CONFIDENTIAL

Onboarding Guide for SAP BTP Configuration

SAP Entitlement Management

Document Version: 1.0

TABLE OF CONTENTS

DOCUMENT HISTORY

The table provides an overview of changes from the last 12 months, with the most recent changes at the top.

Document Version	Date of Update	Change
1.0	Oct 27, 2021	Initial version

1. TECHNICAL SETUP

Once you’ve received an email from SAP welcoming you to **SAP Entitlement Management**, you can start with the first steps.

> ⓘ The technical setup includes the creation of a tenant. Only users with an **Administrator** role for the global account can create tenants. At first, only the recipients of the welcome email have this role. If someone else needs to create a tenant, one of the email recipients must add the relevant user as **Administrator** for the global account. This is described in the section Add administrators to global account.

1.1 Check Successful Completion of Provisioning

Log on to the SAP BTP cockpit to check that **SAP Entitlement Management** is available for your account.

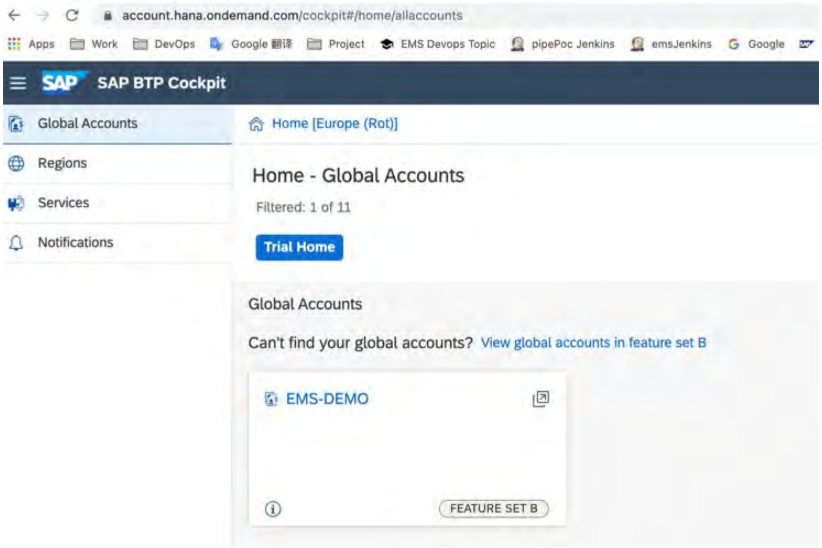
<table>
<tr>
<td>1. Log on to the SAP BTP cockpit using the link in your Welcome email or useeither of these URLs:</td>
<td>

- https://account.hana.ondemand.com
- A logon URL in the region closest to you (to avoid latency). See Regions and API Endpoints Available for the Cloud Foundry Environment in the SAP BTP documentation.

</td>
</tr>
<tr>
<td>2. Open the <b>global account</b> that was used to order <b>SAP Entitlement Management</b>.

ⓘ To find the right global account, you can use the System & Provisioning dashboard in SAP for Me (log on with your S-user ID). In the dashboard, you can find the global account ID under <i>System Name & Number</i>.

ⓘ In this guide, we use “EMS-DEMO” as the example account.</td>
<td>



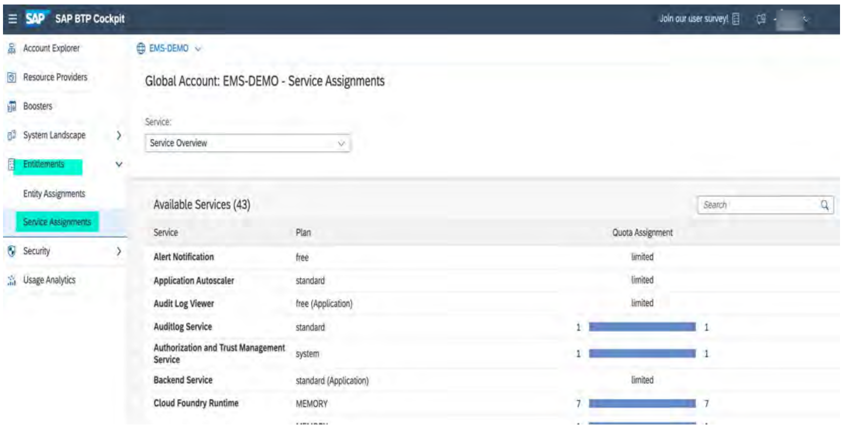
Home - Global Accounts

Filtered: 1 of 11

Global Accounts

Can't find your global accounts? View global accounts in feature set B

</td>
</tr>
<tr>
<td>3. Choose <b>Entitlements → Service Assignments</b> in the navigation panel.</td>
<td>



Global Account: EMS-DEMO - Service Assignments

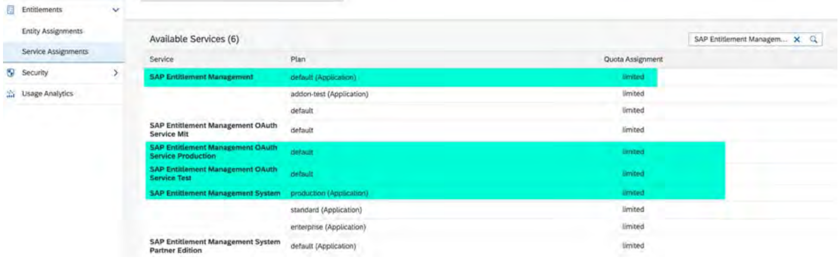
Service: Service Overview

Available Services (43)

<table>
<tr><th>Service</th><th>Plan</th><th>Quota Assignment</th></tr>
<tr><td>Alert Notification</td><td>free</td><td>limited</td></tr>
<tr><td>Application Autoscaler</td><td>standard</td><td>limited</td></tr>
<tr><td>Audit Log Viewer</td><td>free (Application)</td><td>limited</td></tr>
<tr><td>Auditlog Service</td><td>standard</td><td>1 1</td></tr>
<tr><td>Authorization and Trust Management Service</td><td>system</td><td>1 1</td></tr>
<tr><td>Backend Service</td><td>standard (Application)</td><td>limited</td></tr>
<tr><td>Cloud Foundry Runtime</td><td>MEMORY</td><td>7 7</td></tr>
</table>

</td>
</tr>
<tr>
<td>4. In the service overview, search for <b>SAP Entitlement Management</b>.

If the service isn’t displayed, please report this to your local SAP contact or create an BCP incident for component “<b>LOD-EMS</b>”.</td>
<td>



Available Services (6)

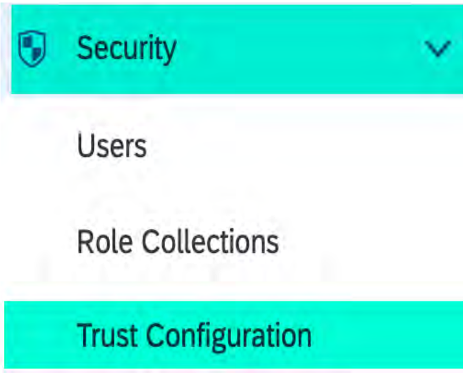
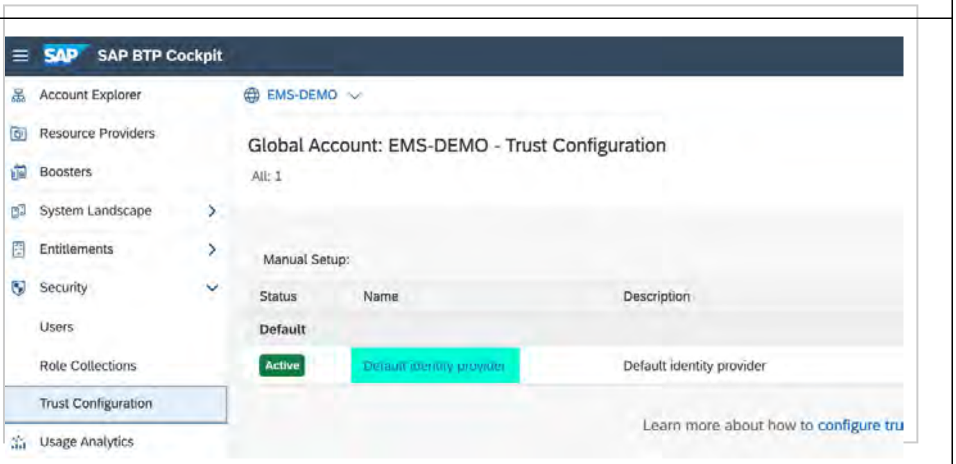
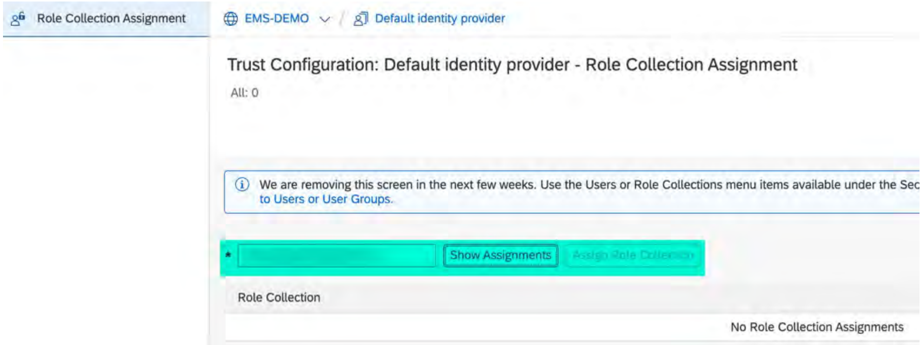
<table>
<tr><th>Service</th><th>Plan</th><th>Quota Assignment</th></tr>
<tr><td>SAP Entitlement Management</td><td>default (Application)</td><td>limited</td></tr>
<tr><td></td><td>addon-test (Application)</td><td>limited</td></tr>
<tr><td></td><td>default</td><td>limited</td></tr>
<tr><td>SAP Entitlement Management OAuth Service Mit</td><td>default</td><td>limited</td></tr>
<tr><td>SAP Entitlement Management OAuth Service Production</td><td>default</td><td>limited</td></tr>
<tr><td>SAP Entitlement Management OAuth Service Test</td><td>default</td><td>limited</td></tr>
<tr><td>SAP Entitlement Management System</td><td>production (Application)</td><td>limited</td></tr>
<tr><td></td><td>standard (Application)</td><td>limited</td></tr>
<tr><td></td><td>enterprise (Application)</td><td>limited</td></tr>
<tr><td>SAP Entitlement Management System Partner Edition</td><td>default (Application)</td><td>limited</td></tr>
</table>

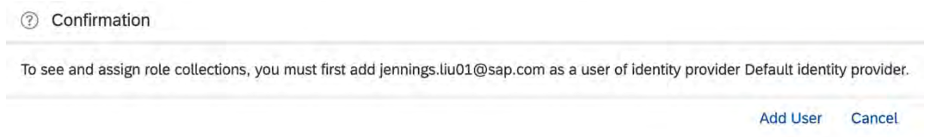
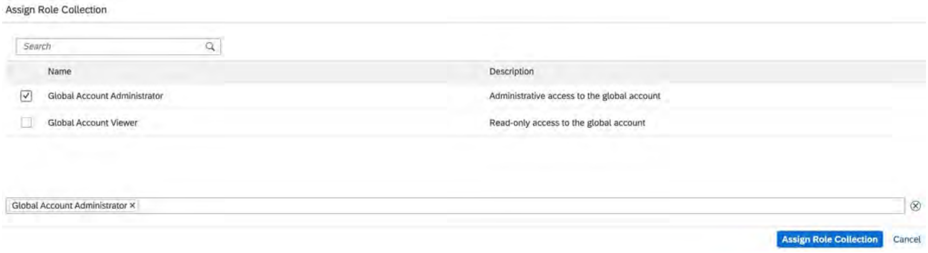
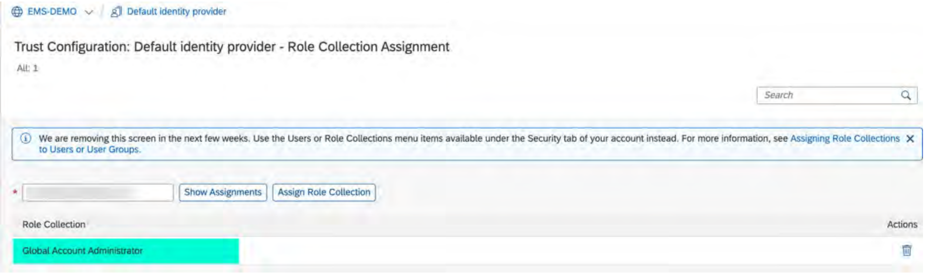
</td>
</tr>
</table>

1.2 Add Administrators to the Global Account

To enable further users to create a tenant, one of the recipients of the Welcome email must add the relevant user as a global account **Administrator**. You add administrators by assigning them a predefined role collection.

