procurement_User	Create requests with material items available on SAP Ariba Buying.
Procurement_Items	Create requests with unlisted items.

By default, these basic authorization policies allow users to view and add items to a request based on all the company codes and plants available in the organization.

Using the basic authorization policies, you can create new custom policies and specify certain company codes and plants and assign them to users.

You can do the following:

- Authorize users to submit requests with items related to all company codes.
  This authorization policy rule grants the user the authorization to submit requests based on all the company codes and plants available in the organization. The basic authorization policy *Procurement_User* already contains this authorization policy rule.
- Authorize users to view or restrict specific company codes.
  This authorization policy rule grants the user the authorization to only view and assign the company codes authorized for them. When you assign this rule, a user can submit requests containing items only related to the company codes and plants authorized for them.
- Authorize users to view or restrict specific plants.
  This authorization policy rule grants the user the authorization to only view and assign the plants authorized for them. When you assign this rule, a user can submit requests containing items only related to the plant and company codes authorized for them.
- Authorize users to add unlisted items to a request related to specific company codes and plants
  This authorization policy rule grants the user the authorization to add unlisted items to a request based on the company code and plant.
- Authorize users to submit a request with unlisted items related to specific company codes and plants
  This authorization policy rule grants the user the authorization to submit a request with unlisted items based on the company code and plant.

As an administrator, do the following to assign policies for users:

Assign a basic authorization policy. SAP Ariba Buying supports the following basic authorization policies:

- **Procurement_User** submit request based on all the company codes and plants available in the organization.
  When you assign the basic authorization policy **Procurement_User** to users, these users can view all the company codes and the associated plants in the organization in their profile settings. The items that buyers add to the request also relate to the plant and company codes authorized for them. The basic authorization policy allows buyers to view and create request with items related to all company codes and plants in the organization authorized for them.
  When you don't specify any authorization policy for users, they don't see any company codes or plants available for them. Users encounter an error while trying to view the company codes or plants in the *: To grant users the authorization to Profile Settings* page. An error also occurs when users don't have any authorization policy and try to submit a request.
- **Procurement_Items**:
  To grant users the authorization to add or submit a request with unlisted items.

You can create and assign authorization policies for users as follows:

1. Do one of the following:
   - Choose to use the basic authorization policies available for SAP Ariba Buying. If you use the basic authorization policies, you only need to assign them to users in the Identity Authentication service.
   - Create new authorization policies using the basic authorization policies available for SAP Ariba Buying in Identity Authentication service.
   If you choose the basic authorization policy **Procurement_User**, ensure that you specify the following:

Field Name	Operator	Specify the Value for...
CompanyCode	Choose any of the following: • = (EQUALS TO) • IN • IS RESTRICTED • IS NOT RESTRICTED	One or more company codes
Plant	• = (EQUALS TO) • IN • IS RESTRICTED • IS NOT RESTRICTED	One or more plants

If you choose the basic authorization policy **Procurement_Items**, ensure that you specify the following:

Field Name	Operator	Specify the Value for...
CompanyCode	Choose any of the following: • = (EQUALS TO) • IN • IS RESTRICTED • IS NOT RESTRICTED	One or more company codes
Plant	• = (EQUALS TO) • IN • IS RESTRICTED • IS NOT RESTRICTED	One or more plants
CatalogId	IS NULL	
ItemType	= (EQUALS TO)	Material
ItemCategory	= (EQUALS TO)	Standard

2. Assign the authorization policy to users in the Identity Authentication service.

> ⓘ Note
>
> • Ensure that you specify the exact values in the table.
> • When you don't specify the authorization policy for unlisted items, users don't see the option to request an unlisted item.

As an administrator, do the following to set up and assign authorization policies for users in the Identity Authentication service:

1. Ensure that you establish a trust with the identity provider in the SAP BTP cockpit. To establish a trust with the identity provider, do the following:
   • Log in to SAP BTP.
   • Go to ▷ *Security* 〉 *Trust Configuration* 〉.
   • Choose *Establish Trust*.
   • Select the identity provider and choose *Establish Trust*.

2. Create a service instance and service binding for the Identity Authentication service. For more information, see Configure OAuth 2.0 Client Authentication with SAP Ariba Buying.

3. As an administrator, you must have the `Manage Groups` role in the SAP Cloud Identity Services to manage all authorization policies for user in the organization.
   For more information about creating authorization policies, see Creating a New Authorization Policy [page 42].

4. Assign authorization policies for user groups. For more information, see Assigning Authorization Policies to Users [page 43].

When you create a new authorization policy, a new user group is automatically created with the same name you specify for the authorization policy. You can assign the newly created policy to users in the user groups. For more information, see Assigning Authorization Policies to Users [page 43].

> ⓘ Note
>
> When you create a new authorization policy from the basic authorization policy and specify the company code or plant, ensure that you only specify the following operators that SAP Ariba Buying supports in the *Select Operator* dialog box:
>
> - = (EQUALS TO)
> - IN
> - IS RESTRICTED
> - IS NOT RESTRICTED
> - IS NULL - This operator is only applicable for the CatalogId field.

Ensure that you have the required roles to enable you to administer the authorization policies. For more information on the roles, see Configuring Authorization Policies.

3.3.2.3 Creating a New Authorization Policy

Follow this procedure to create an authorization policy that authorizes certain company codes and plants for assigned users.

Context

Create a new authorization policy using the basic authorization policy. You can modify the basic authorization policy to authorize certain company codes and plants for assigned users based on your requirements.

Procedure

1. Sign in to Identity Authentication Service. For more information, see Authenticating Identity Provider for an Application.

2. Go to *Application & Resources* and then choose *Applications*.

3. Choose your application for SAP Ariba Buying. The application name includes the data center. For example, "procurement-<datacenter>."

4. Choose the *Authorization Policies* tab.

5. Choose *Create* to create a new authorization policy.

6. Click *Maintain Restrictions*.

7. Choose the basic authorization policy available for you.

8. Choose *Next*. The Create Policy page appears.

9. Specify the rules to restrict users based on the company code or plant. Enter the company codes and plant values that you want to authorize for users.

10. Choose *Next*.

11. Enter the name for the authorization policy. You can also specify a description.

12. Click *Create*.

   A new authorization policy is available for you. When you create a new authorization policy, a new user group is created with the same name you specified for the authorization policy.

   You can assign the newly created policy to users in the user groups. For more information, see Assigning Authorization Policies to Users.

3.3.2.4 Assigning Authorization Policies to Users

Follow this procedure to grant users the permissions they need to perform their tasks in SAP Ariba Buying, base edition.

Context

Granting permissions involves adding users to the user groups associated with specific authorization policies.

When you create a new authorization policy, a new user group is automatically created with the same name you specified for the authorization policy.

For more information, see Assign Authorization Policies.

Procedure

1. Sign in to Identity Authentication Service. For more information, see Authenticating Identity Provider for an Application.

2. Go to *Users & Authorizations* and then choose *User Groups*.

3. Search for the user group. The user group name would contain the name of the authorization policy.

4. Choose the user group and add the users.

3.3.3 Managing User Information

The topics in this list cover the concepts and procedures involved in managing profile and default accounting information for users.

3.3.3.1 About Managing User Information

Administrators can maintain the profile information for users in an organization. Profile information includes company code, currency, and accounting-related values such as cost center and plant.

Users can also change their own profile settings, as required.

The following workflow describes the process for maintaining the profile information for users. As an administrator, do the following to maintain the profile settings:

1. Configure the destination for SAP Ariba Buying, base edition to set up users from Identity Authentication service. For more information, see Creating the Destination for Identity Authentication Service [page 27].
2. Set the default values for users. Go to the app *Configure Buying* and then choose the app *Manage User Defaults*.
   Maintain the default values for each of the company codes that you require for the organization in the app, *Manage User Defaults*. Specify the company code-related values for the plant and currency. For more information, see Maintaining Default Values for Users [page 45].
3. Ensure that users are available on Identity Authentication services and the SAP S/4HANA Cloud system. The user you create on SAP S/4HANA Cloud system must be maintained as a business user. Each user must have the following:
   - A unique email ID that matches the email address in Identity Authentication service
   - Cost center for the work agreement
4. The users that you require must have an active work assignment on the SAP S/4HANA Cloud system. For more information about work assignment for users, see How to Create and Correct Work Agreements.

> ⓘ Note
>
> - Ensure that the work assignment for users that you add do not have the work agreement type, concurrent employment (a second employment for an employee in the same company).
> - In Identity Authentication services, ensure that all users have the employee ID information in the *Login Name* field. This information is required for displaying the name and ID of the user.

5. View the user information in the *Manage User Information* page.
6. Update the user information in the *Manage User Information* page. For more information on updating user information, see Updating the User Information.

Administrators must set up the user information in Identity Authentication service and the SAP S/4HANA Cloud system before users create a request on SAP Ariba Buying.

The user information in SAP Ariba Buying, base edition is populated with information available on Identity Authentication services at periodic intervals.

When you create a new user or edit the existing user information in Identity Authentication services, you don't see the user information immediately in SAP Ariba Buying, base edition. When a user leaves the company,

the administrator on Identify Authentication service deletes the user. In SAP Ariba Buying, base edition, users deleted from Identity Authentication service are retrieved at periodic intervals.

> ⓘ Note
>
> - When deleting users, administrators must ensure that the shadow users are also deleted from Identity Authentication services. For more information about deletion, see Deletion.

The user information is periodically synchronized between the Identity Authentication services and SAP S/4HANA Cloud using the scheduled jobs that run in the background. The scheduled jobs run at the following intervals:

Action	Scheduled job runs and updates are available...
When a new user is created	Every hour
When there is an update to the existing user information	Updates on Identity Authentication services • Every hour • Updates on SAP S/4HANA Cloud • Every 24 hours
When users are deleted	Every 24 hours

We recommend that you don't change the existing frequency of the scheduled jobs to update user information. However, if you choose to change the existing frequency for the scheduled jobs, you must create a case in ServiceNow using the component S2P-P2O-BC.

3.3.3.2   Maintaining Default Values for Users

Define the plant, purchasing organization, purchasing group, general ledger account, and currency for the company codes in your organization.

You define the company codes and specify the related values for the company code. The default values defined for the company code help in maintaining the user information accurately. The information available for the company code is based on the master data that you maintain on the connected system.

You must have the role `Procurement_Configuration_Admin` to define the default values for the company codes.

The app *Manage User Defaults* allows administrators to maintain the following related values for the company code:

- Plant
- Purchasing organization
- Purchasing group
- General ledger account
- Currency

When you define the default values for the purchasing organization, specify the purchasing organization defined for the Corporate-group-wide purchasing or Company-specific purchasing that you've maintained in

the connected system. For more information on purchasing organizations, see Configure Your Organizational Structure.

Administrators can create default values and save them as drafts. Changes can be made to the drafts and activated at a later point of time.

> ⓘ Note
>
> - Administrators must maintain unique company codes. Duplicate company codes are not supported.
> - Plant-specific purchasing organizations are not supported. If you have users with more than one purchasing organization associated to the company code, update their user information with the additional purchasing organizations using the CSV file in the app *Manage User Information*. For more information, see Updating the User Information [page 49].
> - Ensure that the values you specify for the purchasing organization match the related values maintained for the company code and purchasing organization in the connected system.

Maintaining the Default Values [page 46]
    Follow this procedure to maintain default currency and accounting-related values for the company codes you require for your organization.

3.3.3.2.1   Maintaining the Default Values

Follow this procedure to maintain default currency and accounting-related values for the company codes you require for your organization.

Prerequisites

You must have the role `Procurement_Configuration_Admin` to define the default values for the company codes.

Context

Define the company codes and specify the related values for the company code.

> ⓘ Note
>
> Buyer administrators must maintain unique company codes. Duplicate company codes are not supported.

Procedure

1. Go to the *Configure Buying* app.
2. Choose the app *Manage User Defaults*.
3. Choose *Create*. The *Create User Defaults* page appears.
4. Choose the company code and specify the following values related to the company code:
   - Plant
   - Purchasing organization
   - Purchasing group
   - General ledger account
   - Currency

   > ⓘ Note
   >
   > Ensure that you specify the purchasing organization defined for the Corporate-group-wide purchasing or Company-specific purchasing you've maintained in the connected system. Plant-specific purchasing organizations are not supported.

5. Click *Create*. You can review the newly added default values.
6. To edit the default values, go to the *Manage User Defaults* page. Choose the user default values and use the arrow icon on the right-hand side of the default values to view the details. Click *Edit*.

3.3.3.3   Maintaining Information for Multiple Users

As an administrator, you can set up user profile information for multiple users on Identity Authentication service.

SAP Ariba Buying, base edition retrieves the user information from Identity Authentication service each time a new user is created or there are changes to the existing user information. You can view the user information in the app *Manage User Information*.

You must have the role `Procurement_Configuration_Admin` to view and edit the profile information for multiple users.

When a user leaves the company, the administrator on Identify Authentication service deletes the user.

Before you set up the user information, ensure that you specify default values for the company code, plant, purchasing organization, purchasing group, general ledger account, and currency in the *Manage User Defaults* app. SAP Ariba Buying uses the default values for the company code when the company code doesn't exist for the user on the SAP S/4HANA Cloud system.

Users on SAP Ariba Buying can view catalog items based on their purchasing organization. If users have more than one purchasing organization associated to their company code, you can update their user information with the additional purchasing organizations in the app, *Manage User Information*. Download the CSV file and add the different purchasing organizations and other related information for the company code per user. Upload the CSV file and review the values maintained for the different purchasing organizations, purchasing groups, plants, and general ledger accounts related to the company code for each user.

You can also update the existing information for users on SAP Ariba Buying using the CSV file. Ensure that the CSV file you upload does not exceed 10 MB.

For more information on updating user information, see Updating the User Information [page 49].

The table in the *Manage User Information* page contains the following information:

Column Name	Description
User Name	ID for your user. Enter the value available in the *LogonName* field from the Identity Authentication services
Local User ID	Local ID of the user
Global User ID	Global ID of the user
Email	Email address of the user
Company Code	Company code associated to the user
Cost Center	Cost center associated to the user
Plant	Plant associated to the user
Purchasing Organization	Purchasing organization associated to the user
Purchasing Group	Purchasing group associated to the user
General Ledger Account	General ledger account associated to the user
Currency	Currency associated to the user

When there are changes to the user information on Identity Authentication services, SAP Ariba Buying, base edition retrieves and maintains the updated information. The newly retrieved user information applies to the newly added items in the existing carts and the newly created requests. The newly retrieved user information doesn't apply to the existing requests containing the user information. The existing requests continue to have the user information that were previously retrieved.

After you've maintained the user information on Identity Authentication service, users can review the changes to their user profile when they access SAP Ariba Buying, base edition for the first time. This is a one-time activity. However, each time there's a change to the user information on Identity Authentication service, users must review their user information again. Ensure that you maintain the profile information for users before they can create requests.

When you make changes to the authorizations for users, the users can no longer view the items related to the company code that were authorized before. The users must review the newly authorized company code and related values before they start creating requests.

When you either don't have the default values for the company code or it doesn't exist on the SAP S/4HANA Cloud system, you can view the user name, but you can't see the value for the company code, cost center, and joining date.

Viewing the User Information [page 49]
> Follow this procedure to view the user information for multiple users at one time.

Updating the User Information [page 49]
> Update the existing user information on SAP Ariba Buying using the CSV file. If users have more than one purchasing organization associated to their company code, update their user information with the additional purchasing organizations in the CSV file.

3.3.3.3.1 Viewing the User Information

Follow this procedure to view the user information for multiple users at one time.

Prerequisites

- You must have the role `Procurement_Configuration_Admin` to view the app *Manage User Information*.
- On Identity Authentication services, ensure that all users have the employee ID information in the *Login Name* field. SAP Ariba Buying, base edition requires this information to display the name and ID of the user.
- Ensure that default values are specified for the company code, plant, purchasing organization, purchasing group, general ledger account, and currency in the *Manage User Defaults* app after you maintain the user information.
  SAP Ariba Buying, base edition uses the default values for the company code when the company code doesn't exist for the user on the SAP S/4HANA Cloud system.

Context

Procurement administrators must ensure that they enter user information accurately on Identity Authentication service. If the information is incorrect, the user profile could have incorrect values.

Procedure

1. Go to the *Configure Buying* app.
2. Choose the app *Manage User Information*.
3. View the user information. Use the *Search* field to search for users, plants, company codes, etc.

3.3.3.3.2 Updating the User Information

Update the existing user information on SAP Ariba Buying using the CSV file. If users have more than one purchasing organization associated to their company code, update their user information with the additional purchasing organizations in the CSV file.

