# TABLE OF CONTENTS

1  INTRODUCTION .......................................................................................................................... 4
   1.1 Prerequisites ............................................................................................................................... 4
   1.2 Overview ..................................................................................................................................... 5
2  SET UP AN SAP CLOUD PLATFORM GLOBAL ACCOUNT ................................................................. 7
3  CREATE A CLOUD FOUNDRY SUBACCOUNT ................................................................................... 8
4  SUBSCRIBE TO SAP CLOUD PLATFORM AUDIT LOG VIEWER ....................................................... 9
5  SUBSCRIBE TO SAP CLOUD PLATFORM PERSONAL DATA MANAGER ........................................ 10
6  SUBSCRIBE TO GLOBAL TRACK AND TRACE OPTION ............................................................... 11
7  CREATE ONBOARDING ADMINISTRATOR ....................................................................................... 12
   7.1 Maintain Role Collection ........................................................................................................... 12
8  CONFIGURE SAP CLOUD PLATFORM IDENTITY AUTHENTICATION SERVICE .......................... 13
   8.1 Create User Groups ................................................................................................................... 13
   8.2 Create a New User ...................................................................................................................... 14
   8.3 Assign User Groups to a User ..................................................................................................... 14
   8.4 Establish Trust and Federation with User Account and Authentication .................................... 15
   8.5 Configure the Application Authentication ................................................................................. 16
   8.6 Configure the System Authentication ....................................................................................... 16
   8.7 Map Role Collection to User Group .......................................................................................... 16
9  CONFIGURE THIRD-PARTY IDENTITY PROVIDER (OPTIONAL) .................................................... 18
   9.1 Add Your Identity Provider as the Corporate Identity Provider ............................................... 18
   9.2 Establish Trust and Federation with User Account and Authentication .................................... 18
   9.3 Set Default Identity Provider ..................................................................................................... 20
   9.4 Map Role Collection to User Group .......................................................................................... 20
10 CREATE A TECHNICAL USER ...................................................................................................... 21
11 MAINTAIN GENERAL SETTINGS IN ONBOARDING ASSISTANCE APP ....................................... 22
12 CONFIGURE THE NEO ENVIRONMENT FOR GLOBAL TRACK AND TRACE OPTION ............... 23
   12.1 Prerequisites .............................................................................................................................. 23
   12.2 Configure SAP Cloud Platform Neo Subaccount ..................................................................... 24
   12.3 Configure SAP Cloud Platform Authentication Service ............................................................ 25
   12.4 Add SAP Cloud Platform Subaccount as a Trusted Application ............................................. 26
   12.5 Configure SAP Web IDE ........................................................................................................... 27
      12.5.1 Enable SAP Web IDE Full-Stack ........................................................................................... 27
      12.5.2 Import the Destination for the GTT Metadata Service ............................................................ 28
   12.6 Configure SAP Cloud Platform Business Rules Service ............................................................ 29
13 CONNECT TO SAP ERP .................................................................................................................. 30
   13.1 Prerequisites .............................................................................................................................. 31
   13.2 Deploy SAP Cloud Platform Integration Content ....................................................................... 31
      13.2.1 Set up Certificate and Permissions ....................................................................................... 31
1 INTRODUCTION

SAP Logistics Business Network, global track and trace option is a cloud service solution based on the SAP Cloud Platform. Besides global track and trace option, there is an option called freight collaboration. These two options focus on different scenarios in supply chain management.

This document describes the technical steps needed to set up the use of SAP Logistics Business Network, global track and trace option from your SAP Cloud Platform global account.

1.1 Prerequisites

Before you start working through this document, ensure that you have downloaded the most recent version of this Onboarding guide. It is regularly updated with bug fixes and the latest information as it becomes available.

Note
All GTT documents are available from the SAP Help Portal at:
help.sap.com/gtt

1.2 Overview

SAP Logistics Business Network, global track and trace option is an application deployed in the SAP Cloud Platform Cloud Foundry. Its dependent services, SAP Web IDE and SAP Business Rules, run in SAP Cloud Platform Neo environment.

As shown in the diagram, in your Cloud Foundry subaccount, you subscribe to the Audit Log Viewer and the Personal Data Manager needed by the business roles, Audit Specialist and DP&P Specialist, respectively. You also configure roles and role collections to manage your users.

SAP Identity Authentication Service (SAP IAS) serves as your identity provider. In SAP IAS, you create user groups then map them to the role collections in your Cloud Foundry subaccount. Users assigned to a user group get all the relevant authorizations for that group.

Also, as indicated in the diagram, you need to establish trust between the following:

- Cloud Foundry subaccount and SAP IAS: to allow you to use SAP IAS as your identity provider.
- Cloud Foundry subaccount and Neo subaccount: to allow you to connect GTT to its dependent services on Neo.
- Neo subaccount and SAP IAS: to allow you to use Single-Sign-On log in to SAP Web IDE.

Further, in the Administration guide you’ll find the information you need to configure:

- the Neo environment to run services SAP Web IDE and SAP Business Rules
- SAP ERP to access business partner and master data information.

You need to set up roles including the following:

- **Technical user**: a role required by certain services to access the GTT solution.
- **Onboarding administrator**: a role that completes the onboarding tasks in the onboarding assistance app and assigns **solution administrators** for the GTT solution. Solution administrators oversee the running of the GTT solution for example by managing business partners and business users, checking error logs and configuring system parameters.
To begin onboarding, you need:

- an administrator role of an SAP Cloud Platform global account so you can create a new Cloud Foundry subaccount and subscribe to GTT.
- an administrator role of a Neo subaccount. If you already have a Neo subaccount, you can reuse it.

<table>
<thead>
<tr>
<th>Main Role</th>
<th>Task</th>
</tr>
</thead>
</table>
| Administration role of SAP Cloud Platform global account | 2 Set up an SAP Cloud Platform Global Account  
3 Create a Cloud Foundry Subaccount  
4 Subscribe to SAP Cloud Platform Audit Log Viewer  
5 Subscribe to SAP Cloud Platform Personal Data Manager  
6 Subscribe to GTT  
7 Create Onboarding Administrator  
8 Configure SAP Cloud Platform Identity Authentication Service  
9 Configure Third-party Identity Provider (Optional)  
10 Create a Technical User |
| Onboarding Administrator                        | 11 Maintain General settings in Onboarding Assistance App |
| Administrator role of Neo account               | 12 Configure Neo |
| Multiple GTT roles plus SAP ERP user            | 13 Configure SAP ERP |
| Onboarding Administrator                        | 14 Maintain System integration Info in Onboarding Assistance App  
15 Onboard Solution Administrator                |
| Solution Administrator                          | 16 Maintain the Technical User for your company |
2 SET UP AN SAP CLOUD PLATFORM GLOBAL ACCOUNT

Your SAP Cloud Platform global account is the entry point for managing the resources, landscape, and entitlements for your departments and projects in a self-service manner.

SAP Logistics Business Network, global track and trace option is an application run on SAP Cloud Platform. After you have purchased SAP Logistics Business Network, global track and trace option, you are entitled to use SAP Logistics Business Network, global track and trace option.

You receive an initial email with the subject line “SAP Cloud Platform is ready to use”. It contains the following:

- a link to the Home page of SAP Cloud Platform and
- the SAP ID User to log on the SAP Cloud Platform.

You can use this information to start to set up your global account.

If you don't have the initial email, you can do the following:

- To find the official contact in your company who received the initial email, follow the advice in SAP note 2596214.
- If the login details are lost or you want the initial email to be resent, follow the advice in SAP note 2641472.

Context

The SAP ID User has the administrator role of the global account. All global account members have global account administrator permissions for their global account, and can do the following:

1. View all the subaccounts in the global account, meaning all the subaccount tiles in the global account's Subaccounts page.
2. Edit general properties of the subaccounts in the global account from the Edit icon in the subaccount tile.
3. Create a new subaccount in the global account.
4. View, add, and remove global account members.
5. Manage entitlements for the global account.

To set up a global account, first log on to your global account using the SAP ID User and then add members to the global account.

Procedure

1. Use the link in your initial email and your SAP ID User to log on to your global account.
2. In the navigation area of your global account, choose Members. Then Add Members.
3. In the Add Members dialog box, enter one or more SAP user IDs (s-user or p-user), separated by commas, spaces, semicolons, or line breaks under User IDs. Keep the User Base as "accounts.sap.com".

The users you add as members at this global account level are automatically assigned the Administrator role.
3 CREATE A CLOUD FOUNDRY SUBACCOUNT

Prerequisites
You are a member of the global account, that is, you have the administrator role of the global account.

Context
You must create a Cloud Foundry subaccount in your global account to subscribe the SAP Logistics Business Network, global track and trace option application. The following procedure describes how you create a Cloud Foundry subaccount.

Procedure
Follow the procedures available from Create Subaccount Using the Cockpit.

Please read through the link and pay attention to the details in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Name</td>
<td>Enter a name for the subaccount. Use a name that is easy for you to distinguish.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) Enter a description for your subaccount.</td>
</tr>
<tr>
<td>Neo Environment</td>
<td>Do not select this option. Clearing this option creates a Cloud Foundry subaccount.</td>
</tr>
<tr>
<td>Provider</td>
<td>Select Amazon Web Services (AWS)</td>
</tr>
<tr>
<td>Region</td>
<td>Select Europe (Frankfurt)</td>
</tr>
<tr>
<td>Subdomain</td>
<td>The subdomain will become part of the URL for accessing subscribed applications. The subdomain can contain only lowercase letters, digits and hyphens (in the middle) and must be unique within your global account.</td>
</tr>
<tr>
<td>Use for production</td>
<td>Select this option if your account is used for production purposes. Do not select this option if it is for non-production purposes, such as development, testing, and demos.</td>
</tr>
<tr>
<td>Enable beta features</td>
<td>We recommend not to enable the beta features. (You should not use SAP Cloud Platform beta features in subaccounts that belong to productive enterprise accounts. Any use of beta functionality is at the customer's own risk, and SAP shall not be liable for errors or damage caused by the use of beta features.)</td>
</tr>
</tbody>
</table>

After you create the subaccount, you are automatically the administrator of the subaccount.
4 SUBSCRIBE TO SAP CLOUD PLATFORM AUDIT LOG VIEWER

The audit log viewer displays the audit logs for your Cloud Foundry account, produced by SAP applications and services you’ve subscribed to. It is an essential component in the GTT solution infrastructure.

Prerequisites

With your Cloud Foundry subaccount, now you can subscribe to Audit Log Viewer. The application Audit Log Viewer is entitled to the subaccount.

Context

The following procedure describes how you subscribe to Audit Log Viewer.

Procedure

1. In the SAP Cloud Platform Cockpit, go to your Cloud Foundry subaccount.
2. In the left pane, click Subscriptions, and you see all the applications that you can subscribe to.
3. Click the tile Audit Log Viewer.
4. Then click Subscribe.

Now your subscription is complete.
5 SUBSCRIBE TO SAP CLOUD PLATFORM PERSONAL DATA MANAGER

Prerequisites
With your Cloud Foundry subaccount and your subscription to the SaaS application SAP Audit Log Viewer, now you can subscribe to Personal Data Manager. The application Personal Data Manager is entitled to the subaccount.