> ⓘ For more information on the default role collections for administrators, see Role Collections and Roles inGlobal Accounts and Subaccounts [Feature Set B] in the SAP BTP documentation.

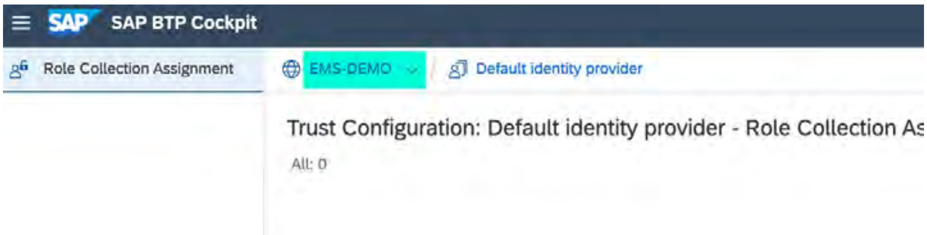
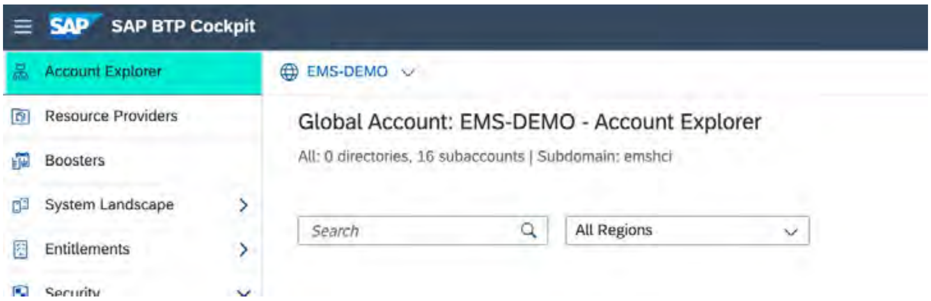
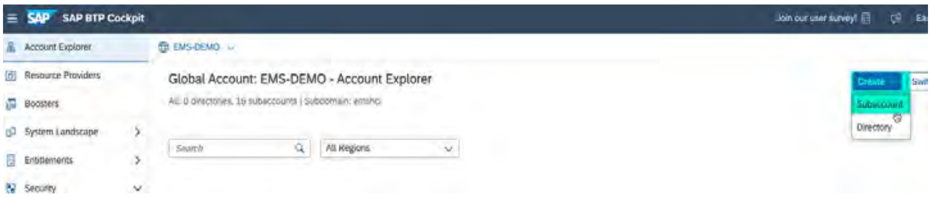
1. In your global account, select **Security →** **Trust Configuration** in the navigation panel.	 Security Users Role Collections Trust Configuration
2. Select the default identity provider.	 SAP SAP BTP Cockpit Account Explorer Resource Providers Boosters System Landscape Entitlements Security Users Role Collections Trust Configuration Usage Analytics EMS-DEMO Global Account: EMS-DEMO - Trust Configuration All: 1 Manual Setup: Status · Name · Description Default Active · Default identity provider · Default identity provider Learn more about how to configure tru
3. You're now in the screen **Role Collection Assignment** of the identity provider. Enter the email address of the user that you want as a global account member and select **Show Assignments**. You see that no role collections are assigned, and the button **Assign Role Collection** is enabled.	 Role Collection Assignment EMS-DEMO / Default identity provider Show Assignments Assign Role Collection Trust Configuration: Default identity provider - Role Collection Assignment All: 0 ⓘ We are removing this screen in the next few weeks. Use the Users or Role Collections menu items available under the Sec to Users or User Groups. Role Collection No Role Collection Assignments

4. <u>Optional</u>: If the user isn't part of the identity provider, you're asked to add the user after selecting **Show Assignments**. Confirm this action.	 Confirmation To see and assign role collections, you must first add jennings.liu01@sap.com as a user of identity provider Default identity provider.
5. Select **Assign Role Collection**. In the dialog, choose the role collection **Global Account Administrator** and confirm the assignment.	 Assign Role Collection Search Name | Description ☑ Global Account Administrator | Administrative access to the global account □ Global Account Viewer | Read-only access to the global account Global Account Administrator ×
6. Now the user should be able to complete configuration tasks.	 EMS-DEMO Default identity provider Trust Configuration: Default identity provider - Role Collection Assignment All: 1 Search We are removing this screen in the next few weeks. Use the Users or Role Collections menu items available under the Security tab of your account instead. For more information, see Assigning Role Collections to Users or User Groups. Show Assignments Assign Role Collection Role Collection | Actions Global Account Administrator

1.3 Create Subaccounts

Subaccounts on SAP BTP are required for deploying applications and using services. When you create a subaccount and subscribe to **SAP Entitlement Management**, a tenant is created.

> ⓘ You need to create one subaccount for each tenant to which you are entitled. Repeat the steps below to create each subaccount.

1. In the breadcrumb menu, select the name of your global account.	 SAP BTP Cockpit Role Collection Assignment EMS-DEMO Default identity provider Trust Configuration: Default identity provider - Role Collection As All: 0
2. You are returned to the **Trust Configuration** screen. In the navigation panel, select **Account Explorer**.	 SAP BTP Cockpit Account Explorer Resource Providers Boosters System Landscape Entitlements Security EMS-DEMO Global Account: EMS-DEMO - Account Explorer All: 0 directories, 16 subaccounts | Subdomain: emshci Search All Regions
3. Select **Create →** **Subaccount.**	 SAP BTP Cockpit Join our user survey! Account Explorer Resource Providers Boosters System Landscape Entitlements Security EMS-DEMO Global Account: EMS-DEMO - Account Explorer All: 0 directories, 16 subaccounts | Subdomain: emshci Search All Regions Create Subaccount Directory

4. Define the subaccount:

   1. Specify a **display name** and short **description**.

      ⓘ In this guide, we use “SAP-DEMO-SUBACC01” as the example subaccount.

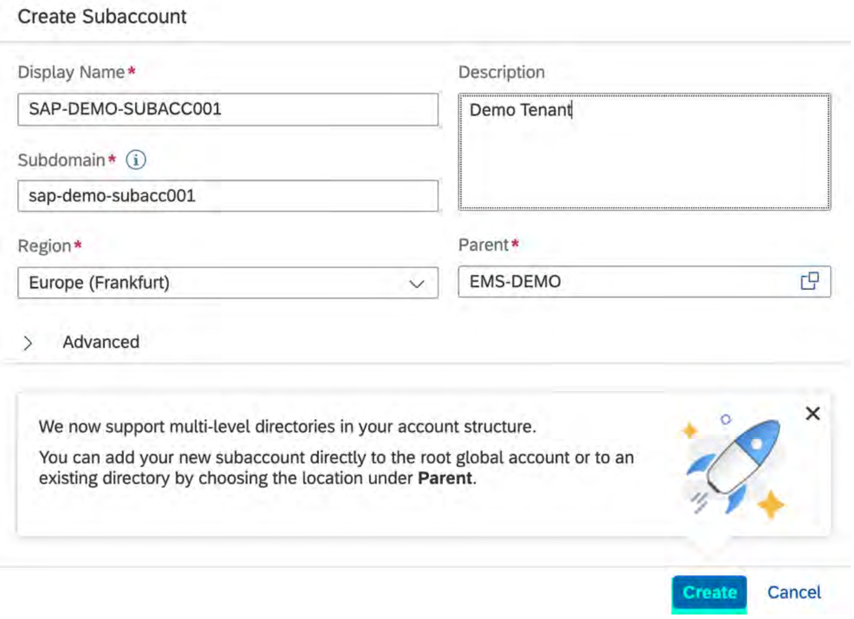
   2. In the **Region** list, scroll to the provider “Amazon Web Services (AWS)” and select your region:
      a. Europe (cf-eu10)
      b. US East (cf-us10)
      c. APJ (cf-ap11)

      Or provider “Microsoft Azure”
      and select region:
      a. US West(WA) (cf-us20)

   3. Enter a name for your **subdomain**.
      ⚠Please read the note beneath the screenshot that explains why this name should be chosen carefully.

   4. For productive subaccounts, don’t select **Enable beta features**.

   5. Select **Create.**



Create Subaccount

Display Name*: SAP-DEMO-SUBACC001

Description: Demo Tenant

Subdomain* ⓘ: sap-demo-subacc001

Region*: Europe (Frankfurt)

Parent*: EMS-DEMO

> Advanced

We now support multi-level directories in your account structure.

You can add your new subaccount directly to the root global account or to an existing directory by choosing the location under **Parent**.

⚠ The **subdomain** is the **tenant name** used for login. Once defined, you can’t change it later.

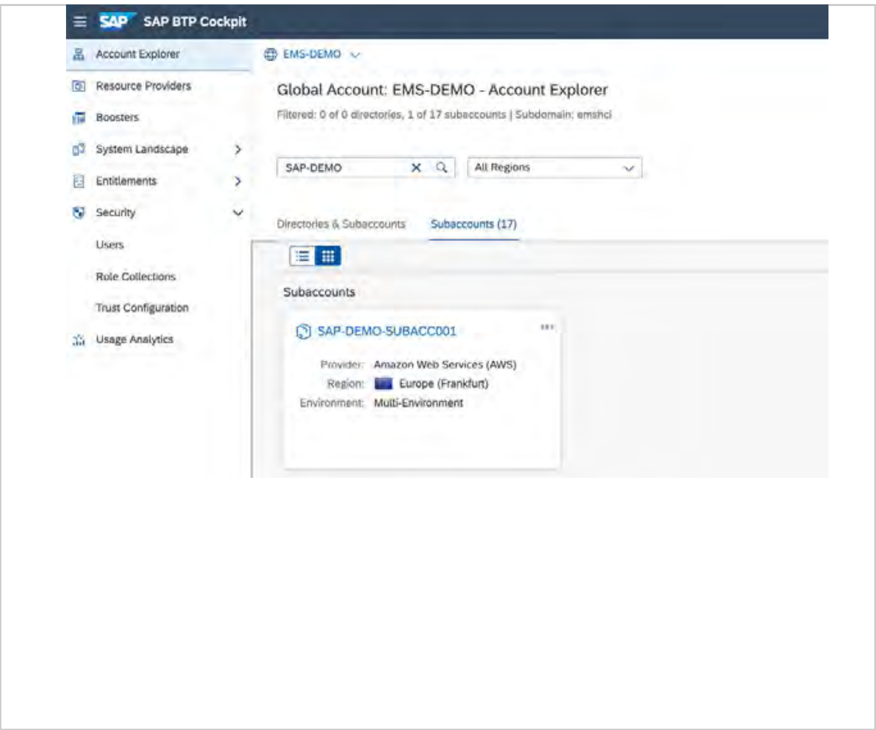
The subdomain also becomes part of the application URL for SAP Entitlement Management according to this pattern:
<subdomain>.ems.cfapps.<region>.hana.ondemand.com

The subdomain can contain only letters, digits, and hyphens. Hyphens aren’t allowed in the beginning or at the end. The subdomain must be unique across all accounts inthe same region of the Cloud Foundry environment of SAP BTP.

You can use upper case and lower case letters; however, they can’t be used to differentiate subdomains (“SUBDOMAIN” and “subdomain” are considered the same).

5. You see a tile for your subaccount on the **Subaccounts** tab. Wait for the “Onboarding” status to finish before accessing the subaccount.

ⓘ You are automatically assigned to the subaccount as administrator.