Prerequisites

- You must have the role `Procurement_Configuration_Admin` to view the app *Manage User Information*.

- On Identity Authentication services, ensure that all users have the employee ID information in the *Login Name* field. SAP Ariba Buying requires this information to display the name and ID of the user.
- Ensure that default values are specified for the company code, plant, purchasing organization, purchasing group, general ledger account, and currency in the *Manage User Defaults* app.
  We recommend that you maintain the default set of values for each company code in the *Manage User Defaults* app. This ensures that when users are created and replicated in SAP Ariba Buying based on their company code, the organizational attributes (purchasing organization, purchasing group, general ledger account, plant, currency) are automatically derived. When the organizational attribute values are not maintained in the Identity Authentication service, the values you see in SAP Ariba Buying are also with empty values. In such cases, you can upload the required values using the CSV file.
  While entering values for the different purchasing organizations in the CSV file, ensure that you maintain the other related information for the company code per user. After you upload the CSV file, you can review the values maintained for the different purchasing organizations, purchasing groups, plants, and general ledger accounts related to the company code for each user.
  Ensure that you keep the following in mind before you upload the CSV file:
  - The CSV file must not exceed 10 MB.
  - If you modify the columns in the CSV file containing the company code, cost center, purchasing organization, purchasing group, general ledger account, or currency, all the previously maintained values are overwritten.
  - We recommend that you do not edit the values in columns UserName, LocalUserID, GlobalUserID and Email. When you modify these values, the file you're trying to upload fails with errors and the values remain unchanged. SAP Ariba Buying uses the information available for users from the Identity Authentication service.
    You can choose *Download Errors* to download the error file and view the errors.
  - Empty rows in the CSV file are skipped during processing.
  - When the CSV file contains duplicate user entries, only the first valid entry is processed for the user. All other duplicate entries are not considered.
  - When you upload the CSV file containing any updates to the user information, SAP Ariba Buying does not apply the values available in the app *Manage User Defaults*.

Context

Procurement administrators must ensure that they enter user information accurately on Identity Authentication service. If the information is incorrect, the user profile could have incorrect values in SAP Ariba Buying.

Procedure

1. Go to the *Configure Buying* app.
2. Choose the app *Manage User Information*.
3. Choose *Download* to download the user information. The file gets downloaded in a CSV format file.
4. Update the user information in the downloaded CSV file.

We recommend that you only have the values that needs changes in the CSV file. To optimize the processing time, remove the entries that do not need changes before you upload the CSV file.

5. Save the CSV file.

6. Choose *Upload* and then choose the CSV file containing the updated user information.

3.3.3.4 Managing User Profiles

Administrators set up and maintain the profile settings for users in their organization. The user profile contains personal information about the user and their organization.

Each user profile contains information for the following:

- Name and address of your organization
- Shipping information
- Accounting information
- Currency

When users sign in for the first time, they can review the information available for their user profile. However, when you change their user information, these users must review their profile settings again before they can start creating requests.

Users can also change their profile settings, as required. The user profile information is automatically populated by the information that the administrator uploads from SAP Ariba Buying, base edition to SAP BTP.

When you make changes to the authorizations for users, the users can no longer view the items related to the company code that were authorized before. Users must review the newly authorized company code and related values before they start creating requests.

> ⓘ Note
>
> - Ensure that you have the necessary authorization policies set up for you. When you don't have any authorization policy assigned, you don't see any company codes or plants in the *Profile Settings* page. For more information, see Managing Authorizations for Users [page 38].
> - If the validity period of the cost center has passed the time duration, you can no longer view the items. Users must review the user profile and choose another cost center with a valid time period related to company code.
> - You can manage your currency exchange rates from the connected system. The price of items is derived based on the currency exchange rates available on the connected system.

Configuring the Profile Setting [page 52]
Follow this procedure to set up your user profile before you start creating requests.

3.3.3.4.1 Configuring the Profile Setting

Follow this procedure to set up your user profile before you start creating requests.

Context

Review the user information and the details in the *Organization*, *Accounting*, and *Currency* sections of your user profile.

> ⓘ Note
>
> - This is a one-time activity. However, you must review the user information again when there are any changes to the profile settings.
> - Ensure that you have the necessary authorization policies set up for you. When you don't have any authorization policy assigned, you don't see any company codes or plants in the *Profile Settings* page. When you don't specify a value in any of the fields or the value doesn't relate to the company code or plant, an error occurs. View the errors and make the necessary changes for the user profile.

Procedure

1. Choose the app *Create Purchase Request*. The home page appears.
2. Choose the menu icon ••• *(Additional Options)* and then choose *Profile Settings*. The user information is already available for you in the *Profile Settings* page.
3. View the user and shipping information. The user information reflects the master data available on the connected system. Do one of the following:

   - Use the existing default values in the *Ship To* and *Shipping Address* fields.
   - Ship to another user with a different delivery address. Choose from the list of values available in the *Ship To* and *Shipping Address* fields. Use the F4 function key to view and choose the values in the dropdown list. You can also search for a user or shipping address.
     You can view the delivery address for the plants and the company codes that have been authorized for you.

4. In the section *Organization and Accounting*, specify the information for the following:

   - *Organization*
     - *Company Code*
     - *Plant*

     You can view the company codes and the associated plants authorized for you. Search or choose from the list of company codes and plants.
   - *Accounting*
     - *Cost Center*

       Specify the cost center related to the company code. You can view the cost centers associated to the company code authorized for you.

5. In the *Currency* field, enter a value to search or choose from the list of currencies.

6. Choose *Start Shopping* to save the changes and proceed to shop for items.

3.3.4 Editing Document IDs

Administrators can define a first document ID for a series of business documents to ensure that unique IDs are consecutively assigned to newly created documents.

As an administrator, you can edit the document ID and thus define the subsequently created document IDs according to your business needs.

Procedure

Select the entry for the document category Purchase Request in the list view and change to Edit mode. Under General Information, adapt the Prefix and Starting Number that you want to have. Prefix and starting number combined give your new First Document ID, based on which the subsequent document IDs are created and assigned to new documents. The Current Document ID shows you the document ID that has been assigned last to a purchase request.

> ⓘ Note
>
> Note that you can use underscores, hyphens and uppercase letters A-Z for a prefix, and numerals 0-9 for the starting number.

Activation

The status *Active* indicates that your changes have been processed. In some cases, it can take up to several minutes for your changes to be processed. In this case, you'll see the status *Changes Pending*. In case of an error, the document IDs are reverted to the previous state, and you have to redo your changes.

Changes in Document ID

Anytime you edit a document ID by changing either the prefix, the starting number, or both, the previous version is recorded here as change, showing the previous first document ID in a series of documents.

3.3.5 Mapping Classification Codes with Material Groups

The topics in this list cover the concepts and procedures involved in mapping UNSPSC classifications in the catalog to material groups in the connected system so item requests can be processed correctly.

About Mapping Classification Codes with Material Groups [page 54]
Mapping the UNSPSC classification used for items in supplier catalogs to the material groups defined in the connected system enables the system to correctly process the line items in requests.

Maintaining Classification Codes [page 55]
Follow this procedure to maintain the classification codes for catalog items and map them to the corresponding material groups. This enables correct processing of purchase requests for material items.

3.3.5.1 About Mapping Classification Codes with Material Groups

Mapping the UNSPSC classification used for items in supplier catalogs to the material groups defined in the connected system enables the system to correctly process the line items in requests.

Classification codes are used to identify the items in a catalog. SAP Ariba Buying, base edition supports the UNSPSC (United Nations Standard Products and Services Code®) classification. For more information on UNSPSC, see www.unspsc.org ↗ .

> ⓘ Note
>
> Classification codes are supported for material items only.

Administrators maintain material items in the connected system based on the material group. Suppliers maintain items in the catalogs based on the UNSPSC classification. The difference between material group and UNSPSC classification results in a mismatch when identifying an item in the catalog with the item in the connected system. To identify the UNSPSC classification for an item in the catalog with the material group for the item in the connected system, administrators must maintain a mapping between them.

You must have the role `Procurement_Configuration_Admin` to define the mapping for the UNSPSC classification with the material group.

To map the UNSPSC for a catalog item, go to the *Manage Classification Code* page and download the template. Maintain the UNSPSC classification and map it to the material group accurately. You must also specify a default value for the UNSPSC classification with the material group.

SAP Ariba Buying, base edition uses the default material group associated to the general ledger account information available for your user profile when a mapping doesn't exist for the material group in the connected system.

The UNSPSC mapping file with the material group must be a comma-separated value (CSV) file and must include the following columns:

Column Name	Description
Classification Code	Eight-digit code for the UNSPSC classification
Material Group ID	Material group for the item

The mapping table on the *Manage Classification Codes* page displays the following information:

Column Name	Description
Classification Code	Eight-digit code for the UNSPSC classification
Material Group ID	Material group for the item
Changed On	Date on which the last change was made

> ⓘ Note
>
> Administrators must ensure that they enter the information for the UNSPSC classification and material groups accurately in the CSV file. Incorrect information causes errors when validating the mapping information in the connected system.

You can search for values only from the *Classification Code* or *Material Group ID* columns.

When you download the CSV mapping file for the first time, it contains the list of columns required for mapping the UNSPSC classification with the material group. Enter the values in each of the columns and upload the file. When you download the file later, the mapping file contains the values uploaded earlier.

When buyer administrators upload the mapping file again, the UNSPSC and material group information is overwritten with the values in the newly uploaded mapping file. The newly uploaded UNSPSC and material group mappings apply to the newly added items in the existing carts and the new purchase requests that buyers create. The newly uploaded mapping values don't apply to the existing requests that contain the line items. The existing requests continue to have the values that were previously uploaded for the UNSPSC and material group.

When the classification codes are incorrect or don't have a mapping for the material group in the connected system, you don't see an error while uploading the mapping file. In such cases, the material group used is the default material group associated with the general ledger account information available for your user profile.

When buyers submit the a purchase request, it's sent to the connected system. The connected system identifies and processes the line items in the request based on the mapping defined between the UNSPSC classification and the material group for the item. There could be a failure when the UNSPSC classification doesn't have a mapping for the material group in the connected system.

Managing Errors

While uploading the mapping file, the file could fail with errors for the following cases:

- Mapping file contains an invalid format or empty rows
- Contains missing columns or a mismatch in the required column names
- Identical values in more than one row in the mapping file
- Mapping file is not a CSV file
- File doesn't contain a default value for the classification code in the first row
- File contains unsafe content
- The classification code or material group field exceeds nine characters

If there are any errors while uploading the file, buyer administrators can download the mapping file, fix the errors, and upload the mapping file containing the UNSPSC and material group again.

3.3.5.2   Maintaining Classification Codes

Follow this procedure to maintain the classification codes for catalog items and map them to the corresponding material groups. This enables correct processing of purchase requests for material items.

Prerequisites

You must have the role `Procurement_Configuration_Admin` to view the tile, *Manage Classification Codes*.

Context

When you define a mapping for the material group and the classification code, the connected system identifies and processes the line items in the request based on the mapping defined between the UNSPSC classification and the material group for the item.

> ⓘ Note
>
> Buyers must ensure that they enter the information for the UNSPSC classification and material groups accurately. Incorrect information causes errors when validating the mapping information on the connected system. Ensure the file is in comma-separated value (CSV) format.

Procedure

1. Go to the *Configure Buying* app.
2. Choose the app *Manage Classification Codes*.
3. Do one of the following:
   * If you're a first-time user, click *Download* to download the template containing the required structure to maintain the classification codes. When you download the template for the first time, the table *Mappings for Classification Codes with Material Groups* is empty. When the table contains values, the file you download contains these values that were last uploaded.
   * If you're a subsequent user, you can download the previously uploaded mapping file and make the required mapping changes.
4. Enter the UNSPSC classification and map it to the material group accurately. Go to Row 1 and specify a default value for the UNSPSC classification with the material group. Use the asterisk (*) symbol to specify the default value.
5. Save the CSV file.
6. Click *Upload* to upload the template.
7. Choose the CSV file containing the UNSPSC classification mapped to the material group and click *OK*.
8. View the codes that you've uploaded.
9. Use the *Search* field to search for the classification code or material group by specifying the classification code or material group ID.

3.3.6 Managing Units of Measure

The topics in this list cover the concepts and procedures involved in mapping the units of measure used in supplier catalogs to the units of measure defined in the connected system.

About Managing Units of Measure [page 57]
> The units of measure used in catalogs can be different from the units of measure defined in the connected system. A mapping between sets of units of measure enables correct processing of unit of measure information in item requests.

Maintaining Units of Measure [page 59]

Follow this procedure to map the units of measure for catalog items to the units of measure defined in the connected system .

3.3.6.1 About Managing Units of Measure

The units of measure used in catalogs can be different from the units of measure defined in the connected system. A mapping between sets of units of measure enables correct processing of unit of measure information in item requests.

A catalog contains items from suppliers. Each item in the catalog has an association to the unit of measure. A unit of measure defines how the item is measured or packaged. For example, EA for each.

Suppliers maintain the units of measure in catalogs based on the industry standards. However, buyers define unique internal units of measure for items on the connected system. As a result, the units of measure in the catalogs from suppliers don't match the units of measure defined on the connected system. To process the units of measure correctly, buyers must maintain a mapping to match the units of measure in the catalog with the units of measure in the connected system.

You must have the role, `Procurement_Configuration_Admin` to define the mapping between the units of measure.

As an administrator, you can define the mapping for the units of measure in the template available in the *Manage Units of Measure* app. Download the template and add the units of measure. You must map the units of measure available in the catalog from the supplier with the units of measure maintained on the connected system.

When you define the mapping, ensure that you specify a default value for the unit of measure. The default unit of measure is used when a mapping for the unit of measure is invalid or doesn't exist on the connected system.

The template file containing the mappings for the units of measure must contain the following information:

Column Name	Description
UnitOfMeasureInCatalog	The unit of measure for the item in the supplier's catalog.
UnitOfMeasureInConnectedSystem	The unit of measure for the item in the the connected system.

The mapping table on the *Manage Units of Measure* page displays the following information:

Column Name	Description
Unit of Measure in Catalog	The unit of measure for the item in the supplier's catalog.
Unit of Measure in Connected System	The unit of measure for the item in the connected system.
Changed On	The date on which the last change was made.

> ⓘ Note
>
> Buyer administrators must ensure that they map the units of measure available in the supplier's catalog with the unit of measure for the items in the connected system accurately. Incorrect information causes errors when mapping the right unit of measure for the item on the connected system.

You can search for values only from the *Unit of Measure in Catalog* or *Unit of Measure in Connected System* columns.

As an administrator, when you download the mapping file for the first time, the mapping file contains the list of columns required for mapping the units of measure in the catalog and the connected system. Enter the values in each of the columns accurately and then upload the file. You must upload the mapping file in a comma-separated value (CSV) file. When you download the file later, the mapping file contains the units of measure that you had uploaded earlier.

When you upload the mapping file later, the existing mapping for the units of measure are overwritten with the values from the newly uploaded mapping file. The newly uploaded mappings for the units of measure apply to the newly added items in the existing carts and the new purchase requests that buyers create. The newly uploaded mappings for the units of measure don't apply to the existing requests containing the line items; the existing requests continue to have the units of measure that were previously uploaded for the supplier.

When buyers add an item to the cart or try to submit the request, the item displays the default unit of measure.

> ⓘ Note
>
> - The mapping file must be in CSV format.
> - We recommend that you download the existing mapping file before you upload a new mapping file containing the units of measure.
> - Translations of the text descriptions for units of measure are supported. When you specify a language that isn't yet supported, the text is displayed in English.

Managing Errors

When you upload the mapping files, the file could fail with errors in the following cases:

- Mapping file contains an invalid format or empty rows
- Contains missing columns or a mismatch in the required column names
- Identical values in more than one row in the mapping file
- Mapping file isn't a CSV file
- File doesn't contain a default value for the units of measure in the first row
- File contains unsafe content

When the units of measure are incorrect or no mapping exists, you don't see an error while uploading the mapping file. In such cases, the system uses the default unit of measure that you defined.

If there are any errors, buyers can download the mapping file, fix the errors, and upload the mapping file containing the units of measure for the supplier's catalog and the connected system again.

3.3.6.2 Maintaining Units of Measure

Follow this procedure to map the units of measure for catalog items to the units of measure defined in the connected system .

Prerequisites

You must have the role `Procurement_Configuration_Admin` to view the app, *Manage Units of Measure*.