Context
The following procedure describes how you subscribe to Personal Data Manager.

Procedure
1. In the SAP Cloud Platform Cockpit, go to your Cloud Foundry subaccount.
2. In the left pane, click Subscriptions, and you see all the applications that you can subscribe to.
3. Click the tile Personal Data Manager.
4. Then click Subscribe.

Now your subscription is complete.
6 SUBSCRIBE TO GLOBAL TRACK AND TRACE OPTION

Subscribing is a preliminary step to use the SaaS application, SAP Logistics Business Network, global track and trace option.

Notes

- If you are a GTT customer, your license provides you with two subscriptions to SAP Logistics Business Network, global track and trace option. Once you have subscribed twice, any further attempt to subscribe will fail.
- If you are a GTT partner, your license provides you with one subscription to SAP Logistics Business Network, global track and trace option. If you have already subscribed, any further attempt to subscribe will fail.

Prerequisites

- A Cloud Foundry subaccount
- A subscription to the SaaS application Audit Log Viewer. This is required to set up the business role, Audit Specialist.
- A subscription to the Personal Data Manager. This is required to set up the business role, DP&P Specialist.

Procedure

To subscribe to SAP Logistics Business Network, global track and trace option:

1. In the SAP Cloud Platform Cockpit, go to your Cloud Foundry subaccount.
2. In the left pane, click Subscriptions, and you see all the applications you can subscribe to.
3. Click on the tile Solution Owner Apps for Global Track and Trace.
4. Then click Subscribe.

Your subscription is complete.

To get the tenant-specific URL for accessing your GTT solution, click Go to Application.
7 CREATE ONBOARDING ADMINISTRATOR

Before using the subscribed GTT solution, you need to maintain a role called Onboarding Administrator to help you complete the whole onboarding process.

To do that, you must be an administrator of the Cloud Foundry subaccount. Note that the person who created the Cloud Foundry subaccount is automatically the administrator of the subaccount.

An Onboarding Administrator will use the Onboarding Assistance app to complete the onboarding of GTT solution and assign Solution Administrators. Then Solution Administrators will take over the GTT solution to run.

7.1 Maintain Role Collection

Role collections group together different roles that can be applied to the application users.

Context

Application developers have defined application-specific role templates in the security descriptor file. Role templates contain role definitions. You can assign the role to a role collection. As an administrator of the Cloud Foundry subaccount of SAP Cloud Platform, you can group application roles in role collections. Typically, these role collections provide authorizations for certain types of users, for example, onboarding administrators.

Once you have created a role collection, you can add roles to the role collection. Since the roles are application-based, you must select the application to see which roles come with the role template of this application. You are free to add roles from multiple applications to your role collection.

Procedure

1. In the SAP Cloud Platform Cockpit, go to your Cloud Foundry subaccount.
2. In the left pane, select Security † Role Collections.
3. Click New Role Collection.
4. Specify role collection name TT_ONBOARDING_ADMINS and a role description and click Save.
5. Select the role collection name TT_ONBOARDING_ADMINS.
6. Click Add Role.
7. In the Add Role dialog box, select the application identifier, role template and role as shown below.

<table>
<thead>
<tr>
<th>Application Identifier</th>
<th>Role Template</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>tt_live!t2464 (customers)</td>
<td>tt_live_TrackAndTrace_OnboardingAssistanceUser</td>
<td>tt_live_TrackAndTrace_OnboardingAssistanceUser</td>
</tr>
<tr>
<td>tt_demo!2464 (partners)</td>
<td>tt_live_TrackAndTrace_OnboardingAssistanceUser</td>
<td>tt_live_TrackAndTrace_OnboardingAssistanceUser</td>
</tr>
</tbody>
</table>

8. Then click Save.
8 CONFIGURE SAP CLOUD PLATFORM IDENTITY AUTHENTICATION SERVICE

SAP Cloud Platform supports SAML 2.0 identity providers. SAP Cloud Platform Identity Authentication Service is an SAML 2.0 identity provider. It is where the business users for SAP Cloud Platform are stored.

Note
If you want to configure an identity provider other than SAP Identity Authentication Service, please go to chapter 9.

With the purchase of SAP Logistics Business Network, global track and trace option, you have a subscription to the Identity Authentication tenant. You will receive an email with the subject line “Activate Your Account for SAP Cloud Platform Identity Authentication Service”. The email contains a link to the landing page of the administration console for Identity Authentication. You can confirm the registration of your first administrator user.

8.1 Create User Groups

Prerequisites
To create user groups, you need the administrator role or you must be assigned to the Manage Groups role of your SAP Cloud Platform Identity Authentication Service in the administration console.

Make sure you have activated your account for SAP Cloud Platform Identity Authentication Service by following the instructions in the email with the subject “Activate Your Account for SAP Cloud Platform Identity Authentication Service.”

Note
If the activation link in the email is invalid or already used, follow the advice in SAP note 2637748.

Context
A user group is a collection of users. User groups serve to create sets of users that have something in common. For example, users who work in the same department or users who have similar tasks in a company.

You will create a user group for Onboarding Administrators.

Procedure
Follow the procedure described in Create a New User Group to create the user group as follows.

<table>
<thead>
<tr>
<th>Name</th>
<th>Display Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>TT_ONBOARDING_ADMINS</td>
<td>TT_ONBOARDING_ADMINS</td>
</tr>
</tbody>
</table>
8.2 Create a New User

As a SAP Cloud Platform Identity Authentication Service administrator, you can create a new user in the administration console for SAP Cloud Platform Identity Authentication Service. The user can be assigned the necessary user groups to have access to relevant applications.

**Context**

You can create a new user to have the onboarding administrator role. Alternatively, you can use your current user to be the onboarding administrator role.

**Procedure**

To create a new user, please refer to Create a New User. If you do not want to create a new user, you can use your current user and skip this task.

8.3 Assign User Groups to a User

As an Identity Authentication tenant administrator, you can assign one or more user groups created for a specific tenant to a user using the administration console for Identity Authentication.

**Context**

- Assign the TT_ONBOARDING_ADMINS user group to a user to assign him/her the role: Onboarding Administrator.
- Assign the TT_DATA_PRIVACY_SPECIALIST user group to a user to assign him/her the role: DP&P specialist.
- Assign the TT_AUDITOR user group to a user to assign him/her the role: Audit specialist.

**Note**

The above roles can only be assigned to users in SAP Identity Authentication Service. The other GTT roles can be assigned in the Onboarding Assistance app (for Solution Administrator role) and the Manage GTT Users app (for other roles).

**Procedure**

To assign the user groups to the user, please refer to Assign Groups to a User.
8.4 Establish Trust and Federation with User Account and Authentication

To make use of your identity provider's user base you must first establish a mutual trust relationship with your SAML 2.0 identity provider. This configuration consists of two steps:

- Establish trust with the SAML 2.0 identity provider in your SAP Cloud Platform subaccount.
- Register your SAP Cloud Platform subaccount in the SAML 2.0 identity provider.

For SAP Logistics Business Network, global track and trace option, the SAML 2.0 identity provider is SAP Cloud Platform Identity Authentication Service.

Procedure

To establish the trust and federation, see the following:

Establish Trust and Federation with UAA Using SAP Cloud Platform Identity Authentication Service.

Note

As you follow this procedure, when you reach the part "Establish Trust with an SAML 2.0 Identity Provider in a Subaccount" note the following:

- Make sure you select the checkboxes: Show SAML Login Link on Login Page and Create Shadow Users During Login.
- Click the pencil icon beside SAP ID Service. Then in the dialog box, keep the status Active, and clear the Available for User Logon option.

This avoids an extra login window for accessing the global track and trace solution.

When you reach the part “Register SAP Cloud Platform Subaccount in the SAML 2.0 Identity Provider” note the following:

- In the step: “choose a name for the application that clearly identifies it as your new service provider”, choose the application name Global Track and Trace.
- In the step: "Choose SAML 2.0 Configuration and import the relevant metadata XML file", use the following link to download the metadata of your subaccount:
  https://<tenant_name>.authentication.eu10.hana.ondemand.com/saml/metadata

Where <tenant_name> is the subdomain name of your Cloud Foundry subaccount. To find this subdomain name, go to your Cloud Foundry subaccount.
8.5 Configure the Application Authentication
You need to configure the application authentication in SAP IAS and later maintain the credential in the GTT solution. The credential will be used for creating GTT users and sending invitation emails.

Procedure
1. Go to the SAP Cloud Platform Identity Authentication Service administration console.
2. Choose Application Resources Applications in the menu or the Application tile.
3. In the Applications pane, choose Global Track and Trace, which was created in the previous procedure “Establish Trust and Federation with User Account and Authentication”.
4. In the right pane, under API AUTHENTICATION, choose HTTP Basic Authentication.
5. Enter the password and choose Save. The user ID is generated automatically. Please record the user ID and password. You'll use them later.

8.6 Configure the System Authentication
You need to configure the system authentication in SAP IAS and later maintain the credential in the GTT solution. The credential will be used for editing GTT users and assigning user groups to users.

Procedure
1. Go to the SAP Cloud Platform Identity Authentication Service administration console.
2. Choose Users Authorizations Administrators in the menu or the Administrators tile.
3. Click Add and choose System.
4. Specify a name of the system, for example, GTT.
5. Click Save.
6. Choose Set Password and enter a valid password for the system. Please record the user ID and its password. You'll use them later.
7. Click Save.

8.7 Map Role Collection to User Group

Prerequisites
You have:
- configured the relevant SAP Cloud Platform Identity Authentication Service user groups and
- determined the mapping relationship of the role collections and the user groups.

Context
You map role collections to user groups so that users in that user group have access to the apps specified in the role collection.
We recommend that you map:
- one role collection to one user group
- the role collections and the user groups with the same name.
Procedure

1. To map the role collections and user groups, go to your SAP Cloud Platform Cloud Foundry subaccount.
2. In the left pane, choose Security \(\Rightarrow\) Trust Configurations. Click the name of the trust configuration you created before.
3. In the left pane, click Role Collection Mappings. Then click New Role Collection Mapping.
4. In the popup dialog box, select a role collection, and fill in the value as shown in the following table.
   - Role Collection: The role collections you configured before.
   - Value: The corresponding user groups in IAS configuration.

<table>
<thead>
<tr>
<th>Role Collection</th>
<th>Value (User Group)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TT_ONBOARDING_ADMINS</td>
<td>TT_ONBOARDING_ADMINS</td>
</tr>
</tbody>
</table>
5. Then click Save.
9 CONFIGURE THIRD-PARTY IDENTITY PROVIDER (OPTIONAL)

SAP Cloud Platform supports SAML 2.0 identity providers. If you want to use a different identity provider, for example, the identity provider your company uses, follow the instructions in this chapter. Note that even if you use a different identity provider, you still need SAP Identity Authentication Service as a media.

9.1 Add Your Identity Provider as the Corporate Identity Provider

To use your identity provider, SAP Identity Authentication Service is still necessary. You need the administrator role of your SAP Cloud Platform Identity Authentication Service in the administration console.

Context

Corporate identity provider provides user authentication to an application.