Global Account: EMS-DEMO - Account Explorer

Filtered: 0 of 0 directories, 1 of 17 subaccounts | Subdomain: emshci

SAP-DEMO

All Regions

Subaccounts

SAP-DEMO-SUBACC001

Provider: Amazon Web Services (AWS)
Region: Europe (Frankfurt)
Environment: Multi-Environment

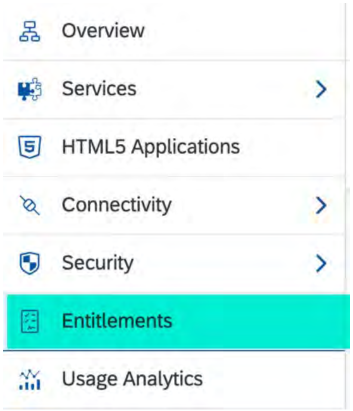
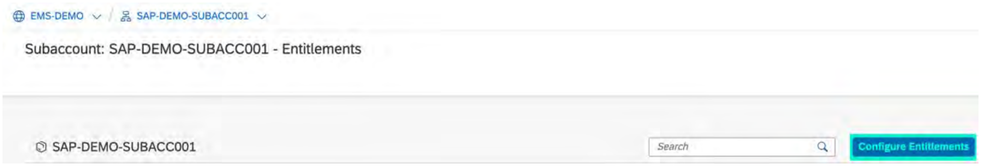
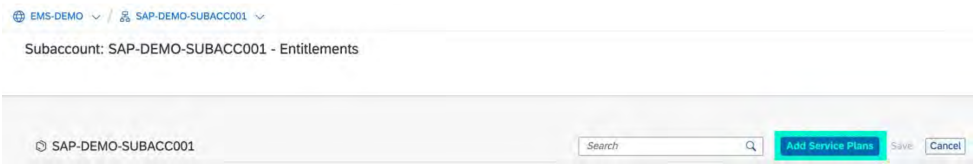
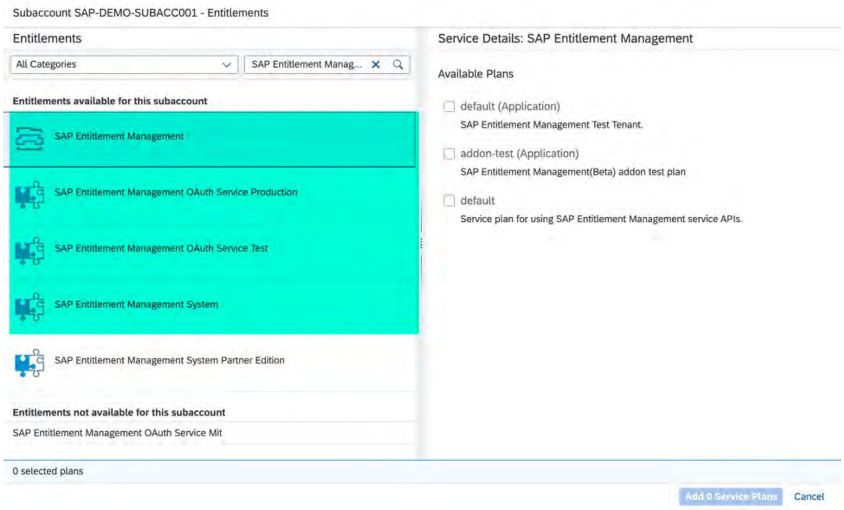
1.4 Assign Entitlements

You need to assign entitlements if you want to use **SAP Entitlement Management** and its APIs.

Your SAP BTP global account has entitlements to use resources, such as services and memory. You distribute quotas of these entitlements to your individual subaccounts (tenants) to define the maximum consumption for each subaccount.

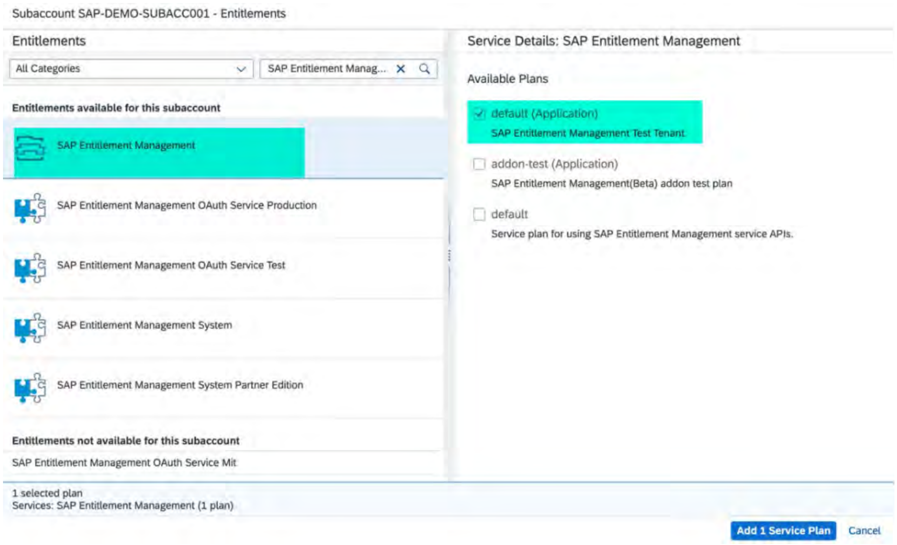
> ⓘ You have a total of three entitlements to distribute across a maximum of three tenants: two test tenants and one production tenant. The table below shows the tenant quota plan mapping.

Tenant Type	**Application/API Plan**
Dev/Test/QA/Sandbox Tenant	SAP Entitlement Management – default SAP Entitlement Management OAuth Service Test – default
Production Tenant	SAP Entitlement Management System – production SAP Entitlement Management OAuth Service Production – default
Addon Test Tenant	SAP Entitlement Management – addon-test SAP Entitlement Management OAuth Service Test – default

1. In your subaccount, select **Entitlements** in the navigation panel.	 Overview Services HTML5 Applications Connectivity Security Entitlements Usage Analytics
2. You see the table of subaccount assignments and service plans. Select **Configure Entitlements**.	 EMS-DEMO / SAP-DEMO-SUBACC001 Subaccount: SAP-DEMO-SUBACC001 - Entitlements SAP-DEMO-SUBACC001 Search Configure Entitlements
3. To open the list of resources that you're entitled to use, select **Add Service Plans**.	 EMS-DEMO / SAP-DEMO-SUBACC001 Subaccount: SAP-DEMO-SUBACC001 - Entitlements SAP-DEMO-SUBACC001 Search Add Service Plans Save Cancel
4. Search for **SAP Entitlement Management**. You will see both services for the application and for the OAuth API.	Subaccount SAP-DEMO-SUBACC001 - Entitlements Entitlements **Entitlements available for this subaccount** SAP Entitlement Management SAP Entitlement Management OAuth Service Production SAP Entitlement Management OAuth Service Test SAP Entitlement Management System SAP Entitlement Management System Partner Edition **Entitlements not available for this subaccount** SAP Entitlement Management OAuth Service Mit Service Details: SAP Entitlement Management Available Plans □ default (Application) SAP Entitlement Management Test Tenant. □ addon-test (Application) SAP Entitlement Management(Beta) addon test plan □ default Service plan for using SAP Entitlement Management service APIs. 0 selected plans

5. Start with the application:
Take Test tenant for example.

Select the service **SAP Entitlement Management**, check the service plan "default", and then add the service plan.



Subaccount SAP-DEMO-SUBACC001 - Entitlements

Entitlements

All Categories | SAP Entitlement Manag...

Entitlements available for this subaccount

- SAP Entitlement Management
- SAP Entitlement Management OAuth Service Production
- SAP Entitlement Management OAuth Service Test
- SAP Entitlement Management System
- SAP Entitlement Management System Partner Edition

Entitlements not available for this subaccount

- SAP Entitlement Management OAuth Service Mit

Service Details: SAP Entitlement Management

Available Plans

☑ default (Application)
SAP Entitlement Management Test Tenant

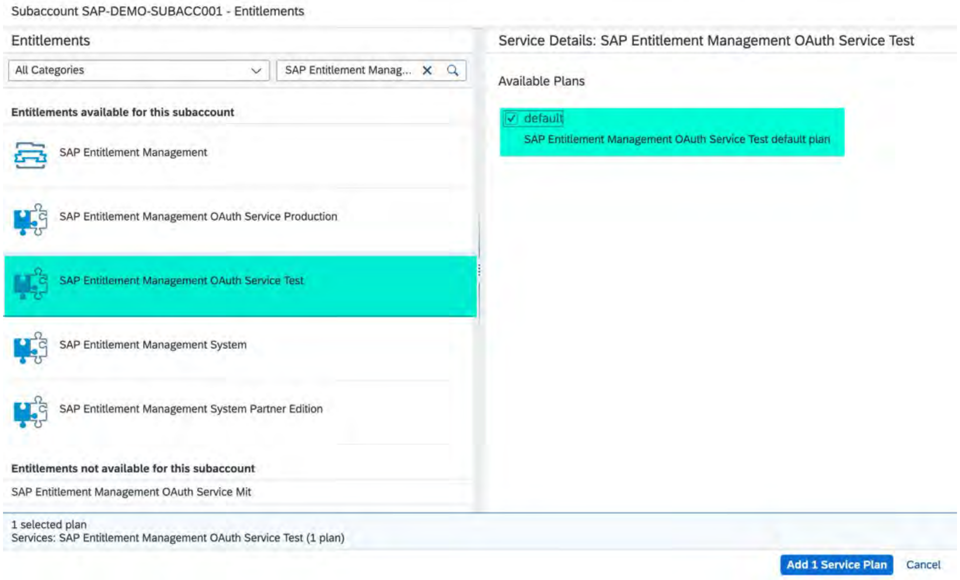
☐ addon-test (Application)
SAP Entitlement Management(Beta) addon test plan

☐ default
Service plan for using SAP Entitlement Management service APIs.

1 selected plan
Services: SAP Entitlement Management (1 plan)

6. Repeat Steps 3-5 for the service **SAP Entitlement Management OAuth Service <Tenant Type>**.

This service enables you to call **SAP Entitlement Management** APIs.



Subaccount SAP-DEMO-SUBACC001 - Entitlements

Entitlements

All Categories | SAP Entitlement Manag...

Entitlements available for this subaccount

- SAP Entitlement Management
- SAP Entitlement Management OAuth Service Production
- SAP Entitlement Management OAuth Service Test
- SAP Entitlement Management System
- SAP Entitlement Management System Partner Edition

Entitlements not available for this subaccount

- SAP Entitlement Management OAuth Service Mit

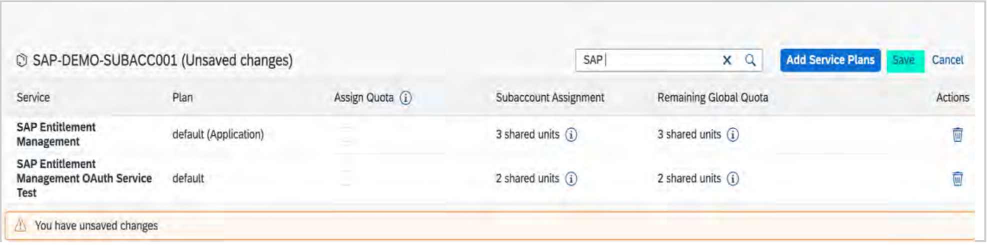
Service Details: SAP Entitlement Management OAuth Service Test

Available Plans

☑ default
SAP Entitlement Management OAuth Service Test default plan

1 selected plan
Services: SAP Entitlement Management OAuth Service Test (1 plan)

7. Save your changes.



SAP-DEMO-SUBACC001 (Unsaved changes)

SAP

Service	Plan	Assign Quota	Subaccount Assignment	Remaining Global Quota	Actions
SAP Entitlement Management	default (Application)		3 shared units	3 shared units	
SAP Entitlement Management OAuth Service Test	default		2 shared units	2 shared units	

⚠ You have unsaved changes

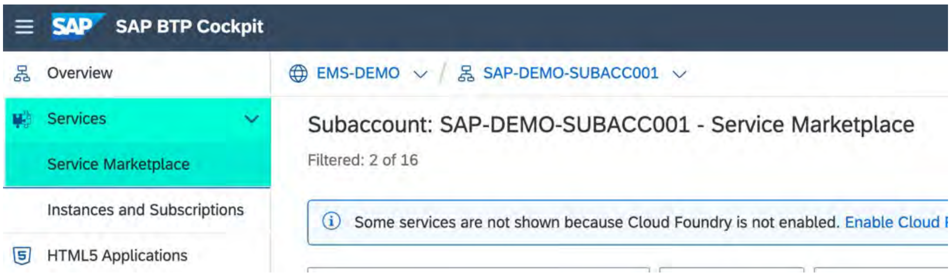
You can adjust quotas for only one subaccount at a time. To adjust quotas for multiple subaccounts, complete these steps for each subaccount.