Context

When you define a mapping for the units of measure in the catalog and the ones used in the connected system, SAP Ariba Buying, base edition processes the purchase request containing the units of measure for the line items successfully.

Administrators must ensure that they enter and map the units of measure available in both the catalog and SAP S/4HANA accurately.

Procedure

1. Go to the *Configure Buying* app.
2. Choose the app *Manage Units of Measure*.
3. Do one of the following:
   - If you're a first-time user, click *Download* to download the template containing the required structure to maintain the units of measure. When you download the template for the first time, the table *Mappings for Units of Measure* is empty. However, after you upload the file, the table displays the values from the file you've uploaded.
   - If you're a subsequent user, you can download the previously uploaded mapping file and make the required mapping changes.
4. Enter the units of measure available in the catalog and map it with the units of measure on SAP S/4HANA Cloud. Go to the first row and specify a default value for the units of measure. Use the asterisk (*) symbol to specify the default value.
5. Save the CSV file.
6. Click *Upload* to upload the template containing the mapping for the units of measure.
7. Choose the CSV file containing the units of measure and click *OK*.
8. View the units of measure that you've uploaded. Use the *Search* field to search for the units of measure.

3.3.7 Managing Supplier IDs

The topics in this list include the concepts and procedures involved in mapping the supplier IDs used in catalogs to the supplier IDs in your connected system.

To identify and match the supplier of an item with the correct supplier record in the connected system, administrators create a mapping file that maps the supplier ID in the catalog to the supplier ID in the connected system.

Follow this procedure to create a mapping file that maps supplier IDs in the catalog to supplier IDs in the connected system. The mapping file enables the items in purchase requests to be matched to the suppliers in your connected system.

3.3.7.1 About Managing Supplier IDs

To identify and match the supplier of an item with the correct supplier record in the connected system, administrators create a mapping file that maps the supplier ID in the catalog to the supplier ID in the connected system.

Procurement buyers can purchase items from catalogs managed or hosted by suppliers. The catalogs that suppliers provide contain information about the items and the ID for suppliers. Supplier IDs help in uniquely identifying the suppliers for items in supplier-managed catalogs and websites.

Buyers maintain unique supplier IDs for their suppliers in the connected system. As a result, the supplier IDs in the catalog differ from the supplier ID that is maintained in the connected system.

You must have the role `Procurement_Configuration_Admin` to define the mapping between the supplier IDs.

As an administrator, you can define the mapping between the supplier IDs in the template available on the *Manage Supplier IDs* app. Download the template and add the mapping for the supplier IDs. You must map the supplier ID available in the catalog with the supplier ID in the connected system.

The supplier information mapping file must contain the following information:

Column Name	Description
CatalogSupplierID	The supplier ID in the catalog.
ConnectedSystemSupplierID	The supplier ID in the connected system. For example, SAP S/4HANA Cloud.

The mapping table on the *Manage Supplier IDs* app displays the following information:

Column Name	Description
Supplier ID in Catalog	The supplier ID in the catalog.
Supplier ID in Connected System	The supplier ID in the back end connected system. For example, SAP S/4HANA Cloud.
Changed On	The date on which the last change was made.

> ⓘ Note
>
> Administrators must ensure that they map the supplier ID available in the catalog with the supplier ID in the connected system accurately. Incorrect information doesn't result in selecting the correct supplier.

You can search for values only from the *Supplier ID in Catalog* or *Supplier ID in Connected System* columns.

When you download the mapping file for the first time, the mapping file contains the list of columns required for mapping the supplier IDs available in the catalog with the supplier IDs in the connected system. Enter the values in each of the columns accurately and upload the file. You must upload the mapping file in a comma-separated value (CSV) file. When you download the file later, the mapping file contains the supplier information that you had uploaded earlier.

When you upload the mapping file again, the supplier information is overwritten with the values from the newly uploaded mapping file. The newly uploaded supplier ID mappings apply to the newly added items in the existing carts and the new purchase requests that buyers create. The newly uploaded supplier ID mappings don't apply to the existing requests containing the line items. The existing requests continue to have the supplier ID mapping values that were previously uploaded for the supplier.

When buyers search for items while shopping, the items display the supplier ID from the catalogs. However, when buyers create and submit a request, the line item details display the mapped supplier ID available in the connected system.

> ⓘ Note
>
> - The mapping file must be in CSV format.
> - SAP recommends that you download the existing mapping file, before you upload a new mapping file containing supplier IDs.

Managing Errors

The mapping file you upload might fail with errors for the following cases:

- Mapping file contains an invalid format or empty rows
- Contains missing columns or a mismatch in the required column names
- Identical values in more than one row in the mapping file
- Mapping file isn't a CSV file
- File contains unsafe content

When the supplier IDs are incorrect or don't have a mapping for the supplier in the connected system, you don't see an error while uploading the mapping file.

If there are any errors on uploading the mapping file, buyers can download the file, fix the errors, and upload the mapping file containing the supplier IDs of the supplier in the connected system and the catalog again.

3.3.7.2　Maintaining Supplier IDs

Follow this procedure to create a mapping file that maps supplier IDs in the catalog to supplier IDs in the connected system. The mapping file enables the items in purchase requests to be matched to the suppliers in your connected system.

Prerequisites

You must have the role `Procurement_Configuration_Admin` to view the tile *Manage Supplier IDs*.

Context

Supplier IDs help in uniquely identifying the supplier.

Administrators must ensure that they enter and map the supplier ID available in the catalog with the supplier ID in the connected system accurately. Incorrect information causes errors when validating the supplier information in the connected system.

Procedure

1. Go to the *Configure Buying* app.
2. Choose the app *Manage Supplier IDs*.
3. Do one of the following:
   - If you're a first-time user, click *Download* to download the template containing the required structure to maintain the supplier IDs. When you download the template for the first time, the table, *Mappings for Supplier IDs* is empty. When the table contains values, the file you download contains the values that were last uploaded.
   - If you're a subsequent user, you can download the previously uploaded mapping file and make the required mapping changes.
4. Enter the supplier ID available in the catalog and map it with the supplier ID on SAP S/4HANA Cloud.
5. Save the CSV file.
6. Click *Upload* to upload the template containing the mapping for the supplier IDs.
7. Choose the CSV file containing the supplier ID and click *OK*.
8. View the supplier ID that you've uploaded. Use the *Search* field to search for the supplier ID.

3.3.8 Approval Workflows

The topics in this list cover the concepts and procedures involved in configuring approval processes used to generate the approval workflows for purchase requests.

Approval Workflow Overview [page 63]
>   As an administrator, you can define and manage the approval process for submitted purchase requests.

SAP Responsibility Management Service [page 65]
>   The SAP Responsibility Management service enables you to use standard rules to define a business process for approval workflows. Use this application to view the standard rules and team functions provided for approval workflows.

Prerequisites for Configuring Approval Processes [page 66]
>   Before you can manage approval processes, make sure to address the prerequisites, such as destination setup and roles. Also be aware of which approval workflow functionality is supported and which functionality is not supported.

Steps to Configure Approval Processes [page 67]
>   Here's an overview of the steps involved in configuring approval processes.

Assigning Roles for Managing Approval Processes [page 68]
>   Follow this procedure to assign role collections with required roles to users who need to view and manage approval workflows.

Creating a Mail Destination [page 71]
>   Follow this procedure to configure the mail destination for sending and receiving email notifications for email-related tasks in approval workflows.

Creating the Destination for Identity Authentication Service [page 72]
>   Follow this procedure to create a destination in SAP Business Technology Platform (SAP BTP) for SAP Ariba Buying, base edition. SAP Ariba Buying requires this destination to connect to the identity directory of Identity Authentication service.

Viewing and Editing the Workflow Package [page 74]
>   Follow this procedure to view the default workflow package and change the existing configuration as needed for your approval process variants.

Defining Teams and Responsibilities [page 76]
>   Follow this procedure to create teams and assign the responsibility definitions for the team members responsible for approving line items in purchase requests.

3.3.8.1 Approval Workflow Overview

As an administrator, you can define and manage the approval process for submitted purchase requests.

When a buyer user submits a request, the approvers receive the request for review. Approvers review the line items and can approve or decline the request for the item in the *My Inbox - Buying* app.

When approvers finish approving the line items in the request, the person who created the request (the requester) receives an email notification. If any approvers reject the line item in the request, the requester receives an email immediately.

Buyers can view and monitor the approval workflow in the *Approvals* tab when they view the line items. For more information, see Viewing the Approvals and Status Flow for an Item in a Request.

The apps in the *Configuration of Workflow and Responsibility Management* section enable you to view and manage approval workflows:

- *Process Flexibility Cockpit*
- *Monitor Workflows*
- *Manage Responsibility Rules*
- *Manage Teams and Responsibilities*

Workflow Package and Process Variants

Use the *Process Flexibility Cockpit* app to view the active approval workflow package and to make changes to the process configuration. The approval workflow package contains process templates, process variants, and other configurations required for defining approval processes.

Process variants are variations of the approval process and are based on the approval process template. By default, the approval workflow package contains a process variant for automatic approval of requests, as described in the following table:

Process Variant	Description
Automatic Approval Variant	Approves the process step automatically in the workflow. This process variant is already available for you in the package. You can use this process variant to automatically approve all line items in the workflow. This process variant doesn't have a start condition.

The automatic approval variant contains just one step, as described in the following table.

Process Step	Defines Conditions For
Automatic_Approval	Approving the line items in the request automatically.

You can create additional process variants that add certain approvers based on your business needs. Each approval process variant contains one or more approval steps. You can create as many approval process variants as you need.

For more information about process variants, see Viewing and Editing the Workflow Package [page 74] and Configure a Process Variant.

You configure the standard rules and team functions for process variants in the *Manage Teams and Responsibilities* app. For more information, see SAP Responsibility Management Service [page 65].

Monitoring Approval Workflow Instances

Use the *Monitor Workflows* app to monitor the approval workflows that are generated by an approval process. The log displays the entire step-by-step process of the workflow.

3.3.8.2 SAP Responsibility Management Service

The SAP Responsibility Management service enables you to use standard rules to define a business process for approval workflows. Use this application to view the standard rules and team functions provided for approval workflows.

This service enables you to:

- View and use the configuration that's already available for approval workflows.
- Create team members for approving the line items in the request.
- Add or remove team members from a team.
- Assign team functions to approve a step in the newly created variant for the approval process.
- Audit the data that SAP Responsibility Management Service uses in SAP Ariba Buying.

Using the *Manage Responsibility Rules* app, you can view the standard rules for the approval process. The following standard rules are available:

- *User Manager Rule (UMRULE)*: You can assign this rule when the user needs the manager's approval to complete the step.
- *Cost Center Owner Rule (CCRULE)*: You can assign this rule when the user needs the cost center's approval to complete the step.

Use the *Manage Teams and Responsibilities* app to create teams and assign team members to be responsible for approving line items in requests. You can assign the team function to the team member for the approval process variant.

Ensure that you create a team based on the company code, plant, purchasing group, or purchasing organization. You can use the team type *Operational Purchasing Team* (OPPURCH) that's already available for you.

You can also assign one or more functions to the team members. SAP Ariba Buying requires the following team functions, which are available for the team type *Operational Purchasing Team* (OPPURCH):

- *Purchasing Manager* (PUR_MANAG)
- *Operational Purchaser* (OP_PURCH)
- *Workflow Administrator* (WF_ADMIN)

You can also create new team functions and assign team members.

For more information about the apps *Manage Responsibility Rules* and *Manage Teams and Responsibilities*, see SAP Responsibility Management service.

Related Information

3.3.8.3 Prerequisites for Configuring Approval Processes

Before you can manage approval processes, make sure to address the prerequisites, such as destination setup and roles. Also be aware of which approval workflow functionality is supported and which functionality is not supported.

Prerequisites

You require the following to configure, view, and process approval workflows:

- Configure the destination *Identity_Authentication_Connectivity_IDS* to connect to the identity directory of the Identity Authentication service. This is required for connecting to SAP Responsibility Management service for the standard rules and team functions. For more information, see Creating the Destination for Identity Authentication Service [page 27].
- Ensure that you have the role `Procurement_Configuration_Admin` or the role collection `Procurement Configuration Admin`. This role allows you to view the SAP Workflow Management apps on the *Configuration* page.
  You also need specific roles and role collections to use the required functionalities in SAP Workflow Management and SAP Build Process Automation.
  To know the required roles for users, see Assigning Roles for Managing Approval Processes [page 68].
- Ensure that you also have the necessary roles for SAP Responsibility Management service. For more information, see User Management in SAP Responsibility Management service.
- Configure the email notifications for approval workflows. Buyers receive notifications when the request has been approved or rejected. Approvers also receive an email when items have been assigned to them for approval. For more information, see Creating a Mail Destination [page 26].
- The following standard rules from SAP Responsibility Management service also have prerequisites:
  - Rule *USERMANAGERRULE*: Ensure that you maintain the manager information on the connected system for the user creating the request. To maintain the manager information, import the employee in the app *Import Employees*. For more information, see Import Employees.
  - Rule *COSTCENTERRULE*: To use this rule, you must maintain the cost center owner's information on the connected system. To maintain the cost center owner's information, go to the app *Manage Cost Centers*. For more information, see Manage Cost Centers.

Supported Approval Workflow Functionality

- Approval workflows are available at the line item level only.
- As an approver, you can approve or reject items in the request containing only indirect material items. Line items with direct materials are not supported.
- You can assign multiple approvers to a series of subsequent process steps. You can't add multiple approvers in a parallel set of steps. Therefore, when you assign multiple approvers in an approval process variant, ensure that you use a series set of steps.
- You can view content in SAP Ariba Buying apps only if you have the required roles and authorization. In some cases, when you open an app, you might see an error or a blank page. This situation occurs when you

don't have the required roles or authorization to view apps. Contact your administrator to ensure that you have the required authorizations to work with the apps you need.

- When you view the apps that have been integrated with SAP Ariba Buying in a language other than English, SAP Ariba Buying displays the text only in English. SAP Ariba Buying doesn't support the translation of the field names and text descriptions in the supported languages for the integrated SAP Workflow Management app.

For additional technical details about approval workflows in apps on SAP BTP, Cloud Foundry environment, see Conventions, Restrictions, and Limits .

3.3.8.4 Steps to Configure Approval Processes

Here's an overview of the steps involved in configuring approval processes.

1. Ensure that you have the role `Procurement_Configuration_Admin` or the role collection `Procurement Configuration Admin`. This role allows you to view the SAP Workflow Management apps on the *Configuration* page.
   You also need specific roles and role collections to use the required functionalities in SAP Workflow Management and SAP Build Process Automation.
   To know the required roles for users, see Assigning Roles for Managing Approval Processes [page 68].
2. Use the apps for SAP Responsibility Management service in the section *Configuration of Workflow and Responsibility Management* on the *Configuration* page to configure the standard rules and add team members. You require this service only if you want to use the preconfigured, standard rules and team functions.
   The *Automatic Approval Variant* is already available for you.
   To use SAP Responsibility Management service, ensure that you have the necessary roles. For more information, see User Management in SAP Responsibility Management service.
3. Configure the destination `Identity_Authentication_Connectivity_IDS` to connect to the identity directory of the Identity Authentication service. This destination is required for connecting to SAP Responsibility Management service for the standard rules and team functions. For more information, see Creating the Destination for Identity Authentication Service [page 27].
4. Configure the email notifications for approval workflows. Buyers receive notifications when the request has been approved or rejected. You must configure the mail destination for approval workflows. If you don't configure the mail destination, you can encounter errors during approvals. For more information, see Creating a Mail Destination [page 26].
5. Go to the *Configure Buying* app.
6. Configure the standard rules and team functions for the variants. You can view the apps for SAP Responsibility Management service in the section *Configuration of Workflow and Responsibility Management*:
   - View the standard rules already available for you in the *Manage Responsibility Rules* app.
   - You can view the default standard team category in the *Manage Teams Configurations* app.

     > ⓘ Note
     >
     > SAP Ariba Buying doesn't support the filtering and sorting functionality in the *My Inbox* app and SAP Responsibility Management service.

   - Create a team and assign team members who must approve the workflows in the app *Manage Teams and Responsibilities*.

Choose from the available responsibility definition and associate it with the corresponding company code. If you don't specify the company code, SAP Ariba Buying considers all the available company codes and related values for the team member. When you assign the company code, ensure that you assign the plants, purchasing group, and purchasing organization related to the company code.