Procedure

To add a corporate identity provider, go to your SAP Identity Authentication Service Administration Console.

1. On the left pane, select Identity Providers and then select Corporate Identity Providers.
2. Then click +Add button, enter a name and click Save.
3. Select the identity provider you have created, choose SAML 2.0 Configuration and import the relevant metadata XML file. Save your changes.

   Note
   The relevant metadata is the metadata of your identity provider.

4. Choose Logout Redirect URL, enter the logout URL and click Save.

9.2 Establish Trust and Federation with User Account and Authentication

To make use of your identity provider’s user base, you must first establish a mutual trust relationship with your SAML 2.0 identity provider. This configuration consists of two steps.

- Establish trust with the SAML 2.0 identity provider in your SAP Cloud Platform subaccount.
- Register your SAP Cloud Platform subaccount in the SAML 2.0 identity provider

For the global track and trace option, the SAML 2.0 identity provider is SAP Cloud Platform Identity Authentication Service.
Procedure
To establish the trust and federation, see the following:
Establish Trust and Federation with UAA Using SAP Cloud Platform Identity Authentication Service.

Note
As you follow this procedure, when you reach the part “Establish Trust with an SAML 2.0 Identity Provider in a Subaccount” note the following:

- Make sure you select the checkboxes: Show SAML Login Link on Login Page and Create Shadow Users During Login.
- Click the pencil icon beside SAP ID Service. Then in the dialog box, keep the status Active, and clear the Available for User Logon option.
  This avoids an extra login window for accessing the global track and trace solution.

When you reach the part “Register SAP Cloud Platform Subaccount in the SAML 2.0 Identity Provider” note the following:

- In the step: “choose a name for the application that clearly identifies it as your new service provider”, choose as the application name Global Track and Trace.
- In the step: "Choose SAML 2.0 Configuration and import the relevant metadata XML file", use the following link to download the metadata of your subaccount:
  https://<tenant_name>.authentication.eu10.hana.ondemand.com/saml/metadata

Where <tenant_name> is the subdomain name of your Cloud Foundry subaccount. To find this subdomain name, go to your Cloud Foundry subaccount.
9.3 Set Default Identity Provider

After you add the corporate identity provider and configure the trust between SAP Cloud Platform and SAP Identity Authentication Service, you can select the default identity provider for your tenant.

Procedure

To select the default identity provider, go to SAP Identity Authentication Service Administration Console.

1. On the left pane, select Applications & Resources and then select Applications.
2. Choose the application you created in the section Establish Trust and Federation with User Account and Authentication.
3. Choose Conditional Authentication. You can select the corporate identity provider you created in the section Add Your Identity Provider as the Corporate Identity Provider as the default identity provider.

9.4 Map Role Collection to User Group

Prerequisites

You have:

- configured the relevant identity provider user groups and
- determined the mapping relationship of the role collections and the user groups.

Context

You map role collections to user groups so that users in that user group have access to the apps specified in the role collection.

We recommend that you map:

- one role collection to one user group
- the role collections and the user groups with the same name.

Procedure

1. Follow chapter 7.1 to create role collections as you need.
2. To map the role collections and user groups, go to your SAP Cloud Platform Cloud Foundry subaccount.
3. In the left pane, choose Security ➤ Trust Configurations. Click the Name of the trust configuration you created before.
4. In the left pane, click Role Collection Mappings. Then click New Role Collection Mapping.
5. In the popup dialog box, select Role Collection, and fill in the value as shown in the following table.
   - Role Collection: The role collections you configured before.
   - Value: The corresponding user groups in your corporate identity provider.

<table>
<thead>
<tr>
<th>Role Collection</th>
<th>Value (User Group)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TT_ONBOARDING_ADMINS</td>
<td>TT_ONBOARDING_ADMINS</td>
</tr>
</tbody>
</table>

6. Then click Save.
10 CREATE A TECHNICAL USER

Context
A technical user is a role but not a person, nor a business user. It is a token used by selected services to access the GTT solution and authenticate the connection between different systems, for example, the Cloud Foundry and Neo environments. But, as it’s implemented as a role, as all roles, it must be set up, for example assigned to a role collection. Further, after setup, the technical user must be registered for its company by a GTT solution administrator using the Manage GTT Users app.

Recommendation
The email address of the technical user must be unique. In particular, it must not be the same as other GTT users. We recommend you use a third-party email address and make sure that this email address is never registered by any GTT business user.

Procedure
1. To create a technical user, go to SAP.com: Registration.
2. Enter the necessary user information and click Register.
3. An activation email with the subject “Activate Your Account for SAP.com” will be sent to your email address. Click the activation link to activate the account.
4. On the profile page, please record your User ID starting with the letter P (P-ID). It will be used later.
11 MAINTAIN GENERAL SETTINGS IN ONBOARDING ASSISTANCE APP

To continue onboarding, you need to maintain tenant and identity authentication service information in the Onboarding Assistance app.

Note
A guided tour is provided in the Onboarding Assistance app. To start the guided tour, click the help icon at the top-right of the Onboarding Assistance app window.

Prerequisites
To maintain the information, you need to have the role Onboarding Administrator. That is, be assigned with the TT_ONBOARDING_ADMINS user group in the administration console of SAP Cloud Platform Identity Authentication Service.

Procedure
1. Log on to the SAP Cloud Platform cockpit.
2. Choose your global account and Cloud Foundry subaccount.
3. Choose Subscriptions.
4. Find the Solution Owner Apps for Global Track and Trace tile and click Go to Application.
5. Log on to the application using the user that is assigned to the “TT_ONBOARDING_ADMINS” user group.
6. On the SAP Fiori Launchpad, click the Onboarding Assistance app tile.
7. In the Global Track and Trace Tenant Information section, choose Edit. Then select the Tenant Role for your tenant in the dropdown list, and click Save. The Tenant Role is your purpose to create the tenant: Test or Productive.
8. In the SAP Identity Authentication Service section, choose Edit. Fill in the following and click Save.
   - the URL of your Identity Authentication Service administration console (the landing page of the administration console for Identity Authentication mentioned in the previous procedure "Configure SAP Cloud Platform Identity Authentication Service")
   - Application Authentication user ID and password (you have recorded in the previous procedure "Configure the Application Authentication")
   - System Authentication user ID and password (you have recorded in the previous procedure "Configure the System Authentication")

Result
Now the predefined user groups, role collections, and the mappings between them are automatically created. For detailed role collection/user groups list, see the Appendix "Default Role Collections and User Groups".
12 CONFIGURE THE NEO ENVIRONMENT FOR GLOBAL TRACK AND TRACE OPTION

This chapter describes how to configure the SAP Cloud Platform Cloud Foundry Neo environment.

After purchasing a license for SAP Logistics Business Network, global track and trace option, you get a Neo subaccount under your global account.

SAP Web IDE and SAP Business Rules service are provided in your SAP Cloud Platform Neo account while GTT metadata models are deployed in your SAP Cloud Platform Cloud Foundry environment subaccount. Therefore, a Security Assertion Markup Language (SAML) trust is required between the two subaccounts.

To connect to SAP Cloud Platform, you are required to establish a SAML trust between the Neo and Cloud Foundry environments. This involves completing configuration in the following three places:

<table>
<thead>
<tr>
<th>Trust between</th>
<th>Set up in</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Cloud Platform Neo environment subaccount and SAP Cloud Platform Identity</td>
<td>SAP Cloud Platform cockpit (Neo environment)</td>
</tr>
<tr>
<td>SAP Cloud Platform Identity and SAP Cloud Platform Neo environment subaccounts</td>
<td>SAP Cloud Platform Identity Authentication Administration Console</td>
</tr>
<tr>
<td>SAP Cloud Platform Cloud Foundry environment subaccount (or identity zone) and SAP Cloud Platform Neo environment subaccount</td>
<td>XS Advanced Administration (Cloud Foundry environment)</td>
</tr>
</tbody>
</table>

After the SAML trust is established between the Neo and Cloud Foundry environments, you then need to configure the solutions or services that you want to run on the Neo environment for use with SAP Logistics Business Network, global track and trace option. For example, configure SAP Web IDE and SAP Cloud Platform Business Rules service.

Related information: Regions and Hosts on SAP Cloud Platform

12.1 Prerequisites

To perform the tasks described in this chapter, you must have the following prerequisites:

- You are able to log on to the SAP Cloud Platform cockpit.
- You have administrator privileges for your Neo environment subaccount.
- You have the role of administrator for the SAP Cloud Platform Identity Authentication Service in the administration console.

For SAP Cloud Platform Business Rules service:

- You have a license for SAP Cloud Platform Business Rules service.
- You have a technical user [P-user] (already created, see Create a Technical User).
12.2 Configure SAP Cloud Platform Neo Subaccount

To use a custom identity provider (and not the default identity provider), you need to configure your SAP Cloud Platform Neo subaccount.

Procedure

1. Log on to the SAP Cloud Platform Cockpit.
2. Choose your global account and Neo subaccount.
4. Choose the Local Service Provider tab then do the following:
   a) Choose Edit.
   b) Change the Configuration Type from Default to Custom, click Generate Key Pair. The Signing Key and Signing Certificate values are generated.
   c) Enter a local provider name. You can enter your subaccount name. Note, keep the name to less than 20 characters to avoid issues later.
   d) Enter Enabled as the Principal Propagation value.
   e) Enter Disabled as the Force Authentication value.
   f) Choose Save.
   g) Choose Get Metadata and save the XML file. This file is needed for the tasks you perform in the administration console of the SAP Cloud Platform Identity Authentication service.