If you have distributed the maximum of your purchased quotas, you can’t increase it further. However, you can move quotas between subaccounts in the same global account.

1.5 Subscribe to SAP Entitlement Management

To use the **SAP Entitlement Management** solution, you must subscribe to the application for your subaccount.

1. Go to your subaccount and select **Services → Service Marketplace** in the navigation panel.



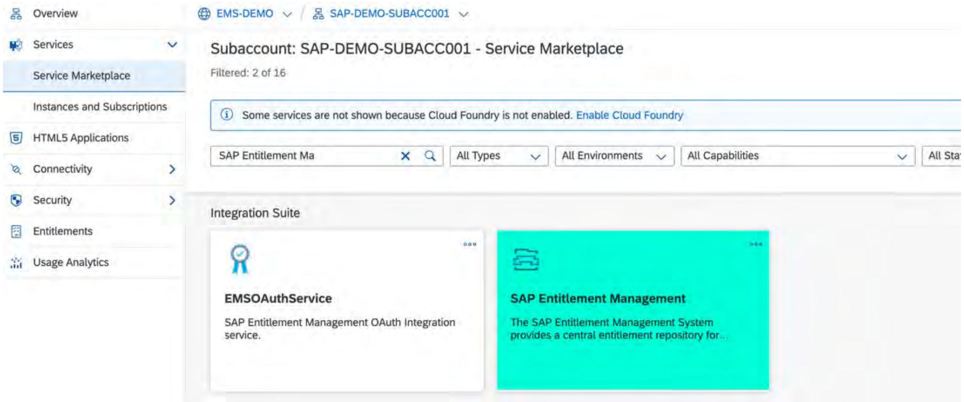
Subaccount: SAP-DEMO-SUBACC001 - Service Marketplace

Filtered: 2 of 16

Some services are not shown because Cloud Foundry is not enabled. Enable Cloud F

2. You see all the services that are available to you.

   Search for and select the application **SAP Entitlement Management**.



Subaccount: SAP-DEMO-SUBACC001 - Service Marketplace

Filtered: 2 of 16

Some services are not shown because Cloud Foundry is not enabled. Enable Cloud Foundry

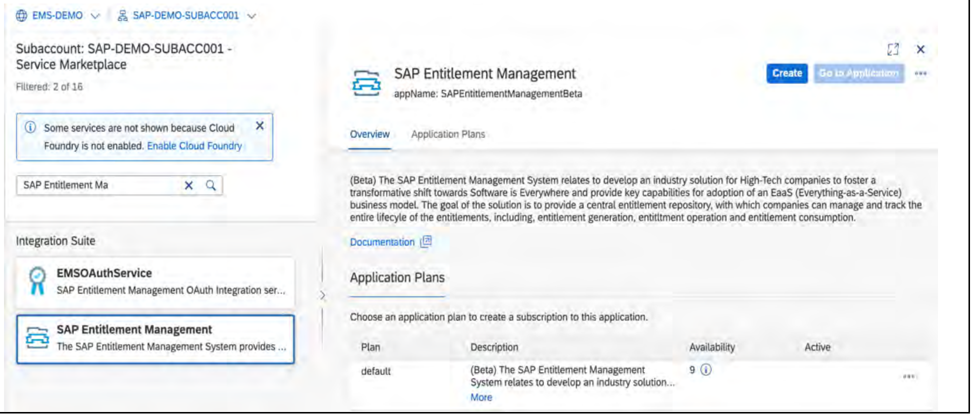
EMSOAuthService

SAP Entitlement Management OAuth Integration service.

SAP Entitlement Management

The SAP Entitlement Management System provides a central entitlement repository for...

3. Under **Application Plans**, display the action menu of the plan for which you want to create a subscription and select **Create**.



Subaccount: SAP-DEMO-SUBACC001 - Service Marketplace

Filtered: 2 of 16

Some services are not shown because Cloud Foundry is not enabled. Enable Cloud Foundry

EMSOAuthService SAP Entitlement Management OAuth Integration ser...

SAP Entitlement Management The SAP Entitlement Management System provides ...

SAP Entitlement Management

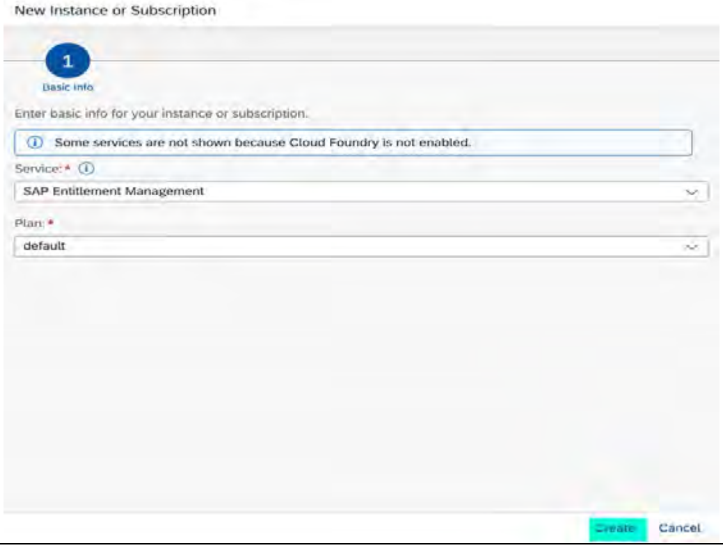
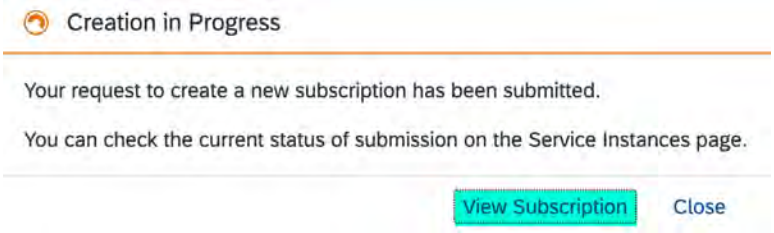
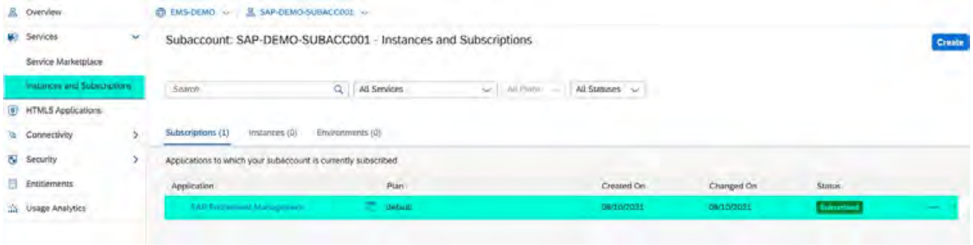
appName: SAPEntitlementManagementBeta

(Beta) The SAP Entitlement Management System relates to develop an industry solution for High-Tech companies to foster a transformative shift towards Software is Everywhere and provide key capabilities for adoption of an EaaS (Everything-as-a-Service) business model. The goal of the solution is to provide a central entitlement repository, with which companies can manage and track the entire lifecyle of the entitlements, including, entitlement generation, entitltment operation and entitlement consumption.

Application Plans

Choose an application plan to create a subscription to this application.

Plan	Description	Availability	Active
default	(Beta) The SAP Entitlement Management System relates to develop an industry solution... More	9	

4. Check the basic info and then select **Create**.	New Instance or Subscription 1 Basic Info Enter basic info for your instance or subscription. Some services are not shown because Cloud Foundry is not enabled. Service: * SAP Entitlement Management Plan: * default
5. The creation process starts. Select **View Subscription** to switch to the **Instances and Subscriptions** screen.	Creation in Progress Your request to create a new subscription has been submitted. You can check the current status of submission on the Service Instances page.
6. Now you're subscribed to the **SAP Entitlement Management** application. With this step, your tenant is created.	 EMS-DEMO / SAP-DEMO-SUBACC001 Subaccount: SAP-DEMO-SUBACC001 - Instances and Subscriptions Search / All Services / All Plans / All Statuses Subscriptions (1) Instances (0) Environments (0) Applications to which your subaccount is currently subscribed Application: SAP Entitlement Management; Plan: default; Created On: 08/10/2021; Changed On: 08/10/2021; Status: Subscribed

2. ENABLE UI ACCESS

This chapter describes how to configure authentication and authorization for the users of your application. You can enable them to log on to the **SAP Entitlement Management** UI and get access to the appropriate apps and data.

2.1 Give Yourself Access as an Administrator

To give **yourself** access to the **SAP Entitlement Management** UI, you need to do the following:

1. Build at least one role collection, as described in the section Build role collections.

   ⓘ For administrators, we recommend the role **EM_Admin**, which provides you with the completeset of authorizations and allows you to test all apps.

2. Assign at least one role collection to your user, as described in the section Assign role collections to users or user groups.
3. Log on to the **SAP Entitlement Management** application.

To enable UI access for further users, repeat Steps 1 and 2 for these users to assign the appropriate role. Please consider that these users must be available in the identity provider (IdP) that is attached to the subaccount. You can find more information on authentication and single sign-on of business users in the sections Enable authentication and single sign-on for business users and Assign your own identity provider (IdP) to your subaccount.

2.2 Define Security Administrators in Your Subaccount

To configure authentication and authorization for business users, you need a platform user with the specific role **User & Role Administrator**. When you create a subaccount, SAP BTP automatically grants this role to your user.

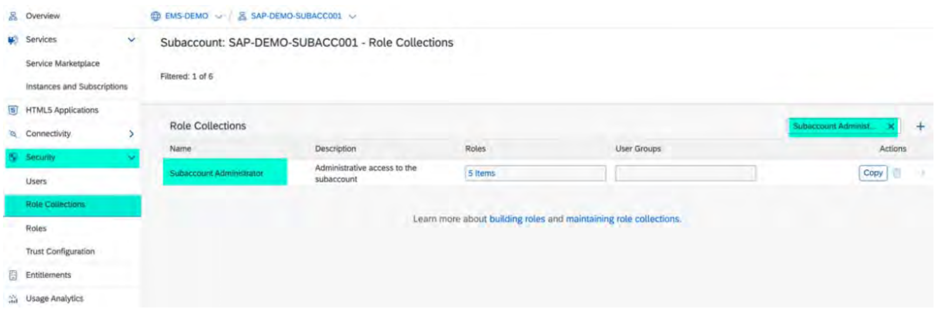
If you want to enable other users to configure authentication and authorization, you can assign the role by adding the users as security administrators in your subaccount. In Cloud Management Tools Feature Set B, this role is bundled in the role collection **Subaccount Administrator**.

For more information, see Role Collections and Roles in Global Accounts and Subaccounts [Feature Set B] in the SAP BTP documentation.

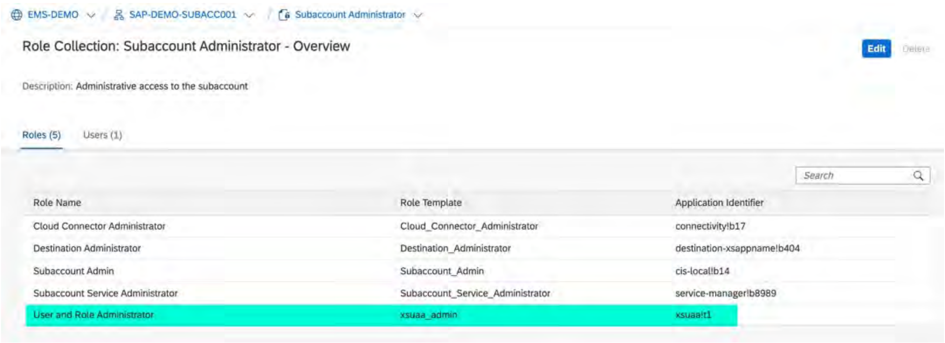
The following instructions show how a security administrator, for example, the user who created the subaccount, can authorize another platform user to also become a security administrator.

The users that you want to add as security administrators in a subaccount must have at least one of the following memberships:

- Member of the Cloud Foundry organization (if available) in the subaccount
- Member of any Cloud Foundry space that belongs to the organization
- Members of the global account that contains your subaccount: see the section Add administrators to global account

1. In your subaccount, choose **Security** → **Role Collections** in the navigation panel. Search for the role collection “Subaccount Administrator”.	 Subaccount: SAP-DEMO-SUBACC001 - Role Collections Filtered: 1 of 6 Role Collections Name: Subaccount Administrator Description: Administrative access to the subaccount Roles: 5 Items Learn more about building roles and maintaining role collections.