> ⓘ Note
>
> - When you specify the company code, plants, purchasing group, and purchasing organization, the approval workflow for the line item is processed based on these values. The values that you specify for the company code, plants, purchasing group, and purchasing organization in the responsibility definition must match the values for the company code, plant, purchasing group, and purchasing organization for the line item. If there's a mismatch between the company code, plant, purchasing group, and purchasing organization, the approval workflow fails.
> - Although SAP Responsibility Management service allows you to create new functions or rules, ensure that you don't add, edit, or delete the existing values for the standard rules, team types, or team functions already available for you.

- Specify the material group for the company code.

  For more information, see SAP Responsibility Management Service [page 65].

7. Go to the app *Process Flexibility Cockpit* and view the details for the entire workflow package containing the process variants.
   In the app *Process Flexibility Cockpit*, click *Process Variants* to view the process variants for approving line items in the workflow. For more information on how to configure approval process variants, see Viewing and Editing the Workflow Package [page 74].

3.3.8.5 Assigning Roles for Managing Approval Processes

Follow this procedure to assign role collections with required roles to users who need to view and manage approval workflows.

Prerequisites

In order to assign role collections to users:

- You must be a BTP subaccount administrator. For information, see Assign Users to Role Collections in the SAP BTP Cockpit [page 7].
- You must have the role `Procurement_Configuration_Admin`.

Context

SAP Ariba Buying provides you few standard role collections. However, you must create a new role collection and add the roles to approve line items in a request. You also need a separate new role collection for the roles required for SAP Workflow Management.

You also assign the role templates for SAP Responsibility Management service to manage teams and team members.

Procedure

1. Open the SAP BTP cockpit.
2. Choose your subaccount available in your global account.
3. Assign the appropriate role collections to users.

   Following are the role collections to assign, depending on whether the users are administrators or end users (approvers).

   Administrator users need the following role collections:

Role Collection	Contains Role	Description
`Procurement Configuration Admin`	`Procurement_Configuration_Admin`	Allows you to configure the settings and functionalities in SAP Ariba Buying. You also require this role for configuring approval workflows.
Create a new role collection for workflows	• `WorkflowAdmin` • `WorkflowContextViewer` • `AdvancedUser` • `RuleAuthor` • `WMBusinessExpert` • `WorkflowBusinessExpert`	Gives you the permission to do the following: • View and manage the workflow definition in the *Monitor Workflows - Workflow Instances* app. • Monitor workflow instances and view the workflow context in the *Monitor Workflows - Workflow Instances* app. • View and configure approval process variants in the *Process Flexibility Cockpit* app. • Create, edit, and manage business rules. • Start workflow instances using the *Monitor Workflows - Workflow Instances* app.
`AdministratorCustomerDataManagementResponsibilityManagement`	`AdministratorCustomerDataManagementResponsibilityManagement`	Gives the user permission to download customer data.

Role Collection	Contains Role	Description
AdministratorResponsibilityM anagement	AdministratorResponsibilityM anagement	Gives the user permission to create responsibility rules and view standard responsibility contexts.
AuditSpecialistResponsibilit yManagement	AuditSpecialistResponsibilit yManagement	Gives the user permission to view and delete agent determination logs.
BusinessConfigurationExpertR esponsibilityManagement	BusinessConfigurationExpertR esponsibilityManagement	Gives the user permission to manage team categories and team types.
BusinessProcessSpecialistRes ponsibilityManagement	BusinessProcessSpecialistRes ponsibilityManagement	Gives the user the permission to manage teams, team members and their functions, and responsibility definitions.

Approvers need the following role collections:

Role Collection	Contains Role	Description
Procurement Approver	Procurement_Approver	Gives the user the permission to approve items in a request. This role also allows you to add comments for line items in a request from the *My Inbox* app. To approve items, you also additionally need the role, WorkflowParticipant in SAP BTP.
Create a new role collection for workflows	WorkflowParticipant	• Gives you the permission to view and manage workflow instances and logs. • Gives the user the permission to approve the line items in the workflow.

To assign role collections to your users, see Assign Role Collections.

4. Save the changes.

3.3.8.6 Creating a Mail Destination

Follow this procedure to configure the mail destination for sending and receiving email notifications for email-related tasks in approval workflows.

Context

Set up the mail destination with the SMTP server information in the provider tenant.

> → Remember
>
> You must configure the mail destination for approval workflows. If you don't configure the mail destination, you can encounter errors during approvals.

Procedure

1. Open the SAP BTP cockpit.
2. Choose your subaccount available in your global account.
3. Choose *Connectivity* and then click *Destinations*.
4. Click *New Destination*.
5. Enter `bpmworkflowruntime_mail` as the name of the mail destination.
6. Choose `MAIL` in the *Type* field.
7. (Optional) Enter a description for the destination.
8. Choose *Internet* in the *Proxy Type* field to access an external mail server.
9. Choose the authentication based on your requirement and specify its related values.
10. To specify additional properties, click *New Property* and specify the property and the required value.
    - Specify the following properties:

Property	Value
mail.transport.protocol	**smtp**
mail.smtp.auth	**true**
mail.smtp.starttls.required	**true**
mail.smtp.host	Host name of your mail server

Property	Value
`mail.smtp.port`	Port of your mail server that monitors the connections. Enter **587**. In some cases, you may need to enter **465**.
`mail.smtp.from`	Mail address of the "From" address for mails sent by the workflow capability. For example, **cpworkflow@example.com**. Enter the email address of an existing mailbox to receive the replies to emails from the workflow capability.
`mail.smtp.ssl.checkserve ridentity`	(Optional) **true** or **false**. The default value is **true**.
`mail.smtp.ssl.trust`	***** or a space-separated list of acceptable host names. If you don't provide a value, trust is based on the certificate provided by the server, which must be part of the SAP JVM default truststore. For more information, see Determine the Trusted CAs of SAP JVM Truststore.
`mail.bpm.send.disabled`	• **true**: When you set the value to **true**, emails are not sent from the mail server. You can set this value to block emails from the server when you're working on the workflow temporarily. • **false**

For more information about the properties, see Configure the Workflow Capability Mail Destination.

11. Save the changes.

3.3.8.7 Creating the Destination for Identity Authentication Service

Follow this procedure to create a destination in SAP Business Technology Platform (SAP BTP) for SAP Ariba Buying, base edition. SAP Ariba Buying requires this destination to connect to the identity directory of Identity Authentication service.

Prerequisites

• Ensure that you maintain the trust store and the key store certificate in the **Destinations** editor of SAP Business Technology Platform (SAP BTP).

Context

Configure this destination for SAP Ariba Buying, base edition to set up users from Identity Authentication service. You also need this destination for the SAP Responsibility Management service to use the standard rules and team functions. For more information, see Identity Authentication Service.

Procedure

1. Go to the SAP Business Technology Platform (SAP BTP) and navigate to your subaccount.
2. In the navigation pane, click ▶ *Connectivity* ❯ *Destination* ◢.
3. Click *New Destination*.
4. Enter the following information:

Parameter	Value
Name	**Identity_Authentication_Connectivity_I DS**
Type	**HTTP**
Description	Enter a description.
URL	Enter the URL containing the tenant ID of your Identify Authentication service. The URL displays in the following format: `https://<tenant ID>.accounts.ondemand.com/scim/Users` ⓘ Note Ensure that you add the URL of the Custom Identity Provider for Applications. For more information, see Establish Trust and Federation Between SAP Authorization and Trust Management Service and SAP Cloud Identity Services
Proxy Type	**Internet**
Authentication	**BasicAuthentication**
User	Add a new technical user as an administrator in the administration console for Identity Authentication. To add a new tenant administrator, you must have the Manage Tenant Configuration role. For more information, see the section Add System as Administrator.
Password	Specify the password of the administrator user in the Identity Authentication service.

5. Choose *Save*.

3.3.8.8   Viewing and Editing the Workflow Package

Follow this procedure to view the default workflow package and change the existing configuration as needed for your approval process variants.

Prerequisites

Ensure that you have the necessary roles and settings. For more information, see Prerequisites for Configuring Approval Processes [page 66].

Context

The *Process Flexibility Cockpit* app enables you to configure approval processes.

> ⓘ Note
>
> When you create a new process variant, you can only add the steps that are available in the package. Don't delete the existing process variants.

Procedure

1. Go to the *Configure Buying* app.
2. Go to the section *Configuration of Workflow and Responsibility Management* and choose *Process Flexibility Cockpit*.
3. Do one of the following:
   - View the available process variants for approving line items in the workflow.
   - Edit the values for the process variant.

     > ⓘ Note
     >
     > Ensure that you don't edit or delete the existing packages. SAP recommends that you don't create new packages either.

4. Create a new process variant for the default workflow package.

   If you don't create any process variants, the *Automatic Approval Variant* applies for all approval workflows. All line items in the request get approved automatically.

   For details on creating process variants in the *Process Flexibility Cockpit* app, see Configure a Process Variant.

5. For each newly created process variant, first delete the step *Automatic Approval*. Then choose the step *Approval Task*.

You can add one or more approval tasks for the variant. You can drag and drop the steps for the variant. You can choose to rename the step for the variant.

6. Specify the start condition for each of the variants.

The start condition triggers the variant to be used based on the conditions and the order that you configure them.

You can specify a start condition for the entire workflow or for each step in the workflow. When you specify the start condition at a step level, ensure that the condition doesn't override the start condition specified for the approval workflow.

You can add one or more conditions or for the start condition. When you add more than one condition, the line item for approval must satisfy both the conditions.

You can also add alternate conditions. When you add an alternate condition, the line item for approval must satisfy only one of the conditions.

> ⓘ Note
>
> - When you create a new process variant, you can only add the steps that are available in the package.
> - You must define the order for the variants in the *Process Variants* list view. The order in the list determines how the system chooses the variant for an approval workflow.
> - If you specify the step condition, ensure that the start and step conditions don't conflict with each other.
> - When you choose the start condition *Request Line Item.Total Net Amount*, the currency for the item displays based on the supplier's currency. SAP recommends that you use the start condition *Request Line Item.Variant Determination Amount* instead of the condition *Request Line Item. Total Net Account.*
> - When you choose the start condition *Request Line Item. Variant Determination Amount*, the default currency used to process the line item is EUR. However, the buyer can view the currency for the item in the user's currency.
>   Before you choose the start condition *Request Line Item.Variant Determination Amount*, you must maintain the mapping of the supplier's currency for the item to the EUR currency associated with this start condition.

7. You can add any number of steps to the process variant. After you complete defining the start conditions, go to the *Details* tab and choose any of the following rules or team functions for every step that you've added to the variant:

Rules

- *USERMANAGERRULE*
- *COSTCENTERRULE*

> ⓘ Note
>
> Before you choose to specify the following standard rules from SAP Responsibility Management service, ensure that you do the following:
>
> - Rule *USERMANAGERRULE*: Ensure that you maintain the manager information on the connected system for the user creating the request. To maintain the manager information, import the employee information using the app *Import Employees*.

- Rule *COSTCENTERRULE*: To use this rule, you must maintain the cost center owner's information on the connected system. To maintain the cost center owner's information, go to the app *Manage Cost Centers*.

  Team Functions

  - *Purchasing Manager* (`PUR_MANAG`)
  - *Operational Purchaser* (`OP_PURCH`)
  - *Workflow Administrator* (`WF_ADMIN`)

- When you search for team functions, ensure that you search using the value PUR_MANAG, OP_PURCH, or WF_ADMIN.

8. Ensure that you define the order for the variants in the *Process variants* list. The order in the list determines how the system chooses the variant for processing the approval workflow.

   When the start condition of the variant matches the values for the line item, the approval workflow is triggered. When none of the conditions match the line item, the approval workflow isn't activated.

   > ⓘ Note
   >
   > Ensure that you define the condition for the variant accurately. Invalid conditions don't trigger the validation for the workflow.

9. Save the variant. When you save the variant, the variant is save as a draft version.
10. Activate the variant.

3.3.8.9 Defining Teams and Responsibilities

Follow this procedure to create teams and assign the responsibility definitions for the team members responsible for approving line items in purchase requests.

Prerequisites

- Ensure that the team members you want to assign are already available in the Identity Authentication service.
- You need the following if you use the following standard rules from the SAP Responsibility Management service:
  - Rule *USERMANAGERRULE*: Ensure that you maintain the manager information on the connected system for the user creating the request. To maintain the manager information, import the employee in the app *Import Employees*. For more information, see Import Employees.
  - Rule *COSTCENTERRULE*: To use this rule, you must maintain the cost center owner's information on the connected system. To maintain the cost center owner's information, go to the app *Manage Cost Centers*. For more information, see Manage Cost Centers.

Procedure

1. Go to the *Configure Buying* app.
2. Choose the app *Manage Teams and Responsibilities*.
3. Choose *Create*.
4. Enter a name for the team in the *Global ID* field.
5. Choose OPPURCH in the *Type* field. The values in the fields *Category* and *Source* are already autopopulated for you.
6. (Optional) Choose to set the status to Enabled or Disabled. You can also enable the team after you save the changes.
7. Specify one or more company codes, plants, purchasing groups, and purchasing organizations for the responsibility definition. When you assign the company code, ensure that you assign the plants, purchasing groups, and purchasing organizations related to the company code.
8. Choose the material group.
9. Specify the team members. Choose *Create* to add the user who is the owner of the team and manages the team members and functions.
10. Add one or more users as team members.
11. Choose *OK*.
12. Assign one of the team functions for each of the team members:

    - *Purchasing Manager* (PUR_MANAG)
    - *Operational Purchaser* (OP_PURCH)
    - *Workflow Administrator* (WF_ADMIN)

13. Save the changes. After you save the changes, ensure that the newly created team is enabled.

3.3.9 Manage Shopping Sites

Administrators create and manage shopping sites. Shopping sites provide access to items from various catalog content providers that users can search for and purchase.

Depending on the shopping site type, a shopping site provides access to one or more catalog content providers.

You can create shopping sites to connect to the following types of catalog content providers:

- *Ariba* - Internal catalogs from SAP Ariba Catalog, from suppliers with whom you've prenegotiated contracts
- *Seller* - Public catalogs from suppliers on SAP Business Network
- **Amazon XX** - Content on Amazon Business
  XX indicates the country/region code of an Amazon Business marketplace. For example, *Amazon US*, *Amazon DE*, and so on.
- *Supplier Stores* - Content from supplier sites
  When you set up a *Supplier Stores* shopping site, you can add connections to multiple supplier sites that allow users to search for items and add them to their SAP Ariba Buying shopping cart.

> ⓘ **Note**
>
> You must have at least one shopping site configured and activated in order to use the Intelligent Features in SAP Ariba Buying for personalized recommendations.

> ⚠ **Caution**
>
> Please note that setting up a connection to a supplier's website excludes EU access compliance.

Configuring Shopping Sites of Type Ariba or Seller

Configuring a shopping site of type *Ariba* or *Seller* for accessing internal or public catalogs involves the following high-level steps:

1. For access to internal catalogs (*Ariba* shopping sites), make sure the suppliers are set up as trading partners, and publish the necessary catalogs.
2. Get an SAP Ariba APIs administrator account on the SAP Ariba developer portal.
   Your organization's SAP Ariba administrator can request this account at the SAP Ariba developer portal: https://developer.ariba.com/api☁. For more information, see Using SAP Ariba APIs.
3. Create an application on the SAP Ariba developer portal and request access to the following APIs for your application:
   * *Internal Catalogs Shop API* - to create a shopping site of type *Ariba*. See Internal Catalogs Shop API.
   * *Public Catalogs Shop API* - to create a shopping site of type *Seller*. See Public Catalogs Shop API.

   > ⓘ **Note**
   >
   > Contact your SAP Ariba representative to request access to these APIs on the SAP Ariba developer portal.

4. In the SAP BTP cockpit, for your subaccount, create and set up the destinations to connect to the shopping sites.
   For more information, see:
   * Creating the Destination for a Shopping Site
   * Creating the Destination to Shop from a Supplier's Website
5. To consume the catalogs and enable shopping using the API, create and enable shopping sites.
   For more information, see Creating a Shopping Site.

Creating a Shopping Site to Connect to Amazon Business

Creating a shopping site to connect to Amazon Business involves the following high-level steps:

1. Register for and set up your account on Amazon Business.
   For assistance, connect with an Amazon Business customer advisor. Note that a separate Amazon Business account is needed for each Marketplace (US, CA, FR, UK, DE, ES, IT, JP.)

> ⓘ Note
>
> You must add the email addresses of all SAP Ariba Buying users that you want to be able to shop on Amazon Business in the members area of the Amazon Business account settings. For each user, the email address you add in Amazon Business must be the same as that used in SAP Ariba Buying.