5. Choose the Application Identity Provider tab and perform the following tasks:
   a) Choose Add Trusted Identity Provider.
   b) Download the SAP Cloud Platform Identity Authentication tenant metadata by navigating to the following link:
   c) \https://<Identity_Authentication_Tenant_ID>.accounts.ondemand.com/saml2/metadata\ where <Identity_Authentication_Tenant_ID> is an ID automatically generated by the system. The first administrator created for the tenant receives an activation email with a URL in it. The URL contains the tenant ID.
   d) In the General tab, choose Browse and upload the identity authentication tenant metadata file that you just downloaded.
   e) In the Attributes tab, choose Add Assertion-Based Attribute. Enter Groups (case-sensitive) in the Assertion Attribute text box and in the Principal Attribute text box. Then choose Save.
12.3 Configure SAP Cloud Platform Authentication Service

Establish trust between SAP Cloud Platform Identity Authentication Service and your Neo subaccount, as follows:

Procedure
1. In a browser, navigate to the administration console of the SAP Cloud Platform Identity Authentication Service.
   Example URL: https://<Identity_Authentication_Tenant_ID>.accounts.ondemand.com/admin/
   <Identity_Authentication_Tenant_ID> is an automatically generated ID by the system. The first administrator created for the tenant receives an activation email with the URL of the administration console.
2. Add an application as follows:
   a) In the left pane, choose Applications under Applications & Resources.
   b) Choose + Add.
   c) Enter your subaccount name as the application name and choose Save. Your application is listed in the middle pane.
   d) Choose your application.
3. Choose SAML 2.0 Configuration and upload the XML file that you downloaded while configuring the custom identity provider (see Configure SAP Cloud Platform Neo Subaccount). Save your changes.
4. Choose the Subject Name Identifier, enter E-Mail as the value, and save your changes.
5. Add an assertion attribute as follows:
   a) Choose Assertion Attributes.
   b) Above the table, choose + Add.
   c) Add Groups as an attribute with value Groups (case-sensitive).
   d) Save your changes.
6. (Optional) If you are using an identity provider other than SAP Identity Authentication Service, choose Conditional Authentication and select the identity provider you created before.
12.4 Add SAP Cloud Platform Subaccount as a Trusted Application

Add the SAP Cloud Platform Neo subaccount as a trusted application in the Cloud Foundry environment as follows:

Procedure
1. Go to your Cloud Foundry subaccount in the SAP Cloud Platform.
2. In the left pane, select SecurityTrust ConfigurationNew Trust Configuration.
3. Change the XML file that you downloaded while configuring the custom identity provider (see Configure SAP Cloud Platform Neo Subaccount) as follows:
   a) Replace all SPSSO strings with IDPSSO.
   b) At the beginning of the XML file, add an XML declaration "<?xml version="1.0"?>".
4. In the Metadata field, upload the changed XML metadata.
5. Choose Parse.
6. In the Status box, select Active.
7. Clear the option Show SAML login link on login page.
8. Specify a name in the Name field.
9. Click Save.
10. Click the Trust Configuration you have created.
11. In the left page, click Role Collection MappingsNew Role Collection Mapping.
12. Select Role Collection: TT_SOLUTION_ADMINS, fill in the value TT_SOLUTION_ADMINS, and save the changes.
13. Click New Role Collection Mapping again. Then select Role Collection: TT_MODELING_EXPERT, fill in the value TT_MODELING_EXPERT, and save the changes.

The trust between SAP Cloud Platform Neo subaccount and Cloud Foundry subaccount is created.
12.5 Configure SAP Web IDE

Configure SAP Web IDE as follows:

1. Enable SAP Web IDE Full-Stack.
2. Import the Destination for the GTT Metadata Service.

12.5.1 Enable SAP Web IDE Full-Stack

Enable SAP Web IDE Full-Stack service and assign permissions to developers as follows:

Procedure

1. Log on to the SAP Cloud Platform Cockpit.
2. Choose your global account and Neo subaccount.
3. Go to Services -> SAP Web IDE Full-Stack and enable the service.
4. Go back to your Neo subaccount.
5. Go to Security -> Authorizations
   a) In the Groups tab, choose New Group to add a new group named WEBIDE_USERS and choose Save.
   b) Above the Roles table, choose Assign. Then in the Assign roles for group WEBIDE_USERS dialog box, select:
      • Subaccount: sapwebide EU2
      • Application: df
      • Role: DiDeveloper
   c) Then choose Save.
6. Go to Security -> Trust, and perform the following tasks.
   a) Choose the Application Identity Provider tab.
   b) Select the name of the identity provider that you added previously.
   c) In the Groups tab, choose Add Assertion-Based Group, and add the following (case-sensitive):

<table>
<thead>
<tr>
<th>Group</th>
<th>Mapping Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEBIDE_USERS</td>
<td>Groups equals TT_MODELING_EXPERT</td>
</tr>
</tbody>
</table>

d) Then choose Add Assertion-Based Group again, and add the following (case-sensitive):

<table>
<thead>
<tr>
<th>Group</th>
<th>Mapping Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEBIDE_USERS</td>
<td>Groups equals TT_SOLUTION_ADMINS</td>
</tr>
</tbody>
</table>

e) Choose Save.
12.5.2 Import the Destination for the GTT Metadata Service

You need to download the destination file in the onboarding assistance app and import the destination into the SAP Cloud Platform cockpit as follows:

**Procedure**

1. Log on to the SAP Cloud Platform Cockpit.
2. Choose your global account and Cloud Foundry subaccount.
3. Choose Subscriptions.
4. Choose the SAP Logistics Business Network, global track and trace option tile and click Go to Application.
5. Log on to the application using the user that is assigned to the user group: TT_ONBOARDINGADMINS.
   
   **Note**
   
   To find the user assigned to the user group TT_ONBOARDINGADMINS, go to the administration console of SAP Cloud Platform Identity Authentication by using the following URL. Then in the left pane, choose Users & Authorizations -> User Groups.
   
   Example URL: https://<Identity_Authentication_Tenant_ID>.accounts.ondemand.com/admin/.
   
   Where <Identity_Authentication_Tenant_ID> is an ID automatically generated by the system. The first administrator created for the tenant receives an activation email with the URL of the administration console.

6. Open Onboarding Assistance app and choose the tab System Integration.
8. In the SAP Cloud Platform cockpit, go to your Neo subaccount.
9. Choose Connectivity -> Destinations to open the Destinations editor.
10. Choose Import Destination and upload the Destination file you just downloaded.
11. Choose Save.
12.6 Configure SAP Cloud Platform Business Rules Service

**Note**
You need to configure the service only when you want to add business rules to your deployed GTT models.

Configure the business rules service as follows:

**Procedure**

1. You need a *P-user* to access the event-to-action engine APIs. This *P-user* provides basic authentication to access the following event-to-action engine APIs, such as the following:
   - https://bpmrulesrepository<<subaccountId>>.int.sap.hana.ondemand.com
   - https://bpmrulesruntime<<subaccountId>>.int.sap.hana.ondemand.com

2. Enable the *Rule Service* in the subaccount.
   a) In the subaccount page, click *Services*.
   b) Search for *Business Rules* and enable.

3. Configure user authorizations.
   a) Create a group *Business Rules*.
      In the subaccount, go to *Security Authorizations*, add a new group named *Business Rules*.
   b) Assign roles for group *Business Rules*.
      Select *Assign* and add two new roles as follows:

      | Subaccount | Application             | Role            |
      |------------|-------------------------|-----------------|
      | Rules      | bpmrulesrepository      | RuleSuperUser   |
      | Rules      | bpmrulesruntime         | RuleSuperUser   |

   c) Select the name of the group *Business Rules* to assign your technical user [*P-user*] to this group. You need the *PID (Person ID)* of your *P-user*. To find the *PID*, use the following URL: https://people.sap.com/manage
13 CONNECT TO SAP ERP

This chapter describes how to use SAP Cloud Platform Integration with the interfaces for SAP Logistics Business Network, global track and trace option to connect to SAP ERP.

These interfaces include:

- **Tracked Processes and Event Messages**
  
  To activate the configuration in the SAP ERP system for process and event tracking with SAP Logistics Business Network, global track and trace option.

- **ERP Master Data Replication**
  
  To integrate SAP ERP master data with SAP Logistics Business Network, global track and trace option. After executing all the steps described, you will be able to replicate the following data from the SAP ERP system to the GTT system:
  
  - Process data such as delivery orders and shipment documents
  - Event data such as Goods_Issue, Packing, Picking, and Load_Begin
  - Master data such as business partner and location

**Tracked Process and Event Messages**

To track a process, the following two types of messages can be triggered in the SAP ERP system:

- Extracted process data is sent with IDOC basic type EHPOST01 when creating and updating the data, to be processed for tracked processes in SAP Logistics Business Network, global track and trace option.

- Extracted event type data is sent with IDOC basic type EVMSTA02 when reporting the data, to be processed for tracked processes in SAP Logistics Business Network, global track and trace option.

In the SAP ERP system, the necessary customizing needs to be maintained to trigger the data extraction and create the IDOCs.

The IDOCs are sent to an SAP Cloud Platform Integration (SAP CI) tenant on which one integration flow has to be configured for each IDOC message type.

**ERP Master Data Replication**

The replication of master data is message-based using IDoc format. SAP ERP supports the following types of messages that represent business partners and locations:

- customer data that uses IDOC message type DEBMAS
- vendor data that uses IDOC message type CREMAS
- address data that uses IDOC message type ADRMAS
- product data that uses IDOC message type MATMAS

When sending data to the Master Data service through SAP Cloud Platform Integration PI, the outbound adapter is an HTTP adapter. Thus, for customer data and vendor data, both the method POST and the method PUT need to be maintained in the SAP ERP Master Data Replication package. There are seven process integration artifacts in the package:

- Replicate Customer from SAP ERP
- Replicate Vendor from SAP ERP
- Replicate Address from SAP ERP
- Replicate Product from SAP ERP
- Replicate Business Partner and Product from SAP ERP
- Replicate Location from SAP ERP
- Failed Logs
This process integration artifact generates an error report for iFlow messages. The report shows all iFlow message errors that occur during a specified time frame on a certain process integration artifact in the SAP ERP Master Data Replication package.

13.1 Prerequisites
To perform the tasks described in this chapter, you must have the following prerequisites:

**SAP ERP**
- You have a specified user in SAP ERP with the necessary roles.
- You have implemented SAP Note 2436001 and SAP Note 2475184 or installed the corresponding support packages. If you manually implement the SAP Notes, the IMG entries for SAP Logistics Business Network, global track and trace option will not be available.

For the sending messages from the SAP ERP system to SAP CI, you have implemented one of the following authentication methods:
- Basic authentication: the RFC user ID in your SAP ERP system has been registered as the SAP CI user ID and assigned appropriate authorization for sending messages. For more information, see Managing User Role Assignments.
- Client-certificate authentication: the client certificate in your SAP ERP system is signed by a certificate authority (CA) that is supported by SAP. For a list of all supported CAs, see Load Balancer Root Certificates Supported by SAP. For the procedure to generate a certificate request and send it to a CA, see Configuring SAP NetWeaver AS for ABAP to Support SSL.

**SAP Cloud Platform Integration PI**
- You have been provided with an SAP Cloud Platform Integration tenant.
- You have installed the Eclipse-based tools for SAP Cloud Platform Integration.

**SAP Logistics Business Network, global track and trace option**
You have a user with the necessary roles in the GTT system.

The following roles perform the stated activities:

<table>
<thead>
<tr>
<th>Role</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP ERP Consultant</td>
<td>• Configures the Sales and Distribution area of SAP ERP</td>
</tr>
<tr>
<td></td>
<td>• Configures integration with other SAP Components of SAP ERP</td>
</tr>
<tr>
<td>System Administrator</td>
<td>• Establishes a secure network connection between the SAP ERP system and</td>
</tr>
<tr>
<td></td>
<td>the GTT system</td>
</tr>
<tr>
<td></td>
<td>• Installs software</td>
</tr>
<tr>
<td>SAP Cloud Platform Integration</td>
<td>Configures the SAP Cloud Platform Integration</td>
</tr>
<tr>
<td>Consultant</td>
<td></td>
</tr>
<tr>
<td>Master Data Specialist</td>
<td>Creates the master data of business partners in non-English languages</td>
</tr>
</tbody>
</table>

13.2 Deploy SAP Cloud Platform Integration Content

13.2.1 Set up Certificate and Permissions
To enable a secure connection between the SAP ERP system and SAP Cloud Platform Integration, the certificates need to be configured correctly.
To establish a secure connection from the SAP ERP system to SAP Cloud Platform Integration, you must import the root certificate from SAP Cloud Platform Integration to the Trust Manager of the SAP ERP system.