2. Ensure that the collection contains the role **User and Role Administrator**. This is the key role for security administrators.



EMS-DEMO / SAP-DEMO-SUBACC001 / Subaccount Administrator

Role Collection: Subaccount Administrator - Overview

Edit Delete

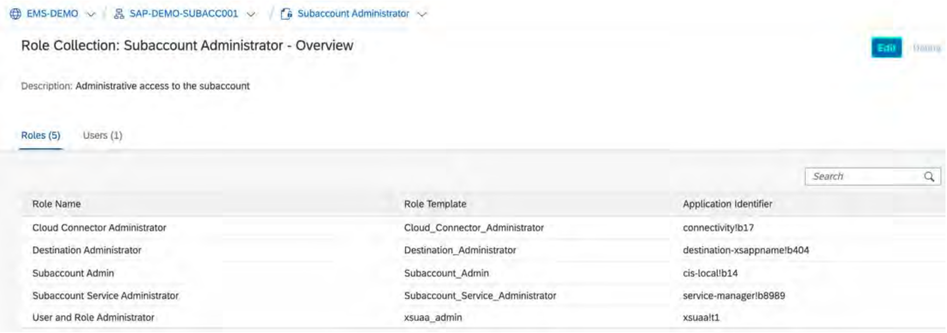
Description: Administrative access to the subaccount

Roles (5) Users (1)

Search

Role Name	Role Template	Application Identifier
Cloud Connector Administrator	Cloud_Connector_Administrator	connectivity!b17
Destination Administrator	Destination_Administrator	destination-xsappname!b404
Subaccount Admin	Subaccount_Admin	cis-local!b14
Subaccount Service Administrator	Subaccount_Service_Administrator	service-manager!b8989
User and Role Administrator	xsuaa_admin	xsuaa!t1

3. To assign to the role collection the users that you want as security administrators, select **Edit**.



EMS-DEMO / SAP-DEMO-SUBACC001 / Subaccount Administrator

Role Collection: Subaccount Administrator - Overview

Edit Delete

Description: Administrative access to the subaccount

Roles (5) Users (1)

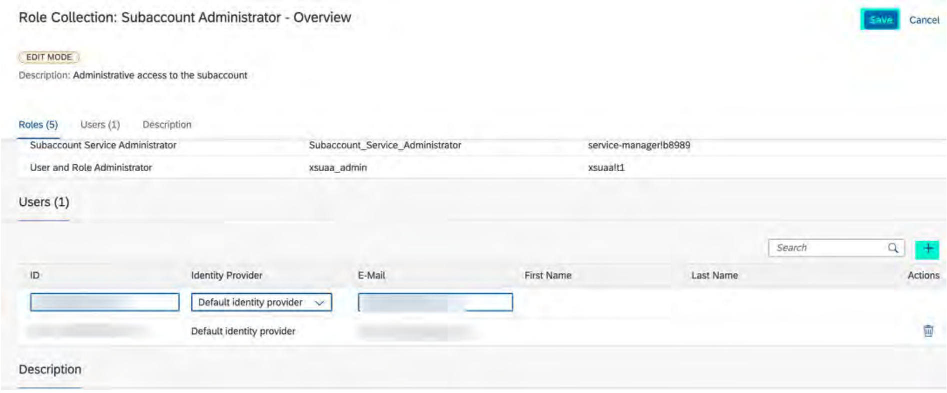
Search

Role Name	Role Template	Application Identifier
Cloud Connector Administrator	Cloud_Connector_Administrator	connectivity!b17
Destination Administrator	Destination_Administrator	destination-xsappname!b404
Subaccount Admin	Subaccount_Admin	cis-local!b14
Subaccount Service Administrator	Subaccount_Service_Administrator	service-manager!b8989
User and Role Administrator	xsuaa_admin	xsuaa!t1

4. With the edit mode enabled, add the security administrators under **Users**.

For each user, enter the ID and the identity provider, then select the plus (**+**) icon.

Once you have added all users, select **Save** to close the edit mode.



Role Collection: Subaccount Administrator - Overview

Save Cancel

EDIT MODE

Description: Administrative access to the subaccount

Roles (5) Users (1) Description

Subaccount Service Administrator	Subaccount_Service_Administrator	service-manager!b8989
User and Role Administrator	xsuaa_admin	xsuaa!t1

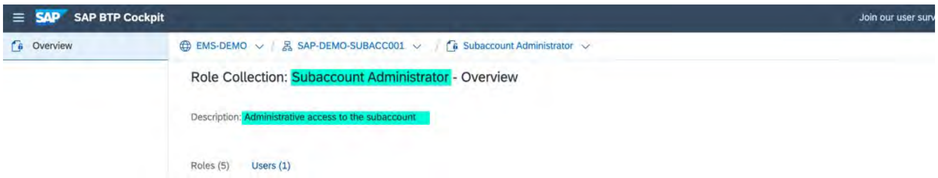
Users (1)

Search +

ID	Identity Provider	E-Mail	First Name	Last Name	Actions
	Default identity provider				
[redacted]	Default identity provider	[redacted]			

Description

5. The added users now have access to the subaccount as security administrators.



SAP BTP Cockpit

Join our user surv

Overview

EMS-DEMO / SAP-DEMO-SUBACC001 / Subaccount Administrator

Role Collection: Subaccount Administrator - Overview

Description: Administrative access to the subaccount

Roles (5) Users (1)

2.3 Enable Authentication and Single Sign-on for Business Users

On SAP BTP, identity information is provided by identity providers (IdPs) and not stored on SAP BTP itself. Accordingly, the authentication of business users to access the SAP Entitlement Management UI is delegated to the identity providers, and users log on with the mechanisms and credentials defined there, (e.g., with their username and password). For an overview, see Security in the SAP BTP documentation.

SAP BTP supports the following identity providers:

- SAML 2.0 standard compliant IdP
- Identity Authentication service (SAP's cloud solution for identity life cycle management) on SAP BTP
- SAP ID service (SAP-administered IdP)

For SAP ID Service, trust is preconfigured on SAP BTP by default, so that you can start using the service without further configuration. Business users with an account in SAP ID service (https://accounts.sap.com/) and who are authorized for **SAP Entitlement Management** can log on using their email address and the respective password.

> ⓘ For productive scenarios of SAP Entitlement Management, we recommend to use your own identity provider,and not SAP ID service. As an SAP-administered IdP, SAP ID service doesn’t support administrative access and has the following restrictions:
>
> - User registration works through self-service: You can’t provision users to SAP ID service, you can’t lock users (for example, if their responsibility within the company changes or if they leave the company).
> - You can’t create user groups to simplify the assignment of role collections.
> - You can’t configure single sign-on to work with other applications controlled by your own identity provider. In other words, you can’t configure IdP proxying with SAP ID service.

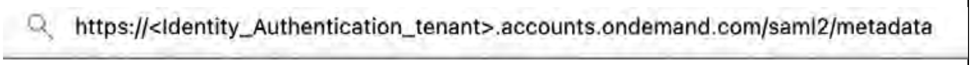
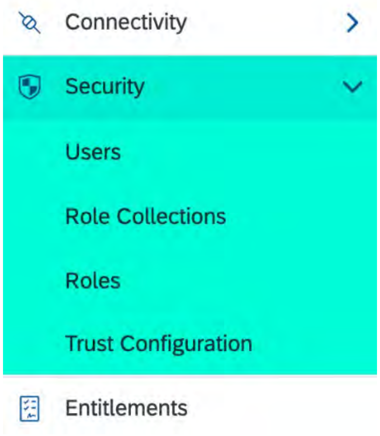
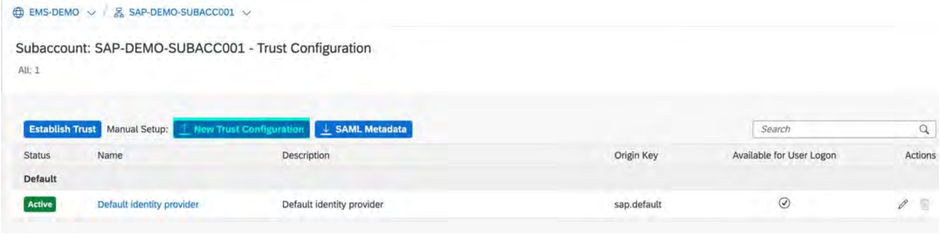
In the following section, the instructions guide you through connecting your own identity provider.

2.4 Assign Your Own Identity Provider (IdP) to Your Subaccount

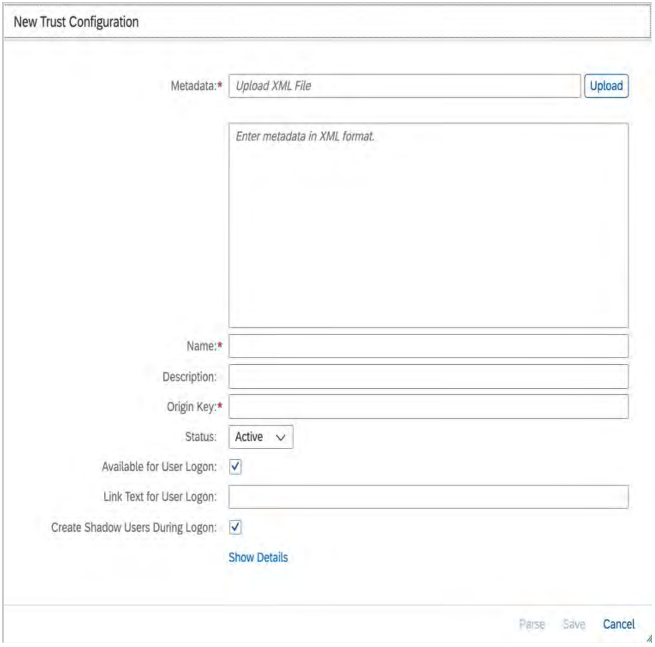
If you use the Identity Authentication service in SAP BTP, you can find more information in the SAP BTP documentation under Manually Establish Trust and Federation Between UAA and Identity Authentication.

If you use a different IdP, you can find more information under Establish Trust and Federation with UAA Using Any SAML Identity Provider.

The following instructions show how to assign **Identity Authentication in SAP BTP** to a subaccount as an identity provider. You do this by defining a mutual trust relationship between the identity provider and the SAP BTP subaccount in the SAP BTP cockpit and the admin console of the Identity Authentication service.

1. Download the SAML 2.0 metadata of your identity provider.	For the Identity Authentication service, enter the URL **https://<Identity_Authentication_tenant>.accounts.ondemand.com/saml2/metadata** in your browser. Replace <Identity_Authentication_tenant> with the subdomain of your tenant for the Identity Authentication service.  https://<Identity_Authentication_tenant>.accounts.ondemand.com/saml2/metadata ⓘ The subdomain of the Identity Authentication service isn't the same as the subdomain of the subaccount that you use for your **SAP Entitlement Management** application.
2. In your global account, select your subaccount and ensure that the **Security** menu is available. ⓘ If the menu isn't available, your user isn't a security administrator and not authorized for assigning an IdP. See the section Define security administrators in your subaccount in this guide for more details.	 Connectivity Security Users Role Collections Roles Trust Configuration Entitlements
3. Select **Trust Configuration** and then select **New Trust Configuration**.	 EMS-DEMO / SAP-DEMO-SUBACC001 Subaccount: SAP-DEMO-SUBACC001 - Trust Configuration All: 1 Establish Trust Manual Setup: New Trust Configuration SAML Metadata Search Status Name Description Origin Key Available for User Logon Actions Default Active Default identity provider Default identity provider sap.default ✓

4. Select **Upload** and add the file with the SAML 2.0 metadata of your identity provider that you downloaded in Step 1.



New Trust Configuration

Metadata:* Upload XML File [Upload]

Enter metadata in XML format.