2. In the SAP BTP cockpit, for your subaccount, create and set up the destinations to connect to the supplier's website.
   For more information, see Creating the Destination to Shop from a Supplier's WebsiteCreating the Destination to Shop from a Supplier's Website.

> ⓘ Note
>
> The call back URL must be whitelisted for your organization's Amazon Business account. Create a Service Now ticket to request the whitelisting, providing the tenant ID in the Service Now ticket.

3. Create and enable shopping sites.
   For more information, see Creating a Shopping Site.

   Creating a Shopping Site [page 79]
       You create one or more shopping sites from the *Manage Shopping Sites* app.

   Adding a Supplier Store [page 82]
       You can add a connection to a supplier site to allow users to search for items on that site and add them to their cart in SAP Ariba Buying.

3.3.9.1   Creating a Shopping Site

You create one or more shopping sites from the *Manage Shopping Sites* app.

Context

Create one or more shopping sites to provide access to catalog content from different catalog content providers to buyer users.

> ⚠ Caution
>
> Please note that setting up a connection to a supplier's website excludes EU access compliance.

Procedure

1. Go to the *Configure Buying* app.
2. Choose the *Manage Shopping Sites* app.

   The available shopping sites are displayed in a table.

3. To create a new shopping site, click *Create*.

4. In the *Type* field, enter or select the type of shopping site that you want to create.

   - Select *Ariba* if you want to create a shopping site that connects to internal catalogs in your SAP Ariba solution.
   - Select *Seller* if you want to create a shopping site that connects public catalogs from suppliers on the SAP Business Network.
   - Select the appropriate Amazon option if you want to create a shopping site that connects to an Amazon Business marketplace.
   - Select *Supplier Stores* if you want to create a shopping site that connects to supplier websites. When you select this option, you will need to add connections to supplier sites. For more information, see Adding a Supplier Store [page 82].

   Additional fields are displayed for you to fill in. The fields that are displayed depend on the type of shopping site.

5. Fill in the required details of the shopping site.

   - The following table describes the fields for a shopping site of type *Ariba*:

Field	Description
Ariba Network ID	The Ariba Network ID (ANID) of your organization.
	ANID is a number that uniquely identifies your company on SAP Business Network.

   - The following table describes the fields for a shopping site of type *Seller*:

Field	Description
Country/Region	The country/region associated with the public catalogs on SAP Business Network that you want to connect to.
Customer ID	The Customer ID of your application in the SAP Ariba developer portal

   - The following fields are displayed for an Amazon Business shopping site. Their values are auto-populated with values from the Amazon API:
     - *Marketplace*
     - *OAuth Domain*
     - *Service Host*
     - *Country/Region*
     - *Ariba Network ID*
     - *Supported Locales*
     - *Supported Countries/Regions*

     Ariba Network ID indicates the SAP Business Network ID (ANID) of the Amazon Business marketplace. The following table lists the ANIDs of the different marketplaces:

Marketplace	Ariba Network ID (ANID)
Amazon US	AN01011737571
Amazon CA	AN01466488898
Amazon DE	AN01053212622
Amazon ES	AN01437008981
Amazon FR	AN01397588490
Amazon GB	AN01053213381
Amazon IT	AN01437045355

> ⓘ Note
>
> When performing a test of the configuration settings using your SAP Business Network test account, ensure that you specify the test account ANID of the specific marketplace. The test account ANID is the production account ANID appended with a -T. For example, the test account ANID of the Amazon US marketplace is AN01011737571-T.

6. If you are creating a shopping site that connects to an Amazon Business marketplace:
   a. Click *Activate* to activate the Amazon site and sign in to your Amazon Business account.
   b. If required, add users to the Amazon Business account.
   c. Sent invitations to users to set up their individual Amazon Business user accounts.

   Users have to activate their individual accounts before they can start shopping.

7. For shopping sites of type *Supplier Stores*, to add a connection to a supplier store, select *Add Supplier Store*.

8. Select the *Enable Shopping Site* checkbox to enable the shopping site.

> ⓘ Note
>
> If a shopping site is not enabled, users will not be able to search for items from it. The shopping site will not be displayed as an option under the *Shopping Site* section in the *Filter By* panel of the search results page.

9. Click *Create* to create the shopping site.

10. To make a shopping site as the default shopping site, select the shopping site in the *Shopping Sites* table and click *Make Default*.

3.3.9.2 Adding a Supplier Store

You can add a connection to a supplier site to allow users to search for items on that site and add them to their cart in SAP Ariba Buying.

Prerequisites

You must create a shopping site of type *Supplier Stores* before you can add connections to individual supplier stores.

Context

> ⚠ Restriction
>
> Secure OCI communication and the store visibility keyword functionality are not available in the current release.

Procedure

1. Do one of the following:

   - If you are in the process of creating a shopping site of type *Supplier Stores* and you selected *Add Supplier Store*, go to step 2.
   - If you are adding a new supplier store connection to an existing *Supplier Stores* shopping site, go to the *Configure Buying* app, choose the *Manage Shopping Sites* app, select the *Supplier Stores* shopping site, and choose *Edit*. Then choose *Add Supplier Store*.

2. Enter the following details in the *General Information* area:

Field	Description
Store Name	Enter the name of the supplier site. For example, "acmeonlinestore.com".
Supplier Logo URL	Add a URL that points to the supplier logo so that the logo appears with the supplier store link in the SAP Ariba Buying search results.
Store Description	Enter a description for the store.

Field	Description
Supplier ID	Select a supplier ID.
	When a shopping cart is sent from SAP Ariba Buying to a user's ERP system, items that were added from a supplier store must contain a supplier ID, so that the ERP system knows which line item is connected with which supplier. Generally, the supplier ID is provided when an item is checked out from the supplier store and returned to SAP Ariba Buying. However, if the supplier ID is not provided at that time, the supplier ID that is selected here is added to the line item when the cart is sent to the user's ERP system.
Enable Supplier Store	If this field is selected, and if the *Supplier Stores* shopping site is also enabled, users will see a link to this store in their SAP Ariba Buying search results if the item they are searching for matches one of the search keywords entered in the *Store Visibility Keywords* field. Users can use this link to navigate to the supplier store, where they can search for items and check out in the supplier store to bring the items back to their SAP Ariba Buying shopping cart.

3. Enter the following details in the *Connection Settings* area:

Field	Description
Integration Channel	Select the integration channel that's supported by the supplier site.
	When you select an integration channel, you can enable the following options:
	• Enable the *View Item Details from Supplier Store in Cart* field to allow users to view product details for items after they have been added to the SAP Ariba Buying cart from the supplier store, if this is supported by the supplier.
	• Enable the *Validate Availability and Price from Supplier Store* field to check and update item availability and price automatically after items have been added to the SAP Ariba Buying cart from the supplier store, if this is supported by the supplier.

Field	Description
OCI Connection Setting	Select the OCI connection setting that's supported by the supplier store.
	With *Secure Communication*, all communication with the supplier store takes place from service to service.
	With *Non-Secure Communication*, all communication with the supplier store happens in the browser.
Secure Communication URL	When you select *Secure Communication* under *OCI Connection Setting*, you must add this endpoint, which is provided by the supplier, to initialize secure communication with the supplier store.
	Choose the data transfer method that's supported by the supplier store for this endpoint.
Store URL	The URL to the supplier store.
	Choose the data transfer method that's supported by the supplier store for this URL.
Authentication Type	Choose *Password Authentication*.
	When you select this, you must enter the following information:
	• *Username Key*: A unique identifier for the username value field. This is provided by the supplier.
	• *Username Value*: The username that is provided by the supplier.
	• *Password Key*: A unique identifier for the password value field. This is provided by the supplier.
	• *Password Value*: The password that is provided by the supplier.

4. Select *Create* in the *Connection Parameters* area, to add connection parameters.

    For example, you might want to add connection parameters for userid and password. For each parameter, enter the *Name*, *Type*, and *Value*, and select *Apply*.

5. Select *Create* at the bottom of the page to create the supplier store.

3.3.10 Managing Announcements

The topics in this list cover the procedures involved in managing announcements that are displayed to users when they're shopping.

Creating Announcements for the Create Purchase Request App [page 85]
> You can create announcements, which allows you to broadcast any business or technical news, such as scheduled maintenance, new available suppliers, or changes to your procurement policies.

Editing, Previewing, Unpublishing, and Deleting Announcements [page 87]

After creating an announcement, you can edit, preview, unpublish, or delete it.

You can add translations for announcements that you create to broadcast business or technical news to users of the *Create Purchase Request* app.

3.3.10.1 Creating Announcements for the *Create Purchase Request* App

You can create announcements, which allows you to broadcast any business or technical news, such as scheduled maintenance, new available suppliers, or changes to your procurement policies.

Prerequisites

You must be assigned the Administrator role (`Procurement_Configuration_Admin`).

Context

Announcements display in a rotating carousel in a wide tile on the *Create Purchase Request* app when users sign in. When users click *Learn More*, a pop-up shows more information. They display for a configured period or until you remove them.

Announcements can optionally have a hyperlink for additional information.

Procedure

1. Go to the *Configure Buying* app.
2. Open the *Manage Announcements* app.

   A table displays the existing announcements.
3. Choose *Create* to start a new announcement.

   A blank announcement form opens.
4. Fill in the details of the announcement.

   The following table describes the fields.

Field	Description
Title	A heading for the announcement

Field	Description
Message	The body of the announcement
	Two lines display in the carousel, and the entire message displays in the popup.
	Enter plain, unformatted text. The app removes return characters and extra spaces, and it doesn't interpret HTML elements.
Link for More Information	A hyperlink that's shown in the pop-up when a user chooses *Learn More*
	The link must contain an http:// or https:// prefix. When users click the link, the link destination opens in a new browser tab.
Contact Person	The name and email address of a contact for the announcement
Announcement Period • *Start Date* • *End Date*	The period of time to include the announcement in the announcement carousel.
	Use the date picker to specify when to start showing the announcement and when to remove it from the carousel.
	ⓘ Note Start Date and End Date are optional fields. If start and end dates are not added, the announcement continues to be displayed in its published state as long as it is not is not deleted or set to unpublished.

5. Choose *Create*.

Results

When you create an announcement, its status is *Published*.

When the announcement period starts, the announcement is included in the carousel.

Next Steps

You can edit, unpublish, and delete announcements.

For more information, see the following:

- Editing, Previewing, Unpublishing, and Deleting Announcements

- Adding Translations for Announcements

3.3.10.2 Editing, Previewing, Unpublishing, and Deleting Announcements

After creating an announcement, you can edit, preview, unpublish, or delete it.

Prerequisites

You must be assigned the Administrator role (`Procurement_Configuration_Admin`).

Procedure

1. Go to the *Configure Buying* app.
2. Open the *Manage Announcements* app.

   A table displays the existing announcements.

3. Do any of the following:

   - To edit an announcement, click on the announcement and choose *Edit*.
     While editing, select the *Saved Version* button at the top of the page to toggle between the saved and draft versions of the announcement.
     After editing the announcement, choose *Save* to make your changes immediately visible to users.
     Choose *Discard Draft* if you want to discard your changes and revert to the original saved version.

   - To preview an announcement, click on the announcement and choose *Preview*.
     The preview displays in the pop-up that users see when they click *Learn More* in the announcement carousel.

   - To unpublish an announcement, select the announcement radio button and choose *Unpublish*.
     Unpublished announcements are removed from the announcements carousel.
     To publish the announcement again, choose *Publish*.

   - To delete an announcement, select the announcement radio button and choose *Delete*.
     Deleted announcements are removed from the announcements carousel on the homepage and from the list of announcements in the *Manage Announcements* app.

3.3.10.3 Adding Translations for Announcements

You can add translations for announcements that you create to broadcast business or technical news to users of the *Create Purchase Request* app.

Prerequisites

You must be assigned the Administrator role (`Procurement_Configuration_Admin`).

Context

You can add translations for an announcement while creating the announcement, or you can edit the announcement later to add translations.

Translations are displayed on the shopping page of the *Create Purchase Request* app based on the user's locale settings. The system looks up the translation based on the locale value, and if it cannot find a corresponding translation it defaults to the original title and message text.

If translations are not included, announcements are displayed in the default language for the customer landscape.

Procedure

1. Go to the *Configure Buying* app.
2. Open the *Manage Announcements* app.

   A table displays the existing announcements.
3. Do one of the following:

   - If you are creating a new announcement, choose *Create*, enter the details for the source announcement, then select the *Translations* tab.
   - If you are adding a translation to an existing announcement, click on the announcement, choose *Edit*, then select the *Translations* tab.
4. Choose *Create* on the *Translations* tab.
5. Select the translation language from the *Language* menu.
6. Enter the translations for the title and message content.
7. Choose *Create*.

3.3.11 Managing Shopping Recommendations

The topics in this list cover the concepts and procedures involved in managing shopping recommendations for users.

Configuring Shopping Recommendations [page 89]
> Use the *Manage Recommendations* app to configure the *Recommendations* tiles on the main page of the *Create Purchase Request* app. Recommendations of relevant products, search results, and links to external sites, with useful information and meaningful images, help users find what they need faster.

Uploading Translations of Recommendations [page 93]
> Use the *Manage Recommendations* app to upload translations of the *Recommendations* tiles on the main page of the *Create Purchase Request* app.

3.3.11.1 Configuring Shopping Recommendations

Use the *Manage Recommendations* app to configure the *Recommendations* tiles on the main page of the *Create Purchase Request* app. Recommendations of relevant products, search results, and links to external sites, with useful information and meaningful images, help users find what they need faster.

Prerequisites

You must be assigned the Administrator role (`Procurement_Configuration_Admin`).

Context

You can configure different recommendations for each company code and plant.

You can configure the following types of recommendations:

- Search: A list of catalog search results defined by keywords that you configure. Search recommendation tiles contain the magnifying glass icon (🔍).
- Item: The details of a specific catalog item
- URL: A link to a web page relevant for users' shopping experience. URL recommendations tiles contain the ↗ icon.

The following figure shows an example of recommendations on the main page of the *Create Purchase Request* app. Tiles are displayed in a carousel that users can scroll through.
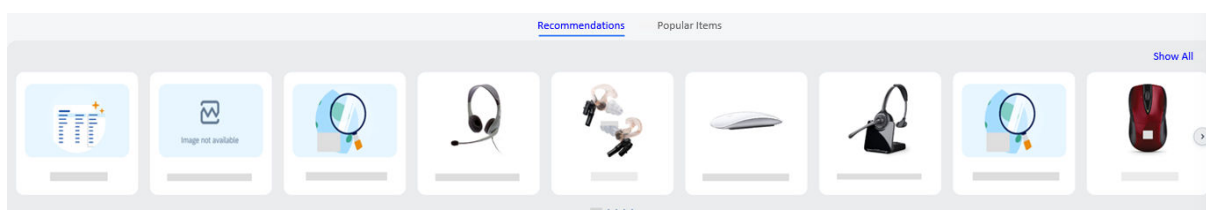
You configure recommendation tiles in a CSV file and then upload the file.

> ⚠ Caution
>
> When you upload a CSV file, the tiles configured in the CSV file completely replace any existing configuration. Whenever you want to make changes, we recommend that you download and modify the CSV file.

Procedure

1. Go to the *Configure Buying* app.

2. Open the *Manage Recommendations* app.

3. Choose the XLS icon (⬇XLS ⌄) and choose *Download*.

   A CSV file with the current tile configuration is downloaded.

4. Modify the CSV file as desired.

   The following table describes the columns in the CSV file.

CSV Column Name	Column Name in Configuration UI	Description	Value Type and Format
ACTIVE	Active	Determines whether the tile is displayed or hidden.	Value values: TRUE, FALSE
COMPANYCODE	Company Code	Company code for which the tile is applicable Visibility settings are not defined by company code and plant. This is an optional field.	String
DESCRIPTION	Description	Description displayed below the tile title	String
DISABLESEARCH	Prevent Search	This field is not currently in use.	

CSV Column Name	Column Name in Configuration UI	Description	Value Type and Format
ITEMID	Catalog Item ID	For tiles that open a specific item, this specifies the unique ID of the item in the catalog. This is the "extProductId" for the item in the catalog. As items can come from one of three sources (internal catalogs, public catalogs, or Amazon Business), the shop ID must also be provided along with the catalog item ID. The shop ID must be listed first, followed by a semi-colon and the catalog item ID. This is an optional field.	String Example: 1fed96d9-0abc-449d-8970-44cdfcc9eef8;AN33330000 0061|CCSL0001||en|US In this example, "1fed96d9-0abc-449d-8970 -44cdfcc9eef8" is the shop ID and "AN33300000061| CCSL0001||en|US" is the catalog item ID.
KEYWORDS	Keywords	For tiles that run a catalog search, specifies the keywords used in the search.	String Separate multiple keywords with a space. For example: **earphone headset**. In this instance the system searches for 'earphone headset', 'earphone' and 'headset'. An asterisk (*) indicates all results.
MATERIALGROUP	Material Group	The material group of the item in your connected system. This is an optional field.	String
PLANT	Plant	Plant for which the tile is applicable. This is an optional field.	String.