**Procedure**

1. Open a web browser (such as Google Chrome) and enter the URL of your SAP Cloud Platform Integration (SAP CI) tenant. Open the Security tab (for example, press F12 in Google Chrome), click View certificate, click Details, and then click View certificate. The Certificate dialog box appears.
2. On the Certification Path tab, select the root certificate, such as “Baltimore CyberTrust Root”, and then click View Certificate. The Certificate dialog box of the root certificate appears.
3. On the Details tab, click Copy to File, and then save the certificate with the Base-64 encoded X.509 format. Now you have a copy of the root certificate.
4. Log on to the SAP ERP system, open the Trust Manager (transaction STRUST), and then open an SSL client. For the client-certificate authentication method, a CA signed client certificate should be added into the SSL client.
   - The CA must be supported by SAP. For a list of all supported CAs, see **Load Balancer Root Certificates Supported by SAP**.
5. In the Certificate area, click Import certificate, and then enter the directory where the copy of the root certificate is located in File Path.
6. Click Add to Certificate List and then save.

For the basic authentication method and the client-certificate authentication method with certificate-to-user mapping, make sure that the SAP CI user that is used to trigger calls from outside the middleware to SAP CI has the necessary permission for sending messages.

We recommend that you assign the following roles to the associated user.

- To enable access to the web tool, to monitor, to deploy integration iflows, or to deploy security content included in integration flows: AuthGroup.IntegrationDeveloper (Application: TMN)
- To enable monitoring and reading of the message payload (for example, MPL attachments): AuthGroup.BusinessExpert (Application: TMN)
- To enable monitoring, deploy integration iflows, or deploy security content on TMN-level (for example, keystores): AuthGroup.Administrator (Application: TMN)
- To enable a sender system to process messages on a tenant using HTTPS/basic authentication: ESBmessaging.send. (Application: IFLMAP)

For more information, see **Overview of Authorization Groups**

You must deploy a Java keystore (Type of JAVA_KEYSTORE, with extension .JKS) on your SAP CI PI tenant in the Eclipse-based tool. The keystore must contain the root certificate of SAP Logistics Business Network, global track and trace option, so that the GTT system can be identified as a trust server by the CI PI tenant. To generate a new tenant client keystore, see **Setting Up the Tenant Client Keystore**. We recommend that you contact SAP for Java keystore deployment.

**Authentication and Authorization (Inbound)**

Authentication and authorization options can be combined in a specific way for inbound communication of SAP CI PI.

<table>
<thead>
<tr>
<th>Authentication Option</th>
<th>Can Be Used with the Following Authorization Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic authentication</td>
<td>Role-based authorization</td>
</tr>
<tr>
<td></td>
<td>For this user, the authorizations are checked based on user-to-role assignments defined on the tenant. To authorize a sender system to process messages on a tenant, the role ESBmessaging.send has to be assigned to the associated user.</td>
</tr>
<tr>
<td>Client-certificate authentication and certificate-to-user</td>
<td>Role-based authorization</td>
</tr>
</tbody>
</table>
user mapping
The sender (client) authenticates itself against the server based on a digital client certificate. Furthermore, this certificate is mapped to a user (based on the information contained in a Certificate-to-User Mapping artifact deployed on the tenant).

| Option | For the user derived from the certificate-to-user mapping, the authorizations are checked based on user-to-role assignments defined on the tenant. To authorize a sender system to process messages on a tenant, the role ESBMessaging.send has to be assigned to the associated user.
| Client-certificate authentication (without certificate-to-user mapping) | Subject/Issuer DN authorization check of a certificate
| The sender (client) authenticates itself against the server based on a digital client certificate. | In a subsequent authorization check, the permissions of the sender are checked on the tenant by evaluating the distinguished name (DN) of the client certificate of the sender.

For more information, see Authentication and Authorization Options (Inbound). If you use client-certificate authentication, you must export the client certificate supported by SAP from the SAP ERP system. If you use client-certification and certificate-to-user mapping for authentication, you must define a certificate-to-user mapping in the SAP CI PI tenant. For more information, see Managing Certificate-to-User Mappings.

You must create valid credentials for your technical users of the GTT system on your SAP CI PI tenant. For more information, see Deploying and Editing a User Credentials Artifact.

### 13.2.2 Copy and Deploy Integration Content

**Procedure**

1. Access the SAP Cloud Platform Integration web-based application.
2. From the Discover page, locate your package and then click to navigate to the details page of the package.
   - package name for master data replication: Integration with SAP ERP – Master Data Replication
   - package name for process and event tracking: Integration with SAP ERP – Tracked Processes and Event Messages
3. Click Copy in the upper right corner of the screen and navigate to the Design page. You can also copy the same package into the workspace multiple times if you want to connect to more than one GTT tenant. To copy an existing package to your workspace, choose Create copy and then specify a unique suffix.
4. For each process integration, choose Actions > Configure, enter the value of the following parameters, and then save your settings.

<table>
<thead>
<tr>
<th>Table 3. Package and Parameter Values</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Package</strong></td>
</tr>
<tr>
<td>SAP ERP Master Data Replication</td>
</tr>
<tr>
<td>SAP ERP Master Data Replication</td>
</tr>
<tr>
<td>SAP ERP Master Data Replication</td>
</tr>
<tr>
<td>---------------------------------</td>
</tr>
<tr>
<td>Process and event tracking (artifact: Create or Update Tracked Processes)</td>
</tr>
<tr>
<td>Process and event tracking (artifact: Create or Update Tracked Processes)</td>
</tr>
<tr>
<td>Process and Event Tracking (artifact: Create or Update Tracked Processes)</td>
</tr>
<tr>
<td>Process and Event Tracking (artifact: Send Event Message)</td>
</tr>
<tr>
<td>Master Data/Process and Event Tracking</td>
</tr>
<tr>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Master Data/Process and Event Tracking</td>
</tr>
<tr>
<td>SAP ERP Master Data Replication</td>
</tr>
<tr>
<td>SAP ERP Master Data Replication</td>
</tr>
<tr>
<td>SAP ERP Master Data Replication</td>
</tr>
<tr>
<td>SAP ERP Master Data Replication</td>
</tr>
<tr>
<td>SAP ERP Master Data Replication</td>
</tr>
<tr>
<td>SAP ERP Master Data Replication</td>
</tr>
</tbody>
</table>

5. Deploy the integration contents in the package.
6. After you deploy the Failed Logs artifact, the system generates a message processing log in the Operation view of the SAP Cloud Platform Integration web-based application. This message processing log contains an error report (a JSON attachment) for iflow messages. You can check the error count, artifact ID, error message, and attachments in the report.

### 13.2.3 Monitor Integration Content

You use the web-based SAP CI monitor application to check if the integration contents have been deployed and started successfully. For more information, see Web-Based Monitoring.

Additionally, you can check the status of messages in the web-based SAP CI monitor application.

### 13.2.4 Endpoint URL

The integration processes for master data replication and process and event messaging are triggered by the SAP ERP system. Therefore, SAP ERP has to know the endpoint URL that is used to connect in SAP Cloud Platform Integration.

To view the endpoint URL in SAP Cloud Platform Integration, proceed as follows:
Procedure

1. Go to Integration Content Monitor > Manage Integration Content.
2. Click the integration content to which you need to send messages.

Results

If it is deployed and started successfully, you can see the endpoint URL. The URL follows this pattern: //<runtime URL of your SAP Cloud Platform Integration environment>//cxf//<address>

The address is the Address field that you specified under the Sender tab of the integration content configuration.

13.3 Settings in the ERP System

This section describes the SAP ERP system settings which are required for activating a specific visibility process, and for establishing communication between SAP ERP and SAP CI.

Note

Before you make these settings, ensure that you have activated the application system interface for SAP Logistics Business Network, global track and trace option for process and event tracking. In the standard system, the application interface is inactive when shipped. Therefore, the relevant BAdIs and BETs are not called.

To activate the application interface for process and event tracking in the SAP ERP system, you must set the PI-EM indicator using transaction BF11.

Procedure

1. Set up communication with SAP CI PI.
2. Set up delta replication scheduling for master data replication.
   This setting is NOT needed for process and event tracking.
3. Define the SAP Cloud Platform Integration tenant for SAP Logistics Business Network, global track and trace option.
   This setting is NOT needed for master data replication.
4. Define application object types and event types.
   This setting is NOT needed for master data replication.

For SAP S/4HANA, you must activate SAP Master Data Governance (MDG) to ensure the scenarios for data replication. For more information about MDG, visit the following website: http://help.sap.com/mdg

13.3.1 Set up Communication with SAP Cloud Platform Integration PI

To set up communication with SAP Cloud Platform Integration PI, you must complete the steps outlined in this section.

- Define Logical Systems
- Create RFC Destinations
- Assign Message Types to IDOC Types
- Create Ports for IDoc Processing
- Create Partner Profiles
- Define Distribution Model
- Define Technical Settings for Business Systems for S/4HANA
- Define Replication Model for S/4HANA
You have various options to orchestrate RFC destinations, ports, partner profiles, and distribution models. For details, see Appendix 1 – Communication Setup Variations.

Define Logical Systems

For master data replication, you need to define two logical systems, with one representing the receiver that receives business partner data, and the other representing the receiver that receives location data. If you are also implementing process and event tracking, you can share either of the logical systems.

Procedure

1. Transaction: SALE > Basic Setting > Logical System > Define Logical System.
3. On the New Entries: Overview of Added Entries screen, enter the required fields.
4. Choose Save.

Create RFC Destinations

In the SAP ERP system, the following four RFC destinations need to be created for master data replication:
- endpoint that receives IDOC DEBMAS06 to replicate customers
  URL endpoint can be found on SAP CI in iFlow with ID com.sap.tnt.md.customerCreation
- endpoint that receives IDOC CREMAS06 to replicate vendors
  URL endpoint can be found on SAP CI in iFlow with ID com.sap.tnt.md.vendorCreation
- endpoint that receives IDOC ADRMAS03 to replicate addresses
  URL endpoint can be found on SAP CI in iFlow with ID com.sap.tnt.md.addressReplication
- endpoint that replicates locations
  URL endpoint can be found on SAP CI in iFlow with ID com.sap.tnt.md.locationReplication
- endpoint that replicates products
  URL endpoint can be found on SAP CI in iFlow with ID com.sap.tnt.md.productReplication

Alternatively, if you are using the "Replicate Business Partner and Product from SAP ERP" artifact, you only need to create two RFC destinations for master data replication.
- endpoint that replicates business partners and products
  URL endpoint can be found on SAP CI in iFlow with ID com.sap.tnt.md.masterdataReplication
- endpoint that replicates locations
  URL endpoint can be found on SAP CI in iFlow with ID com.sap.tnt.md.locationReplication

For more information about process integration artifacts, see Connecting to SAP ERP.

The following two RFC destinations need to be created for process and event tracking (posting tracked processes and sending event messages):
- endpoint that receives IDOC EHPOST01 to post tracked processes
  URL endpoint can be found on SAP CI in iFlow with ID com.sap.tnt.core.processMessaging
- endpoint that receives IDOC EVMSTA02 to send event messages
  URL endpoint can be found on SAP CI in iFlow with ID com.sap.tnt.core.eventMessaging

Before completing to the following procedure, you may need to configure proxy settings, depending on how the SAP ERP system is set up.