Name:*

Description:

Origin Key:*

Status: Active

Available for User Logon: ☑

Link Text for User Logon:

Create Shadow Users During Logon: ☑

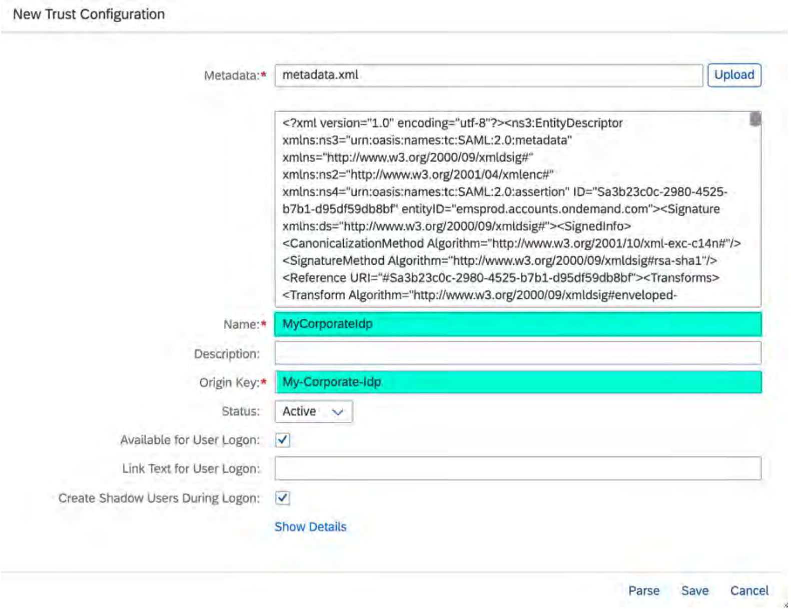
Show Details

Parse Save Cancel

5. Enter a **Name** and **Origin Key** for your identity provider. Then select **Save**.

ⓘ The name is displayed when the identity provider can be selected; for example, when business users log in.
In this guide, we use "My Corporate IdP" as the sample provider.

The origin key is used in the audit log; for example, to uniquely identify the source of an authenticated user.



New Trust Configuration

Metadata:* metadata.xml [Upload]

```
<?xml version="1.0" encoding="utf-8"?><ns3:EntityDescriptor
xmlns:ns3="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns="http://www.w3.org/2000/09/xmldsig#"
xmlns:ns2="http://www.w3.org/2001/04/xmlenc#"
xmlns:ns4="urn:oasis:names:tc:SAML:2.0:assertion" ID="Sa3b23c0c-2980-4525-
b7b1-d95df59db8bf" entityID="emsprod.accounts.ondemand.com"><Signature
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<Reference URI="#Sa3b23c0c-2980-4525-b7b1-d95df59db8bf"><Transforms>
<Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
```

Name:* MyCorporateIdp

Description:

Origin Key:* My-Corporate-Idp

Status: Active

Available for User Logon: ☑

Link Text for User Logon:

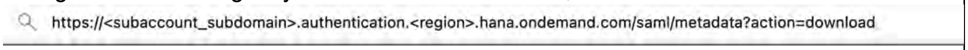
Create Shadow Users During Logon: ☑

Show Details

Parse Save Cancel

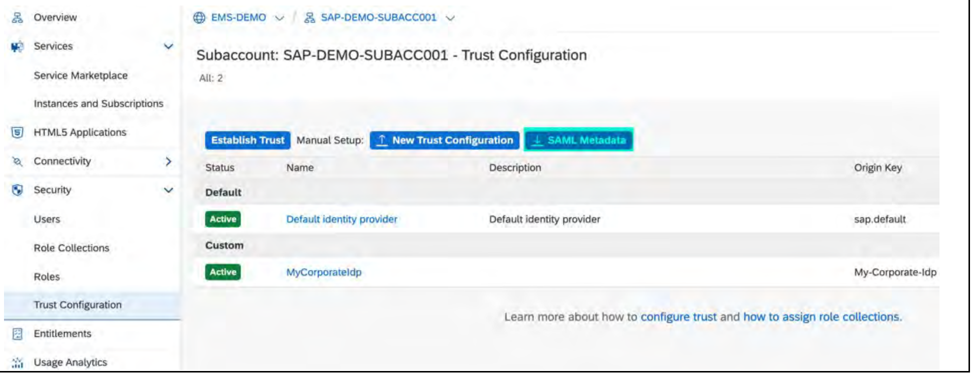
6. Download the SAML 2.0 metadata of your subaccount.

a) Replace <subaccount_subdomain> with the subdomain of your subaccount and <region> with the region your subaccount is located, such as eu10 or us10.



https://<subaccount_subdomain>.authentication.<region>.hana.ondemand.com/saml/metadata?action=download

b) In the **Trust Configuration** screen, select **SAML Metadata**.

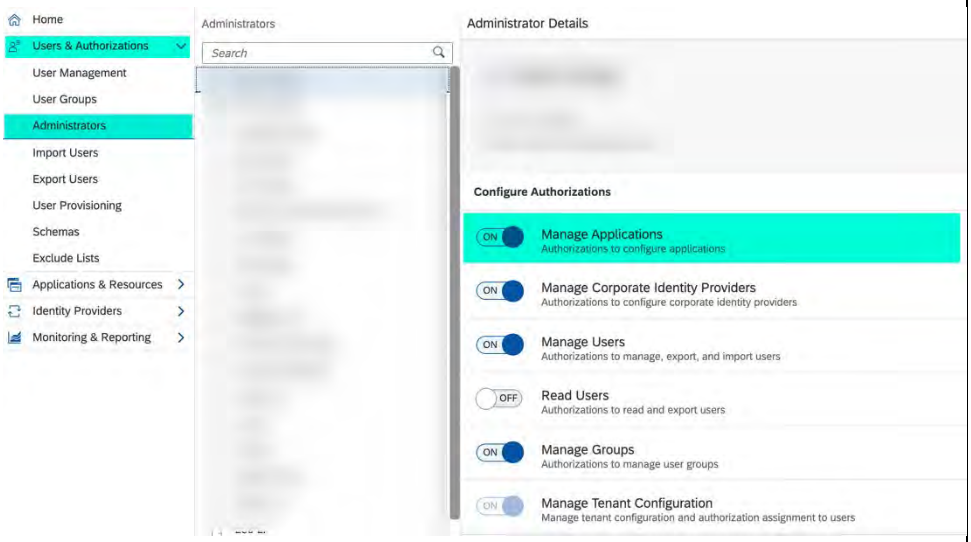
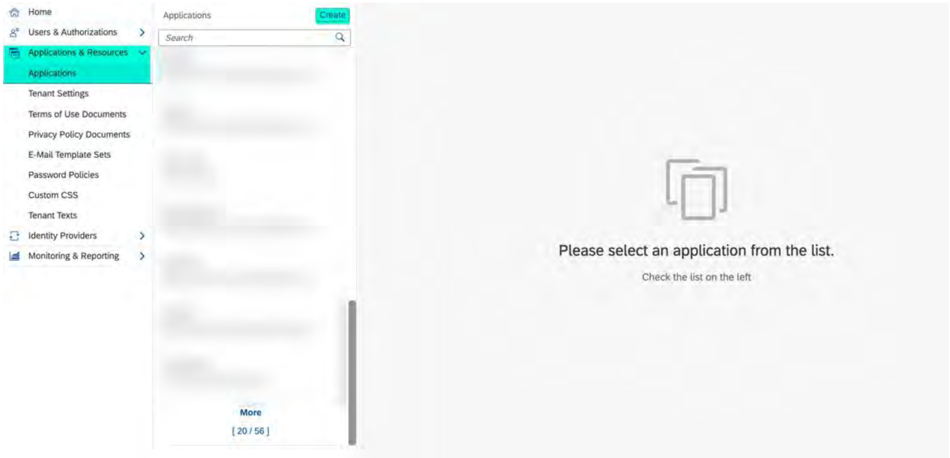


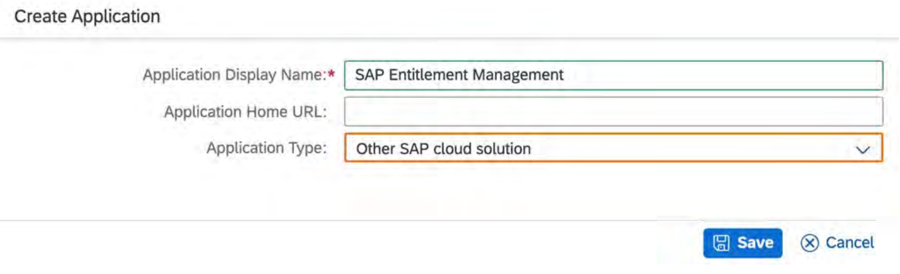
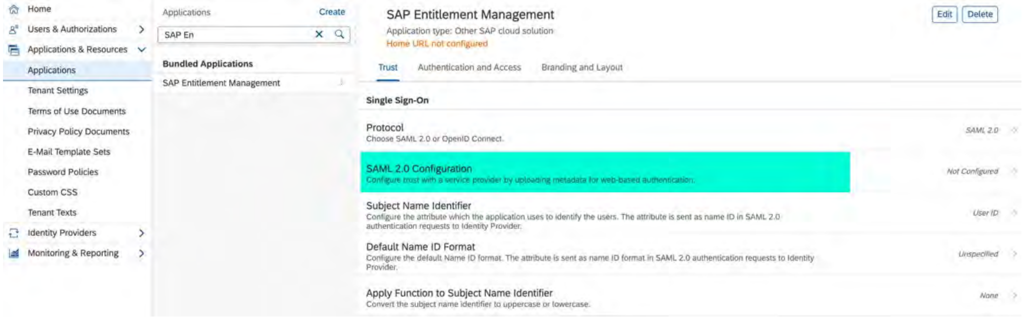
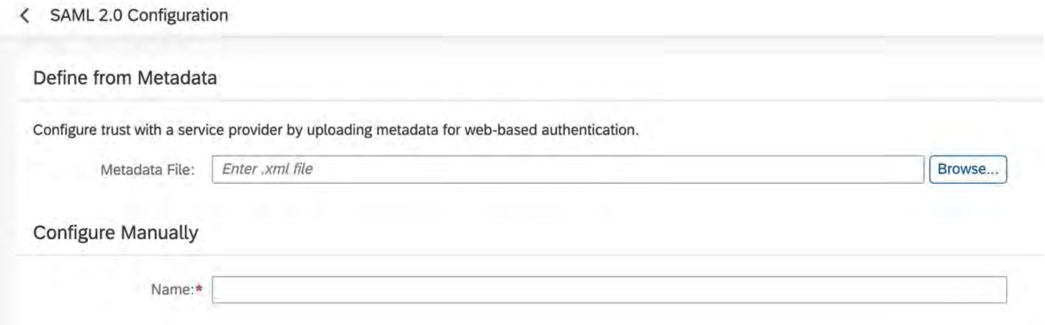
Subaccount: SAP-DEMO-SUBACC001 - Trust Configuration

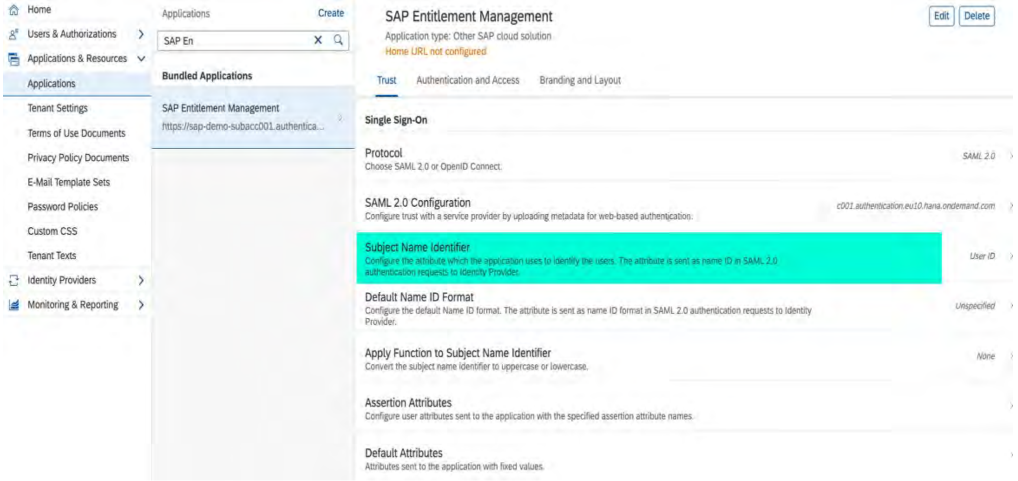
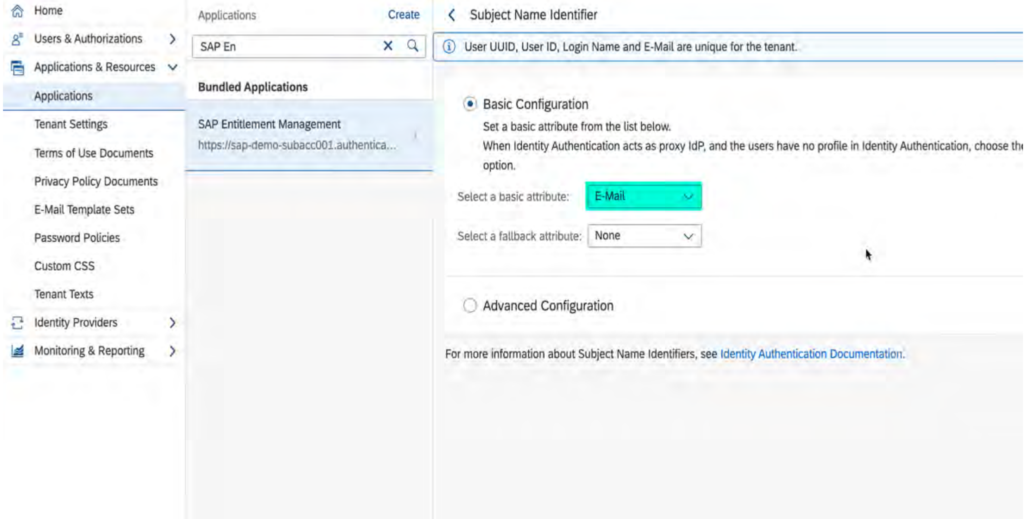
All: 2

Status	Name	Description	Origin Key
Default			
Active	Default identity provider	Default identity provider	sap.default
Custom			
Active	MyCorporateIdp		My-Corporate-Idp

Learn more about how to configure trust and how to assign role collections.