CSV Column Name	Column Name in Configuration UI	Description	Value Type and Format
RANK	Rank	Determines where this tile appears relative to other tiles, but only if all tiles have relative values. A rank of 1 means the tile is the first tile in the *Recommended for You* carousel. This is an optional field.	Integer.
TARGETURL	Target URL	For tiles that go to a specific URL, specifies the URL	Full URL, as in `https://aaaa.bbbb.cccc`
TILEID	Tile and ID	A name and a unique identifier for the tile. If this field is blank the entries will be overwritten.	String
TILEIMAGEURL	Image	A public URL starting with HTTPS/HTTP that points to the image file. This must not be a local file system URL.	Full URL, as in `https://aaaa.bbbb.cccc`
TITLE	Title and ID	Title displayed on the tile	String
TYPE	Search Type	Specifies the type of query that runs when a user chooses the tile.	Valid values: • `CatalogItem` opens the catalog item details for the specified catalog item ID • `CatalogSearch` runs a catalog search based on the specified keywords and displays the search results • `TargetAction` opens the specified URL in a new browser tab
PUNCHOUTLEVEL	Catalog Search Level	The level at which the user will enter a supplier site. This can contain values of 1 or 2, where level 1 takes the user to a search page on the supplier site, and level 2 takes the user directly to an item details page on the supplier site.	Integer

CSV Column Name	Column Name in Configuration UI	Description	Value Type and Format
SHOPID	Shop ID	The ID number for the supplier site.	String
SUPPLIERANID	Supplier Ariba Network ID	The Ariba Network ID (ANID) of the supplier. **ANID** is a number that uniquely identifies the supplier on SAP Business Network.	String
VENDORID	Vendor ID	The supplier's vendor ID.	String

> ⓘ Note
>
> The maximum file size is 1MB.

5. In the the *Manage Recommendations* app, upload the CSV file.
6. Refresh the page to see the results of the upload.

   Users who open the *Create Purchase Request* app can view the new tiles as soon as the upload is complete.

   > ⓘ Note
   >
   > Tiles display default images until you upload custom images. The default image differs based on tile type.

3.3.11.2 Uploading Translations of Recommendations

Use the *Manage Recommendations* app to upload translations of the *Recommendations* tiles on the main page of the *Create Purchase Request* app.

Prerequisites

You must be assigned the Administrator role (`Procurement_Configuration_Admin`).

The tiles you're translating have been configured and uploaded in the *Manage Recommendations* app.

You've downloaded the main recommendations CSV file to get the source content for translation. For more information, see Configuring Shopping Recommendations.

Procedure

1. Go to the *Configure Buying* app.

2. Open the *Manage Recommendations* app.

3. Choose ▌ *Translations* ❯ *Download* ❱.

   A CSV file with the current tile translations is downloaded.

4. Modify the CSV file as desired.

   The following table describes the columns in the CSV file.

CSV Column Name	Column Name in Configuration UI	Description	Value Type and Format
DESCRIPTION	Description	Translation of the tile description	String
KEYWORDS	Keywords	For tiles that run a catalog search, this specifies the keywords used in the search.	String
LOCALE	Locale	The language of the translation, expressed as a 2-letter ISO code.	String Example: DE
TILEID	Tile ID	Unique identifier for the tile Must match an ID in the main `recommended_category.csv` file	String
TITLE	Title	Translation of the tile title	String

> ⓘ Note
>
> The maximum file size is 1MB.

5. In the *Manage Recommendations* app, Choose ▌ *Translations* ❯ *Upload* ❱ to upload the CSV file.

> ⓘ Note
>
> If you are uploading a translation file in the German language, the file must be an UTF-8 encoded CSV file. To encode the file in UTF-8 format you can use the Numbers app on Mac OS devices or the Notepad app on Windows devices and save the file in UTF-8 format. Note that the downloaded translation file is not UTF-8 encoded, so after making changes in that file you must save it as UTF-8 format before uploading it.

6. Refresh the page to see the results of the upload.

   Users who open the SAP Ariba Buying, base edition app can view the new translations as soon as the upload is complete.

3.3.12 Enable Data Provider for Carbon Footprint

Use this app to connect to a third-party data provider of carbon footprint information for the products users view when shopping.

Administrators can enable a third-party data provider to retrieve carbon footprint information for products. Once the data provider is enabled, carbon footprint information is displayed on the product details page.
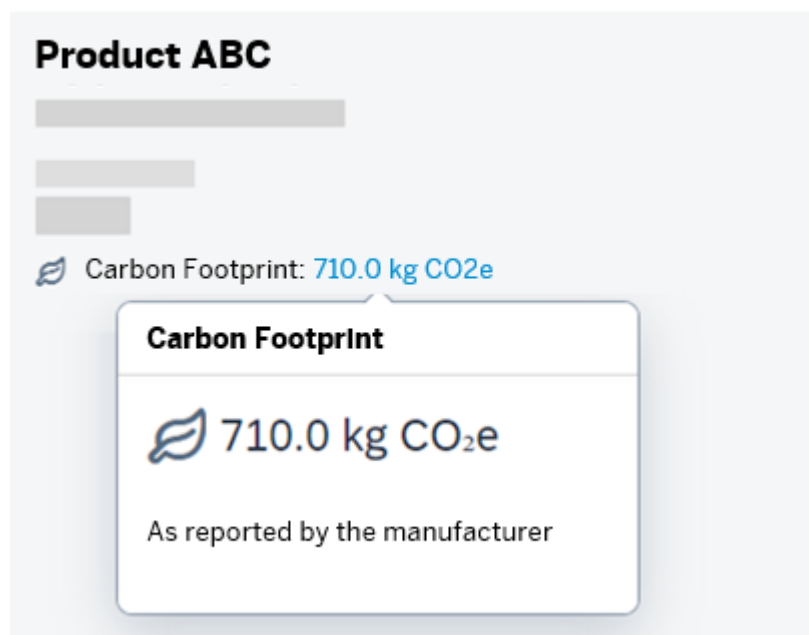
The supported third-party data provider is DitchCarbon, a qualified company through the SAP Partner Program. To retrieve carbon footprint information, you need an account with DitchCarbon. For a demo and to open an account, contact: sapsupport@ditchcarbon.com.

Once you have an account with DitchCarbon, they provide you with an API key that you can enter in the *Enable Data Provider for Carbon Footprint* app. The API key enables SAP Ariba Buying to access the DitchCarbon API and retrieve the carbon footprint data from their database or calculate it based on the parameters submitted. For added security, all API calls are secure.

If you disable the data provider, the *Carbon Footprint* field doesn't appear when users view product details.

Related Information

Carbon Footprint Information for Products
Disabling the Data Provider for Carbon Footprint Information

3.3.12.1 Enabling the Data Provider for Displaying Carbon Footprint Information

Use this procedure to connect to a third-party data provider of carbon footprint information for the products users view when shopping.

Prerequisites

To retrieve carbon footprint information, you need an account with data provider DitchCarbon. For more information, see Enable Data Provider for Carbon Footprint .

Context

When you enable the data provider, users can view carbon footprint information in the *Create Purchase Request* app.

Procedure

1. Go to the *Configure Buying* app.
2. Open the *Enable Data Provider for Carbon Footprint* app.

   The available data provider, DitchCarbon, is displayed.
3. Click the row containing the data provider.
4. Choose *Edit*.
5. Enter the API key provided to you by DitchCarbon.

   Make sure to enter the key exactly as it was provided to you.
6. Ensure that the *Enabled* checkbox is selected.
7. Save your changes.

   The *Enabled* column shows a value of *Yes*.

Results

When the data provider is enabled, the product details page in the *Create Purchase Request* app shows carbon footprint information if it's available in the data provider's database or if the data provider has enough information to calculate the likely carbon footprint.

Related Information

Carbon Footprint Information for Products
Disabling the Data Provider for Carbon Footprint Information

3.3.12.2 Disabling the Data Provider for Carbon Footprint Information

Use this procedure to disable the retrieval of carbon footprint information from the data provider and stop showing carbon footprint information in the *Create Purchase Requests* app.

Context

Disable the retrieval of carbon footprint information by changing the *Enabled* field in the *Enable Data Provider for Carbon Footprint* app.

Procedure

1. Go to the *Configure Buying* app.
2. Open the *Enable Data Provider for Carbon Footprint* app.

   The available data provider, DitchCarbon, is displayed.
3. Click the row containing the data provider.
4. Choose *Edit*.
5. Click the *Enabled* checkbox so that it's no longer selected.

   You can leave the API key in place in case you want to enable the data provider later.
6. Save your changes.

   The *Enabled* column now shows a value of *No*.

Results

Carbon footprint information is no longer retrieved from the data provider. The *Create Purchase Request* app no longer displays fields for carbon footprint information.

If you decide to re-enable the data provider later, edit the data provider details again and select the *Enabled* checkbox. If you removed the API key, re-enter it.

4 Security and Data Protection and Privacy

The topics in this section cover the security features for SAP Ariba Buying.

Since the apps run on SAP BTP, many of the necessary security measures are taken care of by SAP.

As SAP Ariba Buying is an SAP BTP solution, SAP strives to manage responsibilities assuring your security to the maximum extent possible.

To know more about how SAP securely manages your data, see the following documents:

- Security on BTP
- Security Information for SAP Cloud Identity Services - Identity Authentication

   Security Recommendations [page 98]
   > These recommendations help you evaluate the security of the configuration of SAP Ariba Buying in your landscape.

   Authorization [page 103]

   Data Storage Security [page 103]

   Network and Communication Security [page 103]

   Data Protection and Privacy [page 104]

   Audit Logging [page 120]
   > Find a list of audit log messages logged by SAP Ariba Buying.

   User Administration and Authentication [page 124]

4.1 Security Recommendations

These recommendations help you evaluate the security of the configuration of SAP Ariba Buying in your landscape.

> → Remember
>
> As part of the cloud shared responsibility model📄 (restricted access), you're responsible for determining if any of these recommendations are relevant to your environment and to what extent.
>
> The security recommendations are provided as a courtesy, without a warranty, and may be subject to change. For more information, see the disclaimer.

SAP Ariba Buying is delivered with secure default configurations wherever this is possible. However, you might want to review some settings and adjust them to your particular use case and corporate policies.

To find out more about the table headings used below, see Explanation of Table Headings [page 102].

Priority	Secure Operations Map	Topic	Default Settings or Behavior	Recommendation	More Information	Last Update	Index
Recommended	Authentication & Single Sign-On	Authentication: MFA	Authentication of business users is done via the corporate identity provider or the Identity Authentication service. There, SAP Ariba Buying appears as an application. Multi-factor authentication (MFA) is off by default in the Identity Authentication service.	Configure MFA for critical user groups on productive systems.	Multi-Factor Authentication	2024-04-23	ARI-SAB-0001

Priority	Secure Operations Map	Topic	Default Settings or Behavior	Recommendation	More Information	Last Update	Index
Recommended	Roles & Authorizations	Business Users: Data Restrictions	Role collections allow business users to access a scope of applications and services integrated with SAP Ariba Buying. Authorization policies allow business users to access a scope of data based on company code and plant.	Assign users and user groups to the appropriate role collections. Assign authorization policies to your business users.	• Authorization [page 103] (role collections) • About Managing Authorizations for Users [page 38] • Setting Up Roles for SAP Ariba Buying, Base Edition • Authorization Policy for SAP Ariba Buying [page 39]	2024-04-23	ARI-SAB-0002
Critical	Roles & Authorizations	Business Users: Authorization Review	N/A	Conduct regular authorization reviews.	• Authorization [page 103] • Setting Up Roles for SAP Ariba Buying, Base Edition	2024-04-23	ARI-SAB-0003

Other SAP components or solutions:

• SAP BTP Security Recommendations

Component	Additional Information Relevant for SAP Ariba Buying
Identity Authentication service	Authentication of business users can be done is done using the Identity Authentication service. See Managing Users.
Data Retention Manager	The SAP Data Retention Manager service helps in managing the deletion of personal or sensitive data in SAP Ariba Buying, including configuring the retention period. See: • Managing Data as a Data Protection Officer [page 111] • Steps to Configure the Residence and Retention Period [page 112] • If you are using the SAP Data Retention Manager, see SAP Data Retention Manager. If you are using the SAP Data Privacy Integration service, see Data Privacy Integration.

• SAP S/4HANA Cloud Security Recommendations

4.1.1 Explanation of Table Headings

Explanation of Table Headings

Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Information	Last Update	Index
Defines the criticality of the recommendation. For an explanation of the priority levels, see the *Explanation of Priority* table below.	The Secure Operations Map is a reference model to structure the broad area of security for content, discussions, and as a basis for a 360° view on security. For more information about the Secure Operations Map, see Security Overview as part of the *SAP Security Optimization Services Portfolio*.	A topic is a short description or a general heading to find similar topics across services.	Describes the usage of the security setting, including any context, or default setting behavior (if available).	Defines our recommendation for this configuration.	A link to documentation that explains how you can achieve the recommendation.	Date of the last significant change.	A stable unique reference to identify the recommendation.

Explanation of Priority

Priority	Description
Critical	Exposes the system to significant risk or threatens system reliability.
Recommended	Improves the security of the landscape and significantly reduces the attack surface.
Advanced	Extends the recommendation to a higher standard. The recommendation either extends the security standards to higher level of protection or to additional areas, such as your organization-specific requirements.

4.2 Authorization

SAP Ariba Buying supports the following roles and role collections for users.

Role Collection	Role	Description
Procurement User	`Procurement_User` (Procurement User)	A person in an organization who can shop for items.
Procurement Configuration Admin	`Procurement_Configuration_Admin` (Administrator)	An administrator who configures the settings and functionalities in SAP Ariba Buying.
Procurement Approver	`Procurement_Approver` (Approver)	An approver who can review and approve the items in a request.

We recommend removing roles from a user if the user no longer requires them. Ensure that you grant each user only the minimum level of authorization to perform the necessary tasks.

4.3 Data Storage Security

SAP Ariba Buying stores the transactional data on a HANA database. Each tenant has a dedicated schema and provisioned in a schema isolated model. All the configuration and user profile information is also in a schema isolated model.

> ⚠ Caution
>
> Ensure that you don't inadvertently trigger the unsubscription in SAP BTP cockpit. This might result in irrecoverable data loss.

4.4 Network and Communication Security

Inbound Communications

The inbound communication for catalogs from the supplier's website is through HTTPS. This also includes requests coming from other micro-services for SAP Ariba Buying.

The inbound communication for the document status from the connected system is through SOAP messages using HTTPS.

Outbound HTTP Communications

Outbound HTTP communications to SAP BTP services or to other micro-services for SAP Ariba Buying use HTTPS.

Outbound HTTPS Communications

The outbound communication between SAP Ariba Buying and Amazon is through HTTPS and the OAuth2 protocol.

Communication to Connected Systems

Outbound communications from SAP Ariba Buying to the various connected systems depend on your landscape configuration. It is recommended to ensure that HTTPS is in effect.

Connected System

Using SAP Ariba Buying, you can navigate to the Fiori application to view purchase orders and other follow-on documents in the connected system.

The communication to the connected system happens outside the scope of SAP Ariba Buying and it depends on your landscape configuration. However, you must use HTTPS to support the navigation to the connected system.

Communication to SAP S/4HANA Cloud Database

SAP Ariba Buying micro-services connect to SAP S/4HANA Cloud database through Transmission Control Protocol (TCP) with Transport Layer Security (TLS) protocol.

4.5   Data Protection and Privacy

Introduction

Data protection is associated with numerous legal requirements and privacy concerns. In addition to compliance with general data protection and privacy acts, it is necessary to consider compliance with industry-specific legislation in different countries. SAP provides specific features and functions to support compliance with regard to relevant legal requirements, including data protection, which are documented in these templates

along with the assumptions that have been guiding the implementation in the software. By nature of legal requirements the conclusion whether these features are covering customer specific demands as well as the conclusion whether additional measures have to be taken is solely with the customer.