Procedure

2. Select HTTP Connections to External Server and then choose Create.
3. On the RFC Destination screen, enter the following settings:
   - RFC Destination: the name of RFC destination.
   - Connection Type: G.
On the **Technical Settings** tab:
- If the endpoint URL is `https://<runtime URL of your SAP CI environment>/cxf/<address>`:
  - **Target Host**: `<runtime URL of your SAP CI environment>`
  - **Service No.**: 443
  - **Path Prefix**: `/<address>`
- Where address is the **Address** field that you specified under the **Sender** tab of the integration content configuration.

On the **Login & Security** tab:
- **Logon Procedure > Logon with User**: For basic authentication, choose **Basic Authentication**, enter the user credentials which is also registered in SAP CI. For client-certificate authentication, choose **Do Not Use a User**.
- **Logon Procedure > Logon with Ticket**: Keep the default value **Do Not Send Logon Ticket**.
- **Logon Procedure > Security Options > Status of Secure Protocol**: choose Active in SSL and choose the SSL certificate created previously.

4. Choose **Save**.

### Results

After saving, you can execute a connection test. If the setup is correct, you will get a response with HTTP code 500.

**Assign Message Types to IDOC Types**

Message types and IDOC types are used for sending application object types and event messages. You must assign message types to IDOC types.

### Procedure

1. Transaction: WE82.
2. Enter the following new entry:

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Type</td>
<td>AOPOST</td>
</tr>
<tr>
<td>Basic Type</td>
<td>EHPOST01</td>
</tr>
<tr>
<td>Release</td>
<td>741</td>
</tr>
</tbody>
</table>

3. Enter the following new entry:

<table>
<thead>
<tr>
<th>Field</th>
<th>Entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Type</td>
<td>EVMSTA</td>
</tr>
<tr>
<td>Basic Type</td>
<td>EVMSTA02</td>
</tr>
<tr>
<td>Release</td>
<td>46C</td>
</tr>
</tbody>
</table>

4. Save the new entries.

### Create Ports for IDoc Processing

A port is a channel by which the SAP ERP system can exchange data with SAP Cloud Platform Integration PI. This means you create a port of the XML HTTP type, which uses the RFC connection you previously created. Therefore, you must create four ports for the master data replication and three ports for process and event tracking.

### Procedure

2. Select **XML_HTTP** and choose **Create**.
3. On the Ports in IDoc processing screen, enter the following settings:
   - Port: the name of the port
   - Description: description of the port
   - RFC Destination: use the RFC destination you previously created.
   - Content Type: choose Application/x-sap.idoc
   - Select the SOAP Protocol checkbox

4. Choose Save.

Create Partner Profiles

You must create a partner profile for each logical system you previously created. If you are implementing both master data replication and process and event tracking, the two can share one partner profile.

- For the partner profile to replicate business partner data, add DEBMAS, CREMAS, ADRMAS, and MATMAS to the outbound parameters. The receiver ports are the corresponding ports for the RFC destination of sap.tnt.md.customerCreation, sap.tnt.md.vendorCreation, sap.tnt.md.addressReplication, and sap.tnt.md.productReplication.
- For the partner profile to replicate location data, add DEBMAS, CREMAS, and ADRMAS to the outbound parameters. The receiver port is the same port for the RFC destination of sap.tnt.md.locationReplication.

If you are also implementing process and event tracking, add the message types AOPOST and EVMSTA to outbound parameters depending on the logical system you choose to share.

Procedure

2. Select Partner Type LS and choose Create.
3. On the Partner Profiles screen, enter the following settings:
   - Partner No.: the logical system that you defined in the previous step.
   - Partn. Type: LS.
   - On the Post processing: permitted agent tab:
     - Ty.: User
     - Agent: The ERP user with necessary roles
     - Language: EN
4. Choose Save.
5. In the Outbound parameters section, select Create outbound parameter.
6. For the partner profile, enter the following settings:
7. CREMAS (Message type for creating and updating vendors):
8. Message Type: CREMAS
   - On the Outbound Options tab:
     - Receiver Port: the port you created for the corresponding RFC destination
     - Output mode: choose Pass IDoc Immediately.
     - IDoc Type: in Basic type, enter CREMAS06
     - Select the Cancel Processing After Syntax Error checkbox

   - DEBMAS (Message type for creating and updating customers):
     - Message Type: DEBMAS
     - On the Outbound Options tab:
       - Receiver Port: the port you created for the corresponding RFC destination
       - Output mode: choose Pass IDoc Immediately.
       - IDoc Type: in Basic type, enter DEBMAS06
       - Select the Cancel Processing After Syntax Error checkbox

   - ADRMAS (Message type for creating and updating addresses):
     - Message Type: ADRMAS
     - On the Outbound Options tab:
       - Receiver Port: the port you created for the corresponding RFC destination
       - Output mode: choose Pass IDoc Immediately.
       - IDoc Type: in Basic type, enter ADRMAS03
MATMAS (Message type for creating and updating products):
- Message Type: MATMAS
- On the **Outbound Options** tab:
  - Receiver Port: the port you created for the corresponding RFC destination
  - Output mode: choose **Pass IDoc Immediately**.
  - IDoc Type: in Basic type, enter MATMAS05
  - Select the **Cancel Processing After Syntax Error** checkbox

AOPOST (Message type for creating and updating tracked processes):
- Message Type: AOPOST
- On the **Outbound Options** tab:
  - Receiver Port: the port you created for the corresponding RFC destination
  - Output mode: choose **Pass IDoc Immediately**.
  - IDoc Type: in Basic type, enter EHPOST01
  - Select the **Cancel Processing After Syntax Error** checkbox

EVMSTA (Message type for sending event messages):
- Message Type: EVMSTA
- On the **Outbound Options** tab:
  - Receiver Port: the port you created for the corresponding RFC destination
  - Output mode: choose **Pass IDoc Immediately**.
  - IDoc Type: in Basic type, enter EVMSTA02
  - Select the **Cancel Processing After Syntax Error** checkbox

9. Choose **Save**.

---

**Define Distribution Model**

You need to define a distribution model to connect the logical systems you have created.
- For the distribution model to replicate business partner data, add DEBMAS, CREMAS, MATMAS, and BAPI AddressOrg.SaveReplica.
- For the distribution model to replicate location data, add DEBMAS, CREMAS, and BAPI AddressOrg.SaveReplica.

If you are also implementing process and event tracking for business partners and locations, add AOPOST or EVMSTA to outbound parameters (depending on the logical system you choose to share).

**Procedure**

1. Transaction: BD64
2. Switch to edit mode.
3. Choose **Create Model View**.
4. On the **Create Model View** screen, enter the following settings:
   - Short text: short text description for the distribution model
   - Technical name: technical name for the distribution model
5. Choose **Continue**.
6. In the Distribution Model list, select the distribution mode you created, choose **Add Message Type**.
7. On the **Add Message Type** screen, enter the corresponding settings:
   - For sending customers:
     - Sender: the logical system created for the SAP ERP system
     - Receiver: the logical system created for SAP CI
     - Message Type: DEBMAS
   - For sending vendors:
     - Sender: the logical system created for the SAP ERP system
     - Receiver: the logical system created for SAP CI
     - Message Type: CREMAS
   - For sending products:
Define Technical Settings for Business Systems for S/4HANA

Procedure

1. Enter transaction code DRFIMG and then navigate to Define Custom Settings for Data Replication > Define Technical Settings > Define Technical Settings for Business Systems.
2. To define a new business system and maintain the logical system for the receiving systems, choose New Entries.
3. In the Logical System field, enter the logical system name used for IDoc communication. In the RFC Destination field, enter the RFC destination to be used for RFC communication with the receiver system.
4. Select the entry and click Define Bus. Systems, BOs.
5. Create a new entry:
   - For customers, In the BO Type field enter the business object type 159.
   - For vendors, In the BO Type field enter the business object type 266.
6. Select each entry and then double-click Define Bus. Systems, BOs, Communication Channel. Table Define Bus. Systems, BOs, Communication Channel must contain an entry for the IDoc replication. If you cannot find an entry, create a new one. Select the entry containing "Communication Channel: Replication via IDoc". In the Key Harm. column, select Harmonized IDs.

Define Replication Model for S/4HANA

Procedure

1. Enter transaction code DRFIMG and then navigate to Replication > Define Custom Settings for Data Replication > Define Replication Models.
2. Choose Define Replication Model > New Entries.
3. Enter the replication model name and its description.
4. Click to highlight the line and then choose Assign Outbound Implementation.
5. Create a new entry:
   - For customers, In the Outb. Impl. field enter 159_2.
   - For vendors, In the Outb. Impl. field enter 266_2.
6. Select each line and then double-click Assign Target System for Repl. Model/Outb.Impl. Create a new entry and enter the business system name for the receiving system created previously.
8. Locate the newly created replication model and choose **Activate**.

### 13.3.2 Set up Delta Replication Scheduling for Master Data

To schedule delta replication for master data, you must complete the following steps. These steps are not required for process and event tracking.

**Enable Change Pointers (General)**

**Procedure**

2. On the **Activate Change Pointers Generally** screen, select **Change pointers activated-generally**.

**Enable Change Pointers**

**Procedure**

2. On the **Activate Change pointers for Message Type** Overview screen, select **DEBMAS, CREMAS, ADRMAS**, and **MATMAS**.

**Create Variant of IDOC from Change Pointers**

You must create a variant for IDOC MATMAS.

**Procedure**

2. On the **Creating IDoc Type from Change Pointer** screen, enter the message type MATMAS.
3. Choose **Goto > Variant > Save as Variant**.
4. On the **Variant Attributes** screen, enter the values for **Variant Name** and **Description**.
5. Choose **Save**.

**Create Variant of Serialization Group from Change Pointers**

You must create two variants, one for the serialization group (GRP_DEBMAS_ADR) and the other for the serialization group (GRP_CREMAS_ADR).

**Procedure**

2. On the **Generate IDocs for Serialization Group From Change Pointers** screen, enter the corresponding serialization groups. For customer and address, enter GRP_DEBMAS_ADR. For vendor and address, enter GRP_CREMAS_ADR.
3. Choose **Goto > Variant > Save as Variant**.
4. On the **Variant Attributes** screen, enter the values for **Variant Name** and **Description**.
5. Choose **Save**.
Schedule Delta Distribution

You need to create three scheduling jobs; two for the serialization groups, and the other for message type MATMAS.

Procedure

2. On the Define Background Job screen, enter the value for Job Name.
3. Choose Step.
4. On the Create Step 1 screen, enter the following settings:
   In the ABAP program:
   - For the two serialization groups
     - Name: RBDSER01
     - Variant: the variant you created for the serialization group GRP_DEBMAS_ADR or GRP_CREMAS_ADR in the previous step.
   - For message type MATMAS
     - Name: RBDMIDOC
     - Variant: the variant you created for the message type MATMAS in the previous step.
5. Choose Save.
6. Choose Back and return to the Define Background Job screen.
7. Choose Start Condition.
8. On the Start Time screen, choose Immediate, select the Periodic Job checkbox, and then choose Period Values.
9. On the Period Values screen, enter the scheduling period value. For example, set 2 minutes for the period value. By doing this, the system will send out messages to inform you about the business partners actions, such as the create and update operations, every two minutes.
10. Choose Save, and then go back to the Define Background Job screen.
11. Choose Save.
12. Use transaction SM37 to monitor the scheduled and completed job runs.