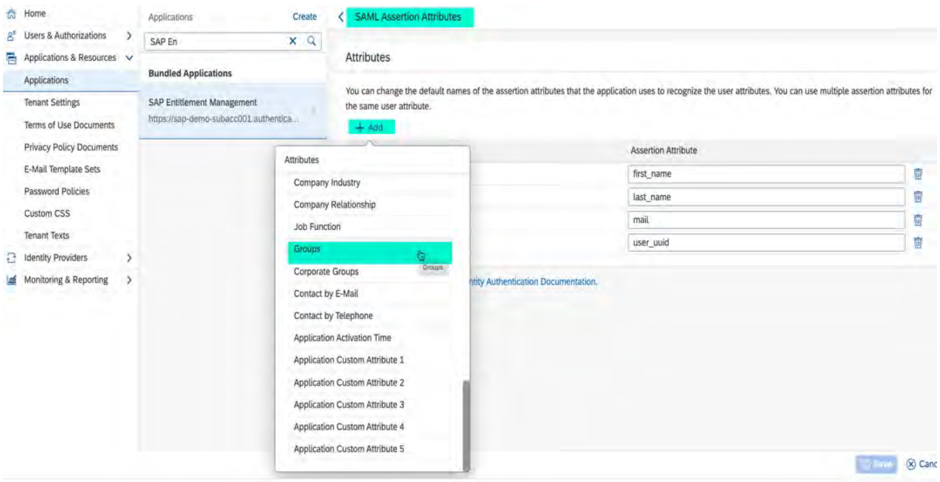
7. Go to the administration UI of your identity provider.	For the Identity Authentication service, replace <Identity_Authentication_tenant> with the name of your IAS tenant: https://<Identity_Authentication_tenant>.accounts.ondemand.com/admin ⓘ Your user needs the administration roles.
8. Ensure that your user has the required authorizations in the identity provider. ⓘ In IAS, your user must be added as **Administrator** and at least have the authorization to **Manage Applications.**	 Home Users & Authorizations User Management User Groups Administrators Import Users Export Users User Provisioning Schemas Exclude Lists Applications & Resources Identity Providers Monitoring & Reporting Administrators Search Administrator Details Configure Authorizations ON Manage Applications Authorizations to configure applications ON Manage Corporate Identity Providers Authorizations to configure corporate identity providers ON Manage Users Authorizations to manage, export, and import users OFF Read Users Authorizations to read and export users ON Manage Groups Authorizations to manage user groups ON Manage Tenant Configuration Manage tenant configuration and authorization assignment to users
9. To add **SAP Entitlement Management** as an application (SAML service provider), choose **Applications & Resources** → **Applications** and select **Create**.	 Home Users & Authorizations Applications & Resources Applications Tenant Settings Terms of Use Documents Privacy Policy Documents E-Mail Template Sets Password Policies Custom CSS Tenant Texts Identity Providers Monitoring & Reporting Applications Create Search More [20 / 56] Please select an application from the list. Check the list on the left

10. Enter the application name and select **Save**.	 Create Application Application Display Name:* SAP Entitlement Management Application Home URL: Application Type: Other SAP cloud solution
11. For the newly created application, select **SAML 2.0 Configuration**.	 Home Users & Authorizations Applications & Resources Applications Tenant Settings Terms of Use Documents Privacy Policy Documents E-Mail Template Sets Password Policies Custom CSS Tenant Texts Identity Providers Monitoring & Reporting Applications Create SAP En Bundled Applications SAP Entitlement Management SAP Entitlement Management Application type: Other SAP cloud solution Home URL not configured Edit Delete Trust Authentication and Access Branding and Layout Single Sign-On Protocol — Choose SAML 2.0 or OpenID Connect. — SAML 2.0 SAML 2.0 Configuration — Configure trust with a service provider by uploading metadata for web-based authentication. — Not Configured Subject Name Identifier — Configure the attribute which the application uses to identify the users. The attribute is sent as name ID in SAML 2.0 authentication requests to Identity Provider. — User ID Default Name ID Format — Configure the default Name ID format. The attribute is sent as name ID format in SAML 2.0 authentication requests to Identity Provider. — Unspecified Apply Function to Subject Name Identifier — Convert the subject name identifier to uppercase or lowercase. — None
12. Under **Define from Metadata**, upload the SAML 2.0 metadata of your subaccount that you previously downloaded.	 SAML 2.0 Configuration Define from Metadata Configure trust with a service provider by uploading metadata for web-based authentication. Metadata File: Enter .xml file Configure Manually Name:*

13. Back in the application, select **Subject Name Identifier**.	 SAP Entitlement Management Application type: Other SAP cloud solution Home URL not configured Trust · Authentication and Access · Branding and Layout **Single Sign-On** Protocol: SAML 2.0 — Choose SAML 2.0 or OpenID Connect. SAML 2.0 Configuration: c001.authentication.eu10.hana.ondemand.com — Configure trust with a service provider by uploading metadata for web-based authentication. Subject Name Identifier: User ID — Configure the attribute which the application uses to identify the users. The attribute is sent as name ID in SAML 2.0 authentication requests to Identity Provider. Default Name ID Format: Unspecified — Configure the default Name ID format. The attribute is sent as name ID format in SAML 2.0 authentication requests to Identity Provider. Apply Function to Subject Name Identifier: None — Convert the subject name identifier to uppercase or lowercase. Assertion Attributes — Configure user attributes sent to the application with the specified assertion attribute names. Default Attributes — Attributes sent to the application with fixed values.
14. Under **Basic Configuration**, select the attribute **E-Mail** and then save.	 Subject Name Identifier ⓘ User UUID, User ID, Login Name and E-Mail are unique for the tenant. ● Basic Configuration Set a basic attribute from the list below. When Identity Authentication acts as proxy IdP, and the users have no profile in Identity Authentication, choose th option. Select a basic attribute: E-Mail Select a fallback attribute: None ○ Advanced Configuration For more information about Subject Name Identifiers, see Identity Authentication Documentation.

15. <u>Optional</u>: If you want to assign role collections to groups rather than to individual users, select **Trust → Assertion Attributes**, select **Add** and assign **Groups** as additional attribute.

   ⚠ The assertion attribute must be "Groups" (case-sensitive).

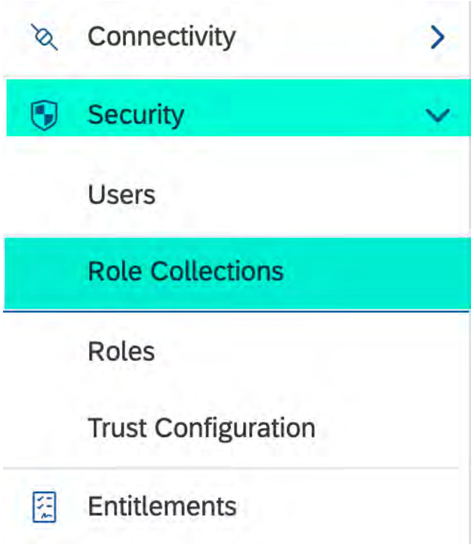
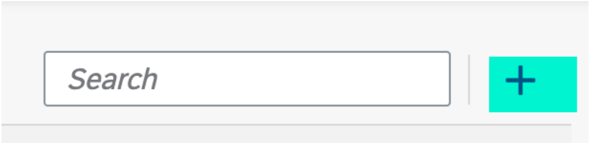
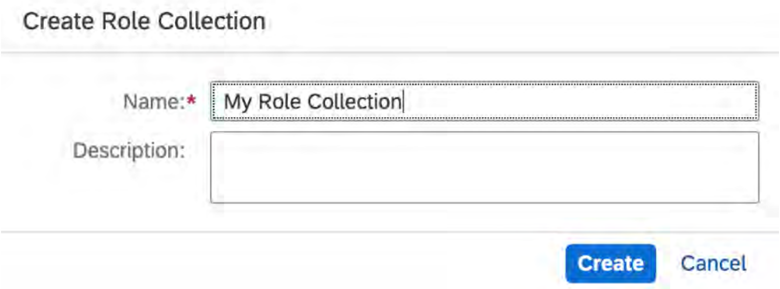
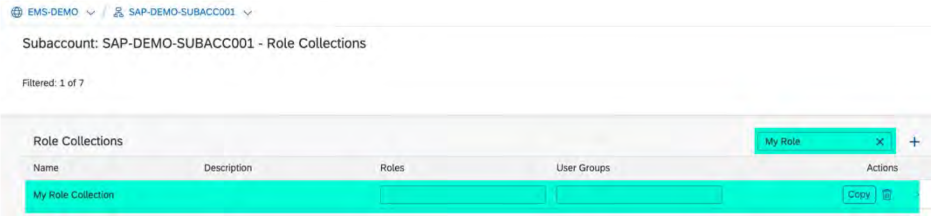