> ⓘ Note
>
> SAP does not provide legal advice in any form. SAP software supports data protection compliance by providing security features and specific data protection-relevant functions, such as simplified blocking and deletion of personal data. In many cases, compliance with applicable data protection and privacy laws will not be covered by a product feature. Definitions and other terms used in this document are not taken from a particular legal source.

> ⚠ Caution
>
> The extent to which data protection is supported by technical means depends on secure system operation. Network security, security note implementation, adequate logging of system changes, and appropriate usage of the system are the basic technical requirements for compliance with data privacy legislation and other legislation.

User Consent

The processing of personal data (including its collection or its transfer) is based on purposes, legitimated by the fulfilment of a contract, a legal obligation, a vital interest, a public interest, a legitimate interest or a consent. In some cases, the data subject may also be the user. This SAP product provides functionality to capture consent of data subjects before collecting personal data, where no other legal ground exists. This allows data subjects to give and withdraw consent to process their personal data. Where data is processed for a purpose different than the original purpose or a privacy statement was changed, likely a new consent needs to be collected.

Read Access

Read Access Logging is considered as an additional safeguard in the protection of personal data, because it helps to identify potential illegitimate access to personal data. Read access logging (RAL) is used to monitor and log read access. Data may be categorized as sensitive by law, by external company policy, or by internal company policy. When these read accesses are logged, you should be able check which user accessed personal data on which access channel and the date and time, depending on the configuration. Read access logging enables you to answer questions about who accessed particular data within a specified time frame. That logging also includes downloading attachments or files, logs for such events shall contain information to identify the attachment. Additionally, as for Read Access Logging across system boundaries, the respective "access" shall be logged as soon as sensitive personal data crosses the boundary from a trusted to an un-trusted area. Here are some examples of such questions:

- Who accessed the data of a given business entity, for example the organizational data?
- Who accessed personal data, for example the employee in an organization?

Furthermore, log records can be viewed and queried, but access to them is restricted by adequate authorizations. The personal data for which read access shall be logged and the retention period of logs, can be configured

SAP captures consent between SAP and the customer in the contractual agreement. However, customers can also maintain their company's consent clauses in the Identity Authentication Service configuration.

Change Logs

Creation and change of personal data need to be documented. Therefore, for review purposes or as a result of legal regulations, it may be necessary to track the changes made to this data. When these changes are logged, you should be able to check which user made which change, the date and time, the previous value, and the current value, depending on the configuration. Furthermore, log records can be viewed and queried, but access to them is restricted by adequate authorizations. The personal data for which changes shall be logged and the retention period of logs, can be configured..

Artificial Intelligence

Solely automated decision-making that involves personal data processing could have serious consequences for individuals. In such decision processes there is no human intervention, therefore this also includes decisions that are based on Artificial Intelligence (AI). Serious impacts on an individual are legal or similarly significant effects, like e-recruiting practices without any human intervention. Such decisions have the potential to have a prolonged or permanent significant impact on the circumstances, behavior, or choices on the individual and lead at its most extreme to exclusion or discrimination. To safeguard the rights and freedom of individuals the data controller needs to evaluate which automated decisions used in this SAP application, could affect an individual's life. In this case, special requirements apply, which includes enabling of human intervention in such decision processes, ensuring that the used AI models do not result in inaccuracies detrimental to data subjects' rights and providing transparency in how AI is used during processing of personal data.

Suppliers

The requests that buyers create on SAP Ariba Buying contain the supplier information. SAP Ariba Buying stores the supplier ID and displays in the request and the follow-on transactional documents.

When the retention period ends, the request is deleted. As a result, the supplier ID information is also deleted. Administrators must ensure that they update the supplier information on SAP Ariba Buying accurately.

To update the supplier ID, administrators must do the following:

- 1. Go to the app, *Manage Supplier IDs*.
  2. Download the mapping file.
  3. Make the necessary changes for the supplier. Map the supplier ID that was deleted with the supplier ID on SAP S/4HANA Cloud.

4. Save the .csv file.
5. Upload the .csv file containing the suppliers ID.

For more information, see Managing Supplier IDs [page 60].

4.5.1 Glossary

The following terms are general to SAP products. Not all terms may be relevant for this SAP product.

Term	Definition
Artificial Intelligence (AI)	The simulation of human intelligence processes by machines and computer systems – typically by learning, coming to its own conclusions, appearing to understand complex content, engaging in natural dialogs with people, enhancing human cognitive performance (also known as cognitive computing) or replacing people on execution of nonroutine tasks. Applications include autonomous vehicles, automatic speech recognition and generation and detecting novel concepts and abstractions (useful for detecting potential new risks and aiding humans to quickly understand very large bodies of ever-changing information)
Automated Decision Making	The ability to make decisions by technological means without human involvement.
Blocking	A method of restricting access to data for which the primary business purpose has ended.
Business Purpose	The legal, contractual, or in other form justified reason for the processing of personal data to complete an end-to-end business process. The personal data used to complete the process is predefined in a purpose, which is defined by the data controller. The process must be defined before the personal data required to fulfill the purpose can be determined.
Consent	The action of the data subject confirming that the usage of his or her personal data shall be allowed for a given purpose. A consent functionality allows the storage of a consent record in relation to a specific purpose and shows if a data subject has granted, withdrawn, or denied consent.
Data Subject	Any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Term	Definition
Deletion	Deletion of **personal data** so that the data is no longer available.
End of Business	Defines the end of active business and the start of residence time and retention period.
End of Purpose (EoP)	The point in time when the processing of a set of personal data is no longer required for the primary business purpose, for example, when a contract is fulfilled. After the EoP has been reached, the data is blocked and can only be accessed by users with special authorizations (for example, tax auditors).
End of Purpose (EoP) check	A method of identifying the point in time for a data set when the processing of **personal data** is no longer required for the primary **business purpose**. After the **EoP** has been reached, the data is **blocked** and can only be accessed by users with special authorization, for example, tax auditors.
Personal data	Any information relating to an identified or identifiable natural person ("data subject"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
Processing of Personal Data	Processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Purpose	The information that specifies the reason and the goal for the processing of a specific set of personal data. As a rule, the purpose references the relevant legal basis for the processing of personal data.
Residence period	The period of time between the end of business and the end of purpose (EoP) for a data set during which the data remains in the database and can be used in case of subsequent processes related to the original purpose. At the end of the longest configured residence period, the data is blocked or deleted. The residence period is part of the overall retention period.

Term	Definition
Retention period	The period of time between the end of the last business activity involving a specific object (for example, a business partner) and the deletion of the corresponding data, subject to applicable laws. The retention period is a combination of the residence period and the blocking period.
Sensitive personal data	A category of personal data that usually includes the following type of information: • Special categories of personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or sex life or sexual orientation. • Personal data subject to professional secrecy • Personal data relating to criminal or administrative offenses • Personal data concerning insurances and bank or credit card accounts
Technical and organizational measures (TOM)	Some basic requirements that support data protection and privacy are often referred to as technical and organizational measures (TOM). The following topics are related to data protection and privacy and require appropriate TOMs, for example: • **Access control:** Authentication features • **Authorizations:** Authorization concept • **Read access logging** • **Transmission control / Communication security** • **Input control / Change logging** • **Availability control** • **Separation by purpose:** Is subject to the organizational model implemented and must be applied as part of the authorization concept.

4.5.2 Managing Data Protection and Privacy

Perform the following steps to configure the residence and retention period for the legal grounds.

You can delete the information for users in the app *Manage Data Subject Deletion*.

Archiving Data [page 114]
   Archive data for requests when the residence period has ended.

Manage Destruction of Data [page 114]
   Define the period for managing the deletion of the archived data.

Manual Deletion of User Information [page 114]

4.5.2.1 Overview

SAP Ariba Buying stores personal data for users. The personal data enables users to create requests with accurate organizational information.

Data on SAP Ariba Buying is classified as follows:

Data	Description
Personal	User information
Transactional	Information about requests, comments, account assignments for the line items
Configuration related to the procurement flow	Information about the following: • Editing document IDs • Maintaining details about suppliers, units of measure, and material groups in the mapping files
Other configuration	Configuration for the displaying announcements and managing recommendations

When there's a requirement to stop storing or processing the personal data, SAP Ariba Buying deletes the transactional data. As a result, the related personal data is also deleted. In addition, when a user leaves the company, the user information is also deleted.

SAP Ariba Buying blocks users from accessing the transactional data starting from the end of the residence period until the end of the retention period.

When the retention period ends, SAP Ariba Buying does the following:

• Deletes all the transactional data
• Marks the required personal data in the configuration as anonymous
• Deletes the user information when the user leaves the company

> ⓘ Note
>
> You can raise a customer incident using the component S2P-P2O-SET if you encounter any issues while configuring or working with the personal data.

4.5.2.2 Managing Data as a Data Protection Officer

You can use the Data Privacy Integration (DPI) service or SAP Data Retention Manager service to manage the personal data. The service runs on the SAP Business Technology Platform and helps in managing the deletion of data in SAP Ariba Buying.

The Data Protection Officer (DPO) must specify rules for deleting data. You need the necessary roles to manage the deletion of data.

You specify the rules in the SAP Data Retention Manager service for the following legal grounds :

- Request Information
- User Profile Information

As a DPO, you specify the legal grounds to set the residence and retention period for requests and users in the SAP Data Retention Manager or Data Privacy Integration (DPI) service. You can configure the time period in the service for the following:

- Residence period: Period during which all requests and user information must be complete and audited. The requests and user information must complete their lifecycle during the residence period.
- Retention period: Period during which you maintain the requests and user information even after the lifecycle of the request and user information is complete. The stipulated period depends on the specific laws based on your country/region.
  For more information about configuring the residence and retention period, see Steps to Configure the Residence and Retention Period [page 112].

> ⓘ Note
>
> Ensure that you maintain the residence period and retention period for the legal grounds User Information and Request Information on SAP S/4HANA Cloud and SAP Business Technology Platform (SAP BTP) with the same time period. The residence period and retention period on SAP S/4HANA Cloud and SAP Business Technology Platform (SAP BTP) must be identical.

For more information, see the following:

- If you are using the SAP Data Retention Manager, see
  - Roles
  - SAP Data Retention Manager
- For definitions about the residence and retention period, see Glossary [page 107].

4.5.2.3 Managing Data as an Administrator

As an administrator, you manage the configuration and data for SAP Ariba Buying.

The following process describes the blocking and deletion of data:

- **Use Case 1**: Deletion of requests at the end of the retention period
  When a Data Protection Officer (DPO) defines the residence and retention period, all requests that have been created by users on SAP Ariba Buying also adhere to the residence and retention period.
  When a user creates a request, the lifecycle of the request ends when the purchase order is invoiced, partially invoiced, or rejected. The invoiced or rejected date is the end of the business and the start of the

residence period. Once the residence period is complete, the user can't view or edit the request on the *My Requests* page.
The requests are deleted at the end of the retention period.

- **Use Case 2**: Deletion of user's personal data when a user leaves the company and all the requests have been deleted
When a user leaves the company, the administrator on the Identity Authentication service deletes the user. SAP Ariba Buying retrieves and stores the users that were deleted from the Identity Authentication service at periodic intervals.

When the Identity Authentication service deletes the users, the following information is also deleted for the user:

- Carts (active, saved, and carts that failed while submitting a request)
- Information on the user's last purchased items

When the retention period ends, the requests are deleted.

As a DPO, you can view the information for users for whom the residence period has elapsed in the following apps:

- If you are using the SAP Data Retention Manager service, see *Configure Data Subject Deletion* in the app *Delete Data Subject Information*. For more information, see Delete Data Subject Information.

Deletion of User Information for Administrators

When the user is an administrator, the user information is marked as Anonymous in all the configuration tasks managed by the administrator. The user or user ID is also displayed as Anonymous when the requests have crossed the residence period and have been deleted. The user or user ID appears in the following apps:

- *Edit Document IDs*
- *Manage Announcements*
- *Manage Recommendations*
- *Manage Supplier IDs*
- *Manage Units of Measures*
- *Manage Classification Codes*
- *Manage User Defaults*

The user profile for the administrator is deleted after the user information has been marked as Anonymous in all the configuration tasks.

4.5.2.4 Steps to Configure the Residence and Retention Period

Perform the following steps to configure the residence and retention period for the legal grounds.

Configure the residence and retention period for the legal grounds in the SAP Data Retention Manager service.

If you are using the SAP Data Retention Manager service, do the following:

1. Define the business purpose in the app *Manage Business Purposes*.
2. Choose *Add Business Purpose* and specify the following values:
   - *Business Purpose*: Enter a name of the business purpose. We recommend that you specify the business purpose based on the company code for your organization.
   - *Application Group*: Choose the name of the application, SAP Ariba Buying.
   - *Data Subject Role*: Choose one of the following:
     - *Procurement User*
     - *All*: Choose this option when you want to archive data for the legal ground, Request Information. Choose this option when you want to create the business purpose for a specific company code in your organization.
   - *Legal Entity*: Choose one of the following:
     - If you have chosen the data subject role as *Procurement User*, specify the company code for your organization.
     - If you have chosen the data subject role *All*, choose All when you want to archive the data for the legal ground, Request Information.
   - Define the residence and retention period rules for each of the legal grounds and save the changes.
     1. Legal Grounds
        - Request Information
        - User Profile Information

        > ⓘ Note
        >
        > When you have selected the legal entity as "All," you can only define the residence and retention period for the legal ground, Request Information. The legal ground User Profile Information is not available for you as SAP Ariba Buying only supports archiving of the data for the legal ground, Request Information.

   - Choose *Save and Activate* after you have defined the residence and retention period rules for both the legal grounds.

4.5.2.5   Delete Data Subject Information

You can delete the information for users in the app *Manage Data Subject Deletion*.

As a Data Protection Officer, you can view the users (data subjects) to be deleted only when the user is no longer in the company and the residence period has elapsed for the legal grounds user profile information and request information .

You can delete users only after they have been deleted in the *Identity Authentication service* and the residence period and retention period has elapsed for the legal grounds user profile information and requests information.

For more information, see the following:

- If you are using the SAP Data Retention Manager service, see Delete Data Subject Information.

4.5.2.6 Archiving Data

Archive data for requests when the residence period has ended.

You can archive the data for requests. The archived data contains requests that have elapsed their residence period. After the residence period has elapsed, users cannot access these legal grounds.

If you are using the SAP Data Retention Manager service, archive the request information by specifying the value for the *Data Subject Role* and *Legal Entity* as All in the app, *Add Business Purpose*:

> ⓘ Note
>
> You can only archive the data for the Request Information .

- If you are using the SAP Data Retention Manager service, see Managing Data Archiving.

4.5.2.7 Manage Destruction of Data

Define the period for managing the deletion of the archived data.

If you are using the SAP Data Retention Manager service, use the app *Manage Data Destruction* in the *SAP Data Retention Manager* service to delete all the archived information that can be deleted. You can delete the information for the requests only after it exceeds the retention period.

To delete the information, you must have an active business purpose with the legal entity and the value for the data subject role as "ALL."

For more information, see the following:

- If you are using the SAP Data Retention Manager service, see Managing Data Destruction.

4.5.2.8 Manual Deletion of User Information

When the retention period is less than one year, the user data is not automatically deleted. The retained data can be deleted by creating a ServiceNow case using the S2P-P2O-SET component.

4.5.3 Data Protection and Privacy for Intelligent Features

Intelligent features in SAP Ariba Buying include personalized recommendations for popular items and items that are frequently bought together and recommended material groups when requesting unlisted items.

Use of Data and Data Privacy

The system uses user interactions as data basis to train the machine learning model for intelligent features. These interactions include viewing a product, adding items to cart, and submitting requests. Any association with a particular user is obfuscated before using the data.

Data Isolation

The data used to train the machine learning is isolated for your particular tenant, and is not used in any other tenant or SAP solution.

Continuous Improvement

The features *Popular Items*, *Recommended Material Groups for Unlisted Items* and *Also Bought Together* provided by SAP as part of SAP Ariba Buying including automation, transaction processing, and machine learning may be continuously improved on behalf of the customer. SAP may use customer data in order to achieve such improvement. To find more details on the listed features, see *Related Information*.

Related Information

Intelligent Features in SAP Ariba Buying

4.5.4 Working with Personal Data

Manage the personal data for users in the organization using the app *SAP Personal Data Manager*.

As an administrator you can use the app *SAP Personal Data Manager* to export personal data for users. When you schedule a request to export the personal data for users, the users receive an email with the link to view their personal data. You need a subscription and the required authorization to access the *SAP Personal Data Manager* service.

The app allows you to view your personal data that has been marked as personal information and the list of applications or services that use them.