13.3.3 Define the SAP Cloud Platform Integration Tenant for Global Track and Trace

To define the SAP Cloud Platform Integration tenant for SAP Logistics Business Network, global track and trace option in SAP ERP, proceed as follows.

Procedure

1. In Customizing, choose Integration with Other SAP Components > Interface to Global Track and Trace > Define Application Interface > Define CI Tenant for Global Track and Trace.
   Transaction: /SAPTRX/ASC0TS_CTT
2. Choose New Entries.
3. Enter the following data:

<table>
<thead>
<tr>
<th>Field</th>
<th>User Actions and Default Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Track and Trace Tenant</td>
<td>Specify the SAP Cloud Platform Integration tenant For example: CIV0387</td>
</tr>
<tr>
<td>CI Log. System</td>
<td>Specify the logical system for the SAP Cloud Platform Integration tenant, as maintained For example: CIV0387</td>
</tr>
<tr>
<td>Global Track and Trace Version</td>
<td>Global Track and Trace</td>
</tr>
<tr>
<td>Description</td>
<td>Provide a description for your SAP Cloud Platform Integration tenant for the GTT system</td>
</tr>
</tbody>
</table>
4. Save your entries.
13.3.4 Define Application Object Types and Event Types

Application object types determine whether a business process or an object is relevant for tracking in SAP Logistics Business Network, global track and trace option, that is, whether a tracked process instance in the GTT system should be created or not. Moreover, the data to be extracted for creating planned events, parameters, and tracking IDs is also defined here. Several application object types can be assigned to one business process type. These are then processed according to their priority and transferred to the GTT system.

Event types determine whether a change to a business process or an object (or parts of it), is relevant to tracking in the GTT system, that is, whether an event message instance should be created for this change. Several event types can be assigned to one business process type. These are then processed according to their priority and transferred to the GTT system.

In the following procedure, the OBP10_DELIV scenario is used as an example for the settings that need to be made regarding application object types and event types. The extractors used in the example need to be enhanced if you want to use them with the template tracked process type com.sap.gtt.app.delivery.DeliveryProcess in SAP Logistics Business Network, global track and trace option. See SAP Note 2462159 regarding further details about what needs to be enhanced by custom coding.

Procedure

1. In Customizing for SAP ECC, choose Integration with Other SAP Components > Interface to Global Track and Trace > Define Application Interface > Define Used Bus. Proc. Types, Appl. Obj. Types, and Evt Types
   Transaction: /SAPTRX/ASC0AO_CTT
   The BPT Process Mode of the business process type that you choose must be Active.
   The business process type for the example scenario to track outbound deliveries is ESC_DELIV. The application object type OBP10_DELIV and the event types OBP10_PICK and OBP10_GI are used in the example scenario.
2. Select the business process type ESC_DELIV.
3. Choose Define Application Object Types and then select OBP10_DELIV.
4. Choose Details.
   On the General Data tab:
   o In the HCI for GTT field, select the appropriate CI ID which was previously created using transaction /SAPTRX/ASC0TS_CTT and will be used for the connection to the GTT system.
   o Select GTT Relevance of Appl. Obj.
5. Choose Define Event Types and then select OBP10_PICK and OBP10_GI.
6. Choose Details.
   o In the HCI for GTT field, select the appropriate CI ID which was previously created using transaction /SAPTRX/ASC0TS_CTT and will be used for the connection to the GTT system.
   o Select GTT Relevance of Event Type.
7. Save your entries.

Next Steps
   o See SAP Note 2462159 for further details about the custom enhancements that need to be implemented for tracking outbound deliveries with the template tracked process type com.sap.gtt.app.delivery.DeliveryProcess in the Global Track and Trace option.
   o See SAP Note 2463015 for a detailed list of the IDOC segments and fields per segment of the IDOC types EHPOST01 and EVMSTA02 that are supported for the integration with the Global Track and Trace option. This is very important if you create your own custom extraction function modules.
13.4 Load Master Data

You can integrate customer, vendor, and product master data from your SAP ERP system with SAP Logistics Business Network, global track and trace option.

- You first complete an initial load of the data by sending it from your SAP ERP system to the logical system you have defined.
- When delta replication is scheduled, the delta load of data occurs automatically as customer, vendor, and product master data is updated

13.4.1 Initial Load

To integrate SAP ERP master data with SAP Logistics Business Network, global track and trace option, you first need an initial load of the business partner, location, and product master data.

Send Customers

Procedure

2. On the Send Customers screen, enter the range of the customers’ IDs, choose DEBMAS in Output type, and choose the logical system that represents SAP Cloud Platform Integration PI for initial load in Logical system.
3. Choose Execute.

Send Vendors

Procedure

5. On the Send Vendor screen, enter the range of the vendors’ IDs, choose CREMAS in Message type, and then choose the logical system that represents SAP Cloud Platform Integration PI for initial load in Target system.
6. Choose Execute.

13.4.2 Delta Load

When delta replication scheduling is complete, subsequent changes to business partner, location, or product data (such as creation or update), automatically trigger message sending of business partners, locations, and products to the SAP CI integration flows.

Use these transactions to create or change business partner, location, and product master data:

Table 4. Master Data Tasks and Transactions

<table>
<thead>
<tr>
<th>Task</th>
<th>Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new customer</td>
<td>XD01</td>
</tr>
<tr>
<td>Change an existing customer</td>
<td>XD02</td>
</tr>
<tr>
<td>Create a new business partner (vendor)</td>
<td>XK01</td>
</tr>
<tr>
<td>Change an existing business partner (vendor)</td>
<td>XK02</td>
</tr>
<tr>
<td>Create a new product</td>
<td>MM01</td>
</tr>
<tr>
<td>Change an existing product</td>
<td>MM02</td>
</tr>
</tbody>
</table>
13.5 Create Master Data in Multiple Language Versions

You can create the master data of business partners and locations (for both customers and vendors) in a non-English language. To do this, click International Versions when you are creating or updating the master data and select an activated version. You can then enter the information in the selected language version.

To activate or deactivate the language versions, use transaction SA09. Additionally, you can use transaction SM30 to create new entries in the V_SAPTSADV view.

Related Information

For more information on international address versions, see SAP Note 316331.
To finish onboarding, you need to maintain system integration information in Onboarding Assistance app.

Note
A guided tour is provided in the Onboarding Assistance app. To start the guided tour, click the help icon at the top-right of the Onboarding Assistance app window.

Prerequisites
To maintain the information, you need to have the role Onboarding Administrator. That is, be assigned with the TT_ONBOARDING_ADMINS user group in the administration console of SAP Cloud Platform Identity Authentication Service.

Procedure
1. Log on to the SAP Cloud Platform cockpit.
2. Choose your global account and Cloud Foundry subaccount.
3. Choose Subscriptions.
4. Find the Solution Owner Apps for Global Track and Trace tile and click Go to Application.
5. Log on to the application using the user that is assigned to the “TT_ONBOARDING_ADMINS” user group.
6. On the SAP Fiori Launchpad, click to open the Onboarding Assistance app.
7. Choose the System Integration tab.
8. In the SAP Cloud Platform Business Rules section, choose Edit. Fill in the URLs and the technical user and password.
   To find the URLs, go to the Neo subaccount under your global account in SAP Cloud Platform Cockpit.
   - bpmrulesrepository URL: In the left pane, choose Connectivity à Destinations. The URL for the destination bpmrulesreposity.
   - bpmrulesruntime URL: In the left pane, choose Connectivity à Destinations. The URL for the destination bpmrulesreposity.
   - Email and password: The email account with password of the technical user you previously created in the step “Create a Technical User”.
9. Click Save.
10. (Optional) In the SAP Cloud Platform Integration Forwarding section, choose Edit. Enter the user and password for logging on to SAP Cloud Platform Integration and click Save.
   The settings are required only when you want to add the ActionCPIForwarding business rules to GTT models. This type of business rules is used to forward the business data from SAP Logistics Business Network, global track and trace option to SAP Cloud Platform Integration. When the data forwarding happens, the user credential you maintain here will be used.
11. (Optional) In the Email Notification – Rule Action section, choose Edit. Fill in the Sender Email, Sender Name, and Reply-To Email. Then click Save.
   The settings are required only when you want to add the ActionEmailNotification business rules to GTT models. This type of business rules is used to send emails to users when certain conditions are met. When such emails are sent, the sender name, sender email, and reply-to email you maintain here will be used.
15 ONBOARD SOLUTION ADMINISTRATOR

Prerequisites
To onboard a solution administrator, you need to be assigned with the TT_ONBOARDING_ADMINS user group in the administration console of SAP Cloud Platform Identity Authentication Service.

Background
The Solution Administrator is the main administrator of the GTT solution and has the most authorizations of all roles. The activities he/she can perform are listed in the following table.

<table>
<thead>
<tr>
<th>Role</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solution Administrator</td>
<td>• Register all types of users for a solution</td>
</tr>
<tr>
<td></td>
<td>• Assign/change the business roles of all types of users</td>
</tr>
<tr>
<td></td>
<td>• Remove from the solution all types of user that have not been activated</td>
</tr>
<tr>
<td></td>
<td>• Lock or unlock any user from the solution</td>
</tr>
</tbody>
</table>

Procedure
To add a solution administrator:
1. Log on to the SAP Cloud Platform cockpit.
2. Choose your global account and Cloud Foundry subaccount.
3. Choose Subscriptions.
4. Find the Solution Owner Apps for Global Track and Trace tile and click Go to Application.
5. Log on to the application using a user that is assigned with the “TT_ONBOARDING_ADMINS” user group.
6. On the SAP Fiori Launchpad, click to open the Onboarding Assistance app and choose the Solution Owner Company Settings tab.
7. In the Company Information section, choose Edit, fill in the company name and email of your company, and click Save.
8. In the Solution Administrators section, click the + icon to assign a solution administrator. Fill in the email, first name, and last name of the user. Then click OK.

Results
An invitation email is sent to the email address of the solution administrator you assigned. When the invitation email is received, the recipients must click the link in the email to confirm their participation. After the confirmation, the contact person can then navigate to the web page of SAP Cloud Platform Identity Authentication Service to activate the account on SAP Logistics Business Network, global track and trace option. The person is then the solution administrator of their tenant.

Note that there is a default time limit of 28 days for recipients of the email to accept the invitation by clicking the link. If the time limit is exceeded, the user should go to the SAP Global Track application, choose the Log On button, and then the Forgot Password? link. This will trigger the Forgot Password process and the user will receive an email to reset his or her password.

Or, you can send the reset password email to the user following this link.