You can search for users (data subject) and see the following:

- In the *Application* section, view the list of applications that use your personal data.
- In the *Requests* section, view the requests you have made for corrections or deletions to your personal data. In the *Export Requests* section, you can view the requests for exporting or downloading your personal data.

For more information about the personal data, see Manage Personal Data.

4.5.4.1   Managing Personal Data

SAP Ariba Buying stores personal data user information in different areas while a user performs different tasks.

The following is an overview of the personal data information that SAP Ariba Buying stores or processes for users:

Application or Page	Fields that Store Personal Data	Description
User Profile App	`User` `UserName` `FirstName` `MiddleName` `LastName` `FullName` `Email` `AddressId` `CompanyCode` `Plant` `DeliverTo` `GLAccount` `CostCenter` `Global User ID`	These fields store the profile information and default settings for users. SAP Ariba Buying processes the user information when users view or modify their user profile information.
Create a Request page	`createdBy` `modifiedBy` `Title` `SupplierID`	These fields store the information for a new cart, an existing cart, or when a user creates a new request. When users use the default cart name, the cart title contains the user's name.
Comments in a Request	`createdBy` `modifiedBy` `UserName`	These fields store the user name of the person who created or modified comments added to a request. A request contains comments from the person creating the request or an approver reviewing the request for approval.

Application or Page	Fields that Store Personal Data	Description
Product Details page	• UserID	This field stores user information to show the user when the item was last purchased. SAP Ariba Buying also stores information on the request ID and date the item was last purchased.
Edit Document IDs app	• UserID	This field stores information about the users that modified the document ID.
Home page of the Create Purchase Request app	• FirstName	This field displays the information for the user name addressed in the salutation. The user name is derived from the user profile.
Announcement pop-up	• FirstName • LastName	These fields store information about the person of contact for the announcement (Learn More popup).
Manage Announcements app	• CompanyCode • CompanyName • Plant • PlantName • UserID • FullName • Email • createdBy • modifiedBy	These fields store information about the administrator and the administrator's organization when they create or edit announcements.
Manage Recommendations app	• Company code • Plant code • Material group • createdBy • modifiedBy	These fields store information about the recommendation for items.
Used in data models on SAP Ariba Buying	• createdBy • updatedBy	These fields are used in the data models that SAP Ariba Buying uses to process the following: • Line items • Requests • Carts • Workflow approval tasks • Approvals • Configuration • Default settings

4.5.4.2 Retrieving Personal Data

You can send a request to retrieve the personal data.

You can retrieve personal data for a user stored on SAP Ariba Buying. To retrieve the personal data, please create a ServiceNow case using the component, S2P-P2O-SET.

4.5.4.3 Scheduling a Request to Export Personal Data for Users

Schedule a request to export the personal data information.

Context

You can export the personal data information for users. Choose to schedule a request to export the personal data information for an application and data subject role as required. You need a subscription and the required authorization to access the service.

Procedure

1. Sign in to *SAP Personal Data Manager*.
2. Choose *SAP Personal Data Manager*.
3. Search for the user (Data Subject) and navigate to the user's detailed information.
4. Choose the application from which you want to export the personal data.
5. On the details page for the application, choose *Export Personal Data*.
6. Choose one of the following:
   - Select the email address of the user. When you choose the email option, the user receives an email to view their personal data.
   - You can choose to download the information in one of the following file formats:
     - PDF
     - JSON
     - XML
7. (Optional) If you want to download all the transactional data for your user, choose *Export all transaction data*.
8. Choose *Export*. A message appears confirming your request to export the data.
9. Go to the *Export Request* section to download the data after your request is processed.

> ⓘ **Note**
> - You can schedule another request to export the data only after the previous export request is complete.
> - For more information about personal data, see Manage Personal Data.

4.5.4.4 Deleting Personal Data

When considering compliance with data protection regulations, it is also necessary to consider compliance with industry-specific legislation in different countries. A typical potential scenario in certain countries is that personal data shall be deleted after the specified, explicit, and legitimate purpose for the processing of personal data has ended, but only if no other retention periods are defined in legislation, for example, retention periods for financial documents. Legal requirements in certain scenarios or countries also often require blocking of data in cases where the specified, explicit, and legitimate purposes for the processing of this data have ended, however, the data still has to be retained in the database due to other legally mandated retention periods. Sometimes, transactional data are personal data with relation to a master data object, e.g. a sales order with reference to a business partner. Therefore, the challenge for deletion and blocking is first to handle transactional data and finally other data, such as business partner data.

Simplified Deletion

The processing of personal data is subject to applicable laws related to the deletion of this data when the specified, explicit, and legitimate purpose for processing this personal data has expired. If there is no longer a legitimate purpose, that requires the retention and use of personal data, it must be deleted irrecoverably. Blocking is necessary when the original retention period has expired but additional applicable extended and overruling (mandated by law) retention periods are still in place. After the expiration of the longest retention period, the data must be deleted.

SAP Ariba Buying deletes the personal data user information in the following fields:

- `User`
- `UserName`
- `FirstName`
- `MiddleName`
- `LastName`
- `FullName`
- `Email`
- `AddressId`
- `CompanyCode`
- `Plant`
- `DeliverTo`
- `GLAccount`
- `CostCenter`

For more information on personal data, see Managing Personal Data [page 116].

4.5.4.5 Deleting Data from Your Subscription

You can delete the personal data from the subscription you have for SAP Ariba Buying.

Context

You must unsubscribe to delete the existing subscription that you have for SAP Ariba Buying. When you unsubscribe, your existing entitlements are removed for your subaccount. Additionally, all your user information is also deleted.

Procedure

1. Open the SAP BTP cockpit.
2. Go to *Instances and Subscriptions*.
3. Choose the tenant for SAP BTP and then choose *Actions* (...) on the top-right hand side.
4. Choose *Delete*.

4.5.4.6 Exporting Data for Customers in the Cloud Environment

Customers can request the export of their data on the cloud.

Customers using cloud solutions can request the export of their data available in the cloud environment. To request the export of customer data, create a ServiceNow case using the component, S2P-P2O-SET.

4.6 Audit Logging

Find a list of audit log messages logged by SAP Ariba Buying.

SAP Ariba Buying integrates with the SAP Audit Log Viewer for the Cloud Foundry Environment, that displays the audit logs for your Cloud Foundry account. To find more details on the SAP Audit Log Viewer and how to subscribe to it, see Audit Log Viewer for the Cloud Foundry Environment.

Security Events (audit.security-events)

Event Grouping	Event	Example Message
Authentication or authorization issues	JSON Web Token (JWT) is expired	`JWT validation failed for endpoint <endpoint> with error: jwt expired`
	JWT has a wrong signature	`JWT validation failed for endpoint <endpoint> with error: invalid signature`
	JWT has the wrong format	`JWT validation failed for endpoint <endpoint> with error: Invalid JWT`
	JWT does not provide the required authorization to access an inbound service	`Authorization check failed: insufficient XSUAA scopes. Endpoint: <endpoint>`
Service subscription or unsubscription	One-time event	

Configuration Changes

Event Grouping	Change/Event	Example Message	Additional Information
Document IDs	Edit document ID	`Configuration modification message. Attribute with name <attribute name> was changed from <previous value> to <new value>.`	Editing Document IDs [page 53]
Announcements	Create announcement		Creating Announcements for the Create Purchase Request App [page 85]
	Edit announcement		
	Delete announcement		
	Fetch user information when creating or editing announcement		
Recommendations	Create recommendation		Configuring Shopping Recommendations
	Edit name of recommendation		

Event Grouping	Change/Event	Example Message	Additional Information
Supplier IDs	Upload / edit mapping of suppliers	`Configuration modification message. Attribute with name <Vendor to Supplier Mapping> was changed from <Old Vendor to Supplier Mapping> to <New Vendor to Supplier Mapping>.`	Managing Supplier IDs [page 60]
Units of measure	Upload / edit mapping of units of measure	`Configuration modification message. Attribute with name <External to Internal UOM Mapping> was changed from <Old External to Internal UOM Mapping> to <New External to Internal UOM Mapping>.`	Managing Units of Measure [page 56]
Classification codes / material groups	Upload / edit mapping of classification codes with material groups	`Configuration modification message. Attribute with name <ClassificationCode to MaterialGroup Mapping> was changed from <Old ClassificationCode to MaterialGroup Mapping> to <New ClassificationCode to MaterialGroup Mapping>.`	Mapping Classification Codes with Material Groups [page 53]
User defaults	Edit user defaults	`Configuration modification message. Attribute with name <Attribute name> was changed from <previous value> to <new value>.`	Maintaining Default Values for Users [page 45]
Shopping sites	Create shopping site		Manage Shopping Sites

Event Grouping	Change/Event	Example Message	Additional Information
	Edit shopping site	`Shop has been updated with Shop ID <shop ID> and Type <shop type>.`	
	Delete shopping site		

Personal Data Access

Event Grouping	Event	Example Message
User profile	User edits own user profile	`Data Modification message. Attribute with name <Attribute name> was changed from <previous value> to <new value>.`
Personal data	User edits address	
	Edit company code	`Data Modification message. Attribute with name <companyCode_CompanyCode> was changed from <Masked Old Value> to <Masked New Value>. The attribute is a part of an object with type <type> and id consisting of: companyCode <xxxx>.`
	Edit plant	`Data Modification message. Attribute with name <Attribute name> was changed from <previous value> to <new value>.`
	Edit shipping address	`Data Modification message. Attribute with name <Attribute name> was changed from <previous value> to <new value>.`
	Edit cost center	`Data Modification message. Attribute with name <Attribute name> was changed from <previous value> to <new value>.`

Related Information

[Audit Logging in the Cloud Foundry Environment](#)

4.7 User Administration and Authentication

User Administration

SAP Ariba Buying users must be registered on the Identity Authentication service. The user authentication is done using the Identity Authentication service.

SAP recommends that you use the multi-factor authentication that is available in the Identity Authentication services.

For more information, see Security Information.

Authentication

SAP Ariba Buying uses the standard OAuth 2.0 with the SAP Authorization and Trust Management service for SAP BTP in the Cloud Foundry environment as authorization server. For more information, see SAP Authorization and Trust Management Service.

When using certificates, ensure that you do the following:

- Use a signed X.509 certificate by a trusted certificate authority (CA). If you use a self-signed certificate, ensure that the digital signatures and time stamps have been validated by a trusted key store.
- Use the client certificate-based authentication to allow a secure communication from one system to another. We recommend that you use client certificates with a short-term validity.

5 Disaster Recovery

This section describes the disaster recovery plan for the data centers used by SAP Ariba Buying.

5.1 About Disaster Recovery

SAP Ariba Buying supports recovering and reinstating your application and data in the event of a disaster.

5.2 High Availability and Reliability

SAP Ariba Buying offers customers a reliable mechanism to mitigate disaster recovery.

Prerequisite

The timing is applicable when the SAP BTP infrastructure and backing services, which SAP Ariba Buying relies on have recovered from the disaster event.

SAP provides customers using SAP Ariba Buying with availability management, security, and data integrity. SAP Ariba Buying provides backup services and an option for disaster recovery that customers can use.

The following is the recovery time to bring up the application in the event of a disaster:

Recovery Time Objective (RTO) and Recovery Point Objective (RPO)

The RTO depends on the nature and extent of the disaster damage. Although SAP Ariba Buying ensure that an outage is avoided, the disaster recovery depends on the scale of the disaster.

In an event of any disaster, the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) is 48 hours to bring up the application and 7 days for customers to verify the data from the original region and data center. This timing is applicable when the infrastructure and service have recovered from the disaster event.

SAP Ariba Buying schedules jobs to execute an automated backup of customer's data. Additionally, a backup of the log files is automatically taken at 15-minute intervals.

As part of the RPO, when SAP Ariba Buying restores the data and restores the system, the loss of data would be a maximum of 15 minutes.

When SAP Ariba Buying cannot recover the data from the original data center because the severity of the disaster, SAP Ariba Buying can choose to recover the data from the data center of another region. The time for the RTO and RPO is 5 days to host the data and bring up the application and 14 days for the customer to verify the data.

5.3   What SAP Ariba Buying Supports

- SAP Ariba Buying only supports the availability zone (AZ) level outage with high availability.
- The Disaster Recovery plan does not cover the following:
    - Data corruption or any accidental data deletion. Customers can request to restore the data from the existing backup.
    - Disasters related to non-IT, personnel, human resources, and real estate

5.4   Disaster Recovery Plan

The following is the disaster recovery plan for SAP Ariba Buying.

When a standard disaster occurs, SAP Ariba Buying does the following:

- Moves the data for SAP Ariba Buying in another region when it cannot recover the data into an existing region
- Verifies that all the application and services are functional
- Imports the data backed up
- Notifies customers when they can test their sites to verify data and its stable environment

5.5   Data Backup Plan

The following is the backup plan for data recovery in SAP Ariba Buying.

SAP Ariba Buying schedules data backup at regular intervals. The backups are replicated to a secondary site, from where they can be restored in case of a disaster.

When there is an inadvertent data destruction, within the primary data center, the data is recovered using the data that was last backed up.

SAP Ariba Buying schedules jobs to execute an automated backup of customer's data. Additionally, a backup of the log files is automatically taken at 15-minute intervals.

As part of the RPO, when SAP Ariba Buying restores the data and restores the system, the loss of data would be a maximum of 15 minutes.

The data backups that SAP Ariba Buying maintains are retained in an encrypted format for a period of 14 days. SAP Ariba Buying follows best practices and ensures that all the necessary steps are taken to prevent data failure to the best of its capability.

5.6   Communication to Customers After a Disaster or Incident

SAP Ariba Buying follows the standard process in communicating an incident or disaster.

Customers can create a ServiceNow case using the related components. When a disaster occurs, customers must contact the designated customer support.

After SAP Ariba Buying evaluates the impact of the damage, customers will be notified with the statuses periodically until the applications and services are up and running.

6 Unsubscribing from SAP Ariba Buying, base edition

You can unsubscribe from the SAP Ariba Buying, base edition when you no longer need it.

When your entitlements to SAP Ariba Buying, base edition ends, you can no longer use it. You must unsubscribe from SAP Ariba Buying, base edition to remove the subscription from your subaccount.

When you unsubscribe, SAP deletes all the data available for SAP Ariba Buying.

    Customers can request the export of their data on the cloud.

    You can unsubscribe from SAP Ariba Buying when the existing entitlements are no longer available.

6.1 Exporting Data for Customers in the Cloud Environment

Customers can request the export of their data on the cloud.

Customers using cloud solutions can request the export of their data available in the cloud environment. To request the export of customer data, create a ServiceNow case using the component, S2P-P2O-SET.

6.2 Unsubscribing from SAP Ariba Buying

You can unsubscribe from SAP Ariba Buying when the existing entitlements are no longer available.

Prerequisites

Before you unsubscribe, we recommend that you back up your data from SAP Ariba Buying. For more information, see .

Context

When your entitlements to SAP Ariba Buying ends, you can no longer use SAP Ariba Buying. You must unsubscribe from SAP Ariba Buying in the SAP BTP cockpit to remove the subscription from your subaccount.

When you unsubscribe, SAP deletes all data included in the SAP Ariba Buying solution immediately. The deleted data includes the personal data that SAP Ariba Buying stores. For more information on personal data, see Working with Personal Data [page 115].

For more information about the personal data that SAP Ariba Buying stores, see Managing Data Protection and Privacy [page 109].

Procedure

1. Open the SAP BTP cockpit.
2. Go to *Instances and Subscriptions*.
3. Choose the tenant for SAP BTP and then choose *Actions* (**...**) on the top-right hand side.
4. Choose *Delete*.

7 Support

When you encounter errors using SAP Ariba Buying and you need support from SAP, you can reach out to us. Tell us about the issue you're facing by reporting an incident on the SAP Support Portal.

Use the following components available for SAP Ariba Buying when reporting an incident:

Component	Use this component to raise issues ...
S2P-P2O-BC	occurring in any configuration application.
S2P-P2O-SET	occurring when you set up or subscribe to SAP Ariba Buying, or when you request the export of your data due to contract termination.
S2P-P2O-WFL	related to workflow.
S2P-P2O-BX-CAT	related to shopping sites.
S2P-P2O-BX-SRC	related to product search.
S2P-P2O-BX-SC	related to cart.
S2P-P2O-AI	related to intelligent features in SAP Ariba Buying.
S2P-P2O-BX-LP	related to the home page of the *Create Purchase Request* app.
S2P-P2O-BX	only if none of the `S2P-P2O-BX-*` components in this table apply.

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.

THE BEST RUN **SAP**