Note
Different SAP solutions share a common Identity Authentication Service tenant. If the solution administrator user already got an account in SAP Identity Authentication Service, he/she won't receive the invitation email. The user can log on to the GTT solution using his/her account with the corresponding password used in other SAP products.
16 MAINTAIN THE TECHNICAL USER FOR YOUR COMPANY

16.1 Assign Role Collections to the Technical User

Context
SAP ID service provides identity service to the technical user. It is used as an identity provider service for creating users and user groups. For each tenant (that is, for each customer using the platform services) there is a dedicated SAP ID service instance.

Procedure
1. To assign the role collections to the technical user, go to the Cloud Foundry subaccount in SAP Cloud Platform.
2. Click Security: Trust Configuration. Click the default trust configuration SAP ID Service. Search the technical user (you have created one in the previous procedure "Create a Technical User") in the E-Mail Address box.
3. When there is a pop-up dialogue box saying, “To see and assign role collections, you must first add <Email address of your technical user> as a user of identity provider SAP ID Service.”. Click Add User.
4. Click Assign Role Collection. Add TT_SOLUTION_ADMINS to the user.

16.2 Maintain Technical User

Prerequisites
A solution administrator of a GTT solution can maintain a technical user for his/her company.

Procedure
1. Log on to the SAP Cloud Platform cockpit.
2. Choose your global account and Cloud Foundry subaccount.
3. Choose Subscriptions.
4. Find the Solution Owner Apps for Global Track and Trace tile and click Go to Application.
5. Click the Manage GTT Users tile to open the app.
6. Click the Manage Technical Users icon on the upper right of the page.
7. Fill in the email address of your technical user.
8. Click Save.

Recommendation
The email address of the technical user must be unique. In particular, it must not be the same as other GTT users. We recommend you use a third-party email address and make sure that this email address is never registered by any GTT business user.
17 FREQUENTLY ASKED QUESTIONS

1. What is the next step after I complete all the tasks described in the onboarding guide?
   At the end of onboarding, you, as an onboarding administrator, create the role of solution administrator. This passes the relay baton to the solution administrator. To proceed, the solution administrator will then follow the instructions in the administration guide.

2. I assigned a user as a solution administrator, but the user didn't receive an activation email. Why?
   Different SAP solutions share a common Identity Authentication Service tenant. The user may already have an account in SAP Identity Authentication Service. In that case, ask the user to log on to the GTT solution using his/her account with the corresponding password used in other SAP products.

3. Do I need a standalone Cloud Foundry subaccount for global track and trace option?
   Yes, we recommend that you use a standalone Cloud Foundry subaccount.

4. May I have multiple Cloud Foundry subaccounts subscribing to SAP Logistics Business Network, global track and trace option?
   - If you are a GTT customer, your license provides you with two subscriptions to SAP Logistics Business Network, global track and trace option. Once you have subscribed twice, any further attempt to subscribe will fail.
   - If you are a GTT partner, your license provides you with one subscription to SAP Global Track and Trace. If you have already subscribed, any further attempt to subscribe will fail.

5. Why does my subscription to global track and trace option fail?
   Subscription failure can be caused by various reasons. You may have met the subscription quantity limit; or, you may try to re-subscribe right after you’ve unsubscribed. If that’s the case, we recommend that you wait and re-subscribe at least 30 minutes after your unsubscribing.

6. Why do I need two types of subaccounts, the Cloud Foundry subaccount and the Neo subaccount?
   A GTT solution is an application deployed on the Cloud Foundry environment. Its dependent services, SAP Web IDE and SAP Business Rules, run on the Neo environment. So, we need two types of subaccounts for these apps and services.

7. Why do I need a Neo subaccount?
   GTT solution depends on services SAP Web IDE and SAP Business Rules. These two services are on the Neo environment. Besides, a Neo subaccount is the prerequisite to using SAP IAS as the identity provider.

8. Can I use the same Neo subaccount for GTT solution and other products?
   Yes.

9. What is a technical user?
   A technical user is not a person. It is used to enable the connection between different systems.

10. Can I use the same technical user for different services?
    Yes.
11. Can I set a user account to log on to the GTT system using the same email address as that of a technical user?

If an email address has already been used as a user account to log on to the GTT system. Can I still use this email address to register a technical user?

We highly recommend that you use different email addresses to register GTT users and technical users. SAP IAS is the identity provider for GTT users while SAP ID Service serves as the identity provider for technical users.

12. Can I use any service other than SAP Identity Authentication Service as the identity provider?

Yes. See Configure Third-party Identity Provider (Optional).

13. If I have an existing SAP IAS tenant, can I use it for my GTT solution?

Yes.

14. GTT solution has different user roles. Where should I assign those roles to users?

See the table below.

<table>
<thead>
<tr>
<th>Service or App</th>
<th>User Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Identity Authentication Service</td>
<td>Onboarding Administrator, Audit Specialist, DP&amp;P specialist</td>
</tr>
<tr>
<td>GTT Onboarding Assistance app</td>
<td>Solution Administrator</td>
</tr>
<tr>
<td>GTT Manage GTT Users app</td>
<td>Roles other than the ones we mention in first two rows</td>
</tr>
</tbody>
</table>

15. What if I don't enable the SAP Web IDE service?

You must enable the SAP Web IDE service. GTT solution is a model-driven application. The system relies on the SAP Web IDE plugin to deploy models.

16. What if I don't enable SAP Business Rules?

It depends. If you don’t use any rule-driven features, you can skip enabling SAP Business Rules. However, if you rely on rule-driven features, enabling SAP Business Rules is a must.
18 APPENDIX

SAP Logistics Business Network, global track and trace option has roles, role collections and user groups. You need to configure these after you finish the onboarding process. This appendix describes how to maintain roles in SAP Cloud Platform Cloud Foundry subaccount and lists the default roles, role collections and user groups.

18.1 Maintain Roles

Roles define the type of access granted to an application.

Context

A role is an instance of a role template, which defines the type of access permitted for an application. You build a role based on a role template and assign the role to a role collection.

Procedure

1. In the SAP Cloud Platform Cockpit, go to the Cloud Foundry subaccount that you created.
2. In the left pane, click Subscriptions.
3. Click Solution Owner Apps for Global Track and Trace.
4. In Application Configuration, click Manage Roles.
   You'll see the default roles that have been predefined. You can create more roles to fit your use case.
5. Click New Role.
6. Specify a Name, a Description (optional), select a Template, and then fill in the Attributes.
7. Click Save.

18.2 Default Roles, Templates and Attributes

For a list of all the default roles, templates and attributes, refer to the User Management by Solution Administrators section in the Administration guide.
## 18.3 Default Role Collections and User Groups

The following table shows the default mappings between role collections and user groups:

<table>
<thead>
<tr>
<th>Role Collection/ User Group</th>
<th>Description</th>
<th>Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>TT_AUDITOR</td>
<td>for administrators who need to view the information of all users</td>
<td>tt_live_Auditor</td>
</tr>
<tr>
<td>TT_DATA_PRIVACY_SPECIALIST</td>
<td>for administrators who manage the personal data of users</td>
<td>tt_live_DataPrivacySpecialist</td>
</tr>
<tr>
<td>TT_DELIVERY_BP</td>
<td>for users who have the administrator role for shipment-related models (solution participants)</td>
<td>TT_Delivery_BP</td>
</tr>
<tr>
<td>TT_DELIVERY_SO</td>
<td>for users who have the administrator role for shipment-related models (solution owner)</td>
<td>TT_Delivery_SO</td>
</tr>
<tr>
<td>TT_LOCAL_ADMIN_GROUP</td>
<td>for users who have the administrator role for business user management</td>
<td>tt_live_TrackAndTrace_LocalAdmin</td>
</tr>
<tr>
<td>TT_MASTERDATA_SPECIALIST</td>
<td>Master Data Specialist is a template role to provide additional authorization for master data management. By default, this role only allows user access to the Master Data Management apps.</td>
<td>tt_live_MasterDataSpecialist</td>
</tr>
<tr>
<td>TT_MODELING_EXPERT</td>
<td>a template role to provide additional authorization for metadata modeling, model management and rule authoring. By default, this role only allows user access to the Metadata Modeling and GTT Model Management apps.</td>
<td>tt_live_ModelingExpert</td>
</tr>
<tr>
<td>TT_ONBOARDING_ADMINS</td>
<td>for users who have the technical role, onboarding administrator</td>
<td>tt_live_TrackAndTrace_Onboarding AssistanceUser</td>
</tr>
<tr>
<td>TT_PURCHASEORDER_BP</td>
<td>for users who have the administrator role for purchasing-related models (solution participant)</td>
<td>TT_Purchaseorder_BP</td>
</tr>
<tr>
<td>TT_PURCHASEORDER_SO</td>
<td>for users who have the administrator role for purchasing-related models (solution owner)</td>
<td>TT_Purchaseorder_SO</td>
</tr>
<tr>
<td>TT_SHIPMENT_BP</td>
<td>for users who have the administrator role for shipment-related models (solution participant)</td>
<td>TT_Shipment_BP</td>
</tr>
<tr>
<td>TT_SHIPMENT_SO</td>
<td>for users who have the administrator role for shipment-related models (solution owner)</td>
<td>TT_Shipment_SO</td>
</tr>
<tr>
<td>TT_SOLUTION_ADMINS</td>
<td>for solution administrators who have the administrator role for master data and business partner management</td>
<td>tt_live_TrackAndTrace_BucketOwner</td>
</tr>
<tr>
<td>TT_USER_GROUP</td>
<td>for business users who need access to the business apps</td>
<td>tt_live_TrackAndTrace_AppUser tt_live_TrackAndTrace_IntegrationUser</td>
</tr>
</tbody>
</table>

### Notes
1. Role Collection and User Group are the counterpart concept in the relevant system:
   - Role collection is used in SAP Cloud Platform.
   - User group is used in SAP Identity Authentication Service.
2. The roles for each role collection are the standardized configuration. You can also organize the role according to your own requirements.
APPENDIX 1 – COMMUNICATION SETUP VARIATIONS

This section introduces variations for how you set up communication with SAP Cloud Platform Integration PI.

Variation 1

- Use the following integration artifacts to replicate business partners and products.
  - Replicate Customer from SAP ERP
  - Replicate Vendor from SAP ERP
  - Replicate Address from SAP ERP
  - Replicate Product from SAP ERP
- Event and process tracking is wrapped into the same partner profile with the four artifacts above.
- Use the Replicate Location from SAP ERP artifact to replicate locations.

Variation 2

- Use the following integration artifacts to replicate business partners and products.
  - Replicate Customer from SAP ERP
  - Replicate Vendor from SAP ERP
  - Replicate Address from SAP ERP
  - Replicate Product from SAP ERP
- Use the Replicate Location from SAP ERP artifact to replicate locations.
- Event and process tracking is wrapped into the same partner profile with the one for locations.
Variation 3

- Use the Replicate Business Partner and Product from SAP ERP artifact to replicate business partners and products.
- Event and process tracking is wrapped into the same partner profile with the one for business partners and products.
- Use the Replicate Location from SAP ERP artifact to replicate locations.

Variation 4

- Use the Replicate Business Partner and Product from SAP ERP artifact to replicate business partners and products.
- Use the Replicate Location from SAP ERP artifact to replicate locations.
- Event and process tracking is wrapped into the same partner profile with the one for locations.