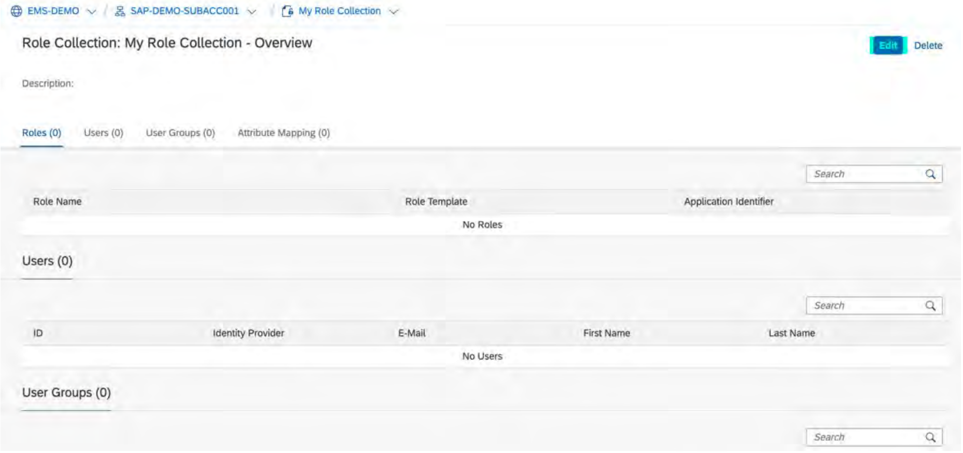
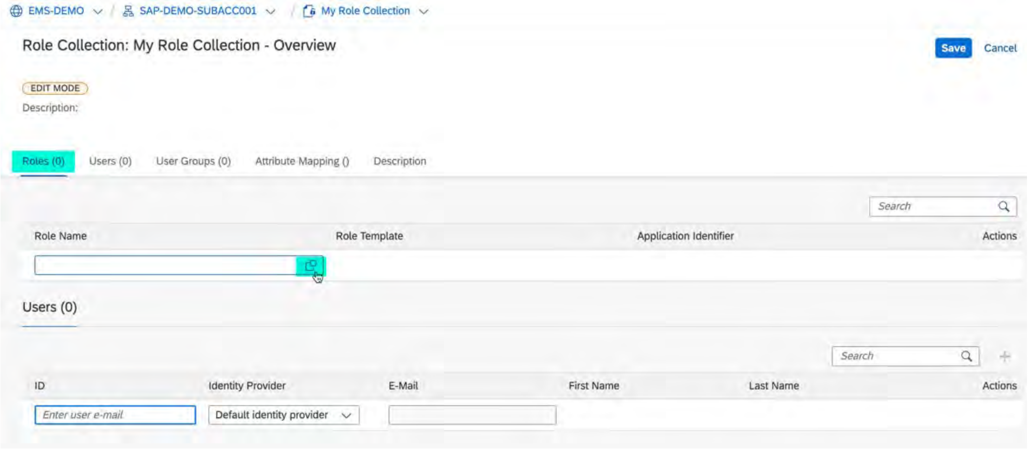
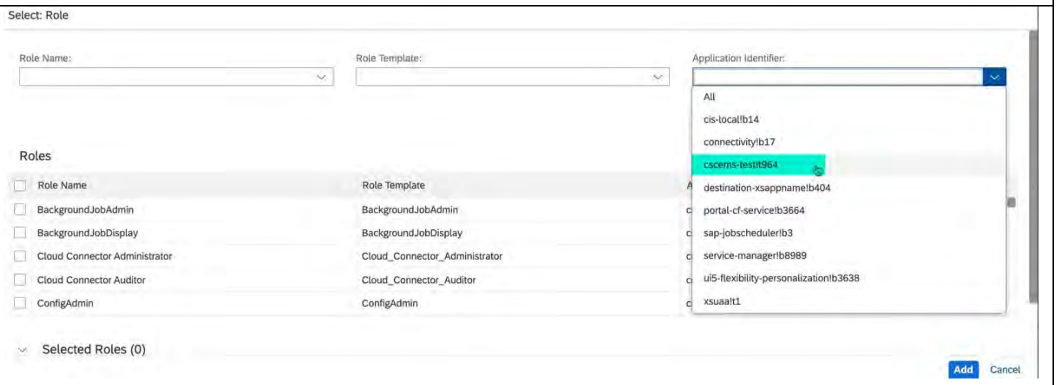
You can change the default names of the assertion attributes that the application uses to recognize the user attributes. You can use multiple assertion attributes for the same user attribute.

Assertion Attribute
first_name
last_name
mail
user_uuid

2.5 Build Role Collections

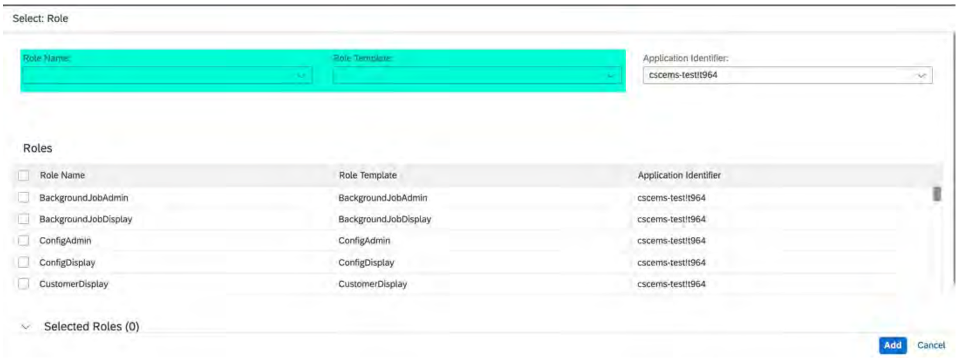
You need to define role collections to control user authorization for the SAP Entitlement Management UI and apps.

1. In your global account, open the subaccount. In the navigation panel, select **Security → Role Collections**.	 Connectivity Security Users Role Collections Roles Trust Configuration Entitlements
2. To create a new role collection, select the plus (**+** **)** icon on the right of the search field.	
3. Name your role collection and select **Create**. In this guide, we use "My Role Collection" as the example name.	 Create Role Collection Name:* My Role Collection Description:
4. To start adding roles, search for the new role collection in the table and select the row.	 EMS-DEMO / SAP-DEMO-SUBACC001 Subaccount: SAP-DEMO-SUBACC001 - Role Collections Filtered: 1 of 7 Role Collections My Role Name | Description | Roles | User Groups | Actions My Role Collection | | | | Copy

5. In the overview of the role collection, select **Edit** to open the screen in edit mode.	 EMS-DEMO / SAP-DEMO-SUBACC001 / My Role Collection Role Collection: My Role Collection - Overview Edit Delete Description: Roles (0) Users (0) User Groups (0) Attribute Mapping (0) Search Role Name · Role Template · Application Identifier No Roles Users (0) Search ID · Identity Provider · E-Mail · First Name · Last Name No Users User Groups (0) Search
6. Under **Roles → Role Name**, select the icon of the input field to open the role selector.	 EMS-DEMO / SAP-DEMO-SUBACC001 / My Role Collection Role Collection: My Role Collection - Overview Save Cancel EDIT MODE Description: Roles (0) Users (0) User Groups (0) Attribute Mapping () Description Search Role Name · Role Template · Application Identifier · Actions Users (0) Search ID · Identity Provider · E-Mail · First Name · Last Name · Actions Enter user e-mail · Default identity provider
7. In the list **Application Identifier**, choose the identifier that begins with "cscems". This identifier filters by the roles from **SAP Entitlement Management**.	 Select: Role Role Name: · Role Template: · Application Identifier: All cis-local!b14 connectivity!b17 cscems-test!t964 destination-xsappname!b404 portal-cf-service!b3664 sap-jobscheduler!b3 service-manager!b8989 ui5-flexibility-personalization!b3638 xsuaa!t1 Roles Role Name · Role Template BackgroundJobAdmin · BackgroundJobAdmin BackgroundJobDisplay · BackgroundJobDisplay Cloud Connector Administrator · Cloud_Connector_Administrator Cloud Connector Auditor · Cloud_Connector_Auditor ConfigAdmin · ConfigAdmin Selected Roles (0) Add Cancel

8. The table **Roles** shows all the available roles for **SAP Entitlement Management**. You can filter by roles and templates to reduce the number of rows. Then select the roles that you want in your collection.

   ⓘ You can find information about the available role templates under [Build Role Collections]() in the *Setup and Administration Guide*.



Select: Role

Role Name:

Role Template:

Application Identifier: cscems-test!t964

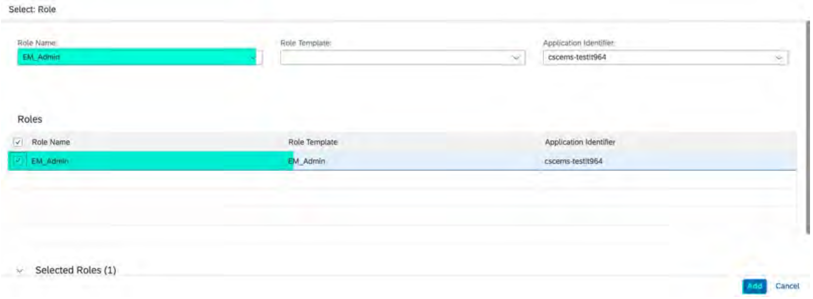
Roles

□	Role Name	Role Template	Application Identifier
□	BackgroundJobAdmin	BackgroundJobAdmin	cscems-test!t964
□	BackgroundJobDisplay	BackgroundJobDisplay	cscems-test!t964
□	ConfigAdmin	ConfigAdmin	cscems-test!t964
□	ConfigDisplay	ConfigDisplay	cscems-test!t964
□	CustomerDisplay	CustomerDisplay	cscems-test!t964

Selected Roles (0)

9. Once you have selected all the roles for the collection, select **Add** to confirm the selection.

   ⓘ The screenshot shows the role “EM_Admin”,which provides the complete set of authorizations, as an example. For productive use, we recommend that you configure suitable roles for your users.



Select: Role

Role Name: EM_Admin

Role Template:

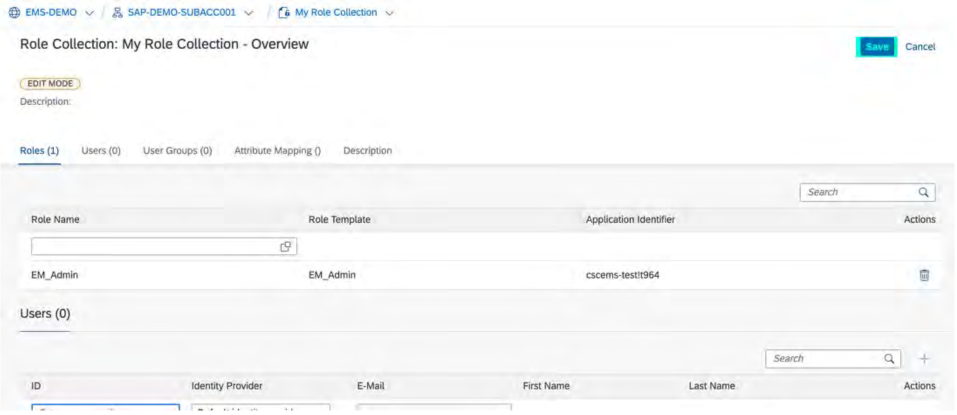
Application Identifier: cscems-test!t964

Roles

☑	Role Name	Role Template	Application Identifier
☑	EM_Admin	EM_Admin	cscems-test!t964

Selected Roles (1)

10. Select **Save** to close the edit mode.



Role Collection: My Role Collection - Overview

Description:

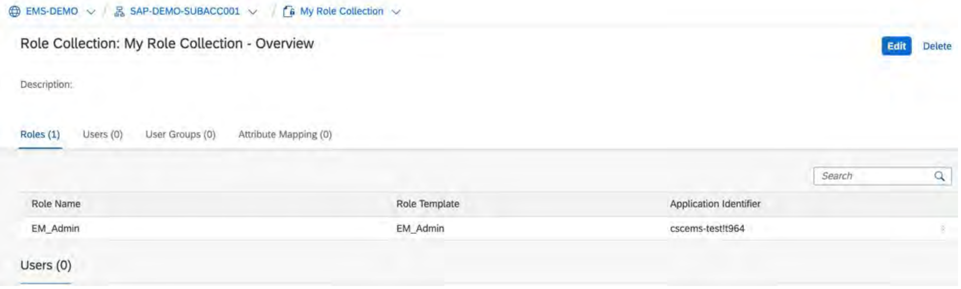
Role Name	Role Template	Application Identifier	Actions
EM_Admin	EM_Admin	cscems-test!t964	

Users (0)

ID	Identity Provider	E-Mail	First Name	Last Name	Actions

11. Your role now collection shows the assigned roles.

    Repeat these steps if you want to add further roles to the collection.



Role Collection: My Role Collection - Overview

Description:

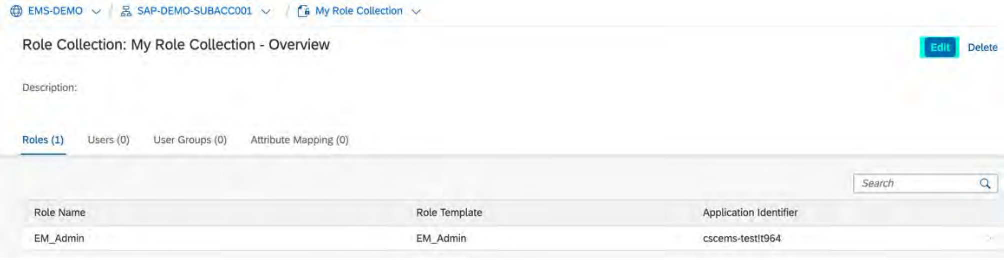
Role Name	Role Template	Application Identifier
EM_Admin	EM_Admin	cscems-test!t964

Users (0)

2.6 Assign Role Collections to Users or User Groups

In the SAP BTP cockpit, you must assign role collections to IdP users or user groups. The following steps show how to assign collections to individual users with the example identity provider that we set up in the section Assign your own identity provider (IdP) to your subaccount in this guide.

1. Create or open the role collection. In the overview, select **Edit** to open the screen in edit mode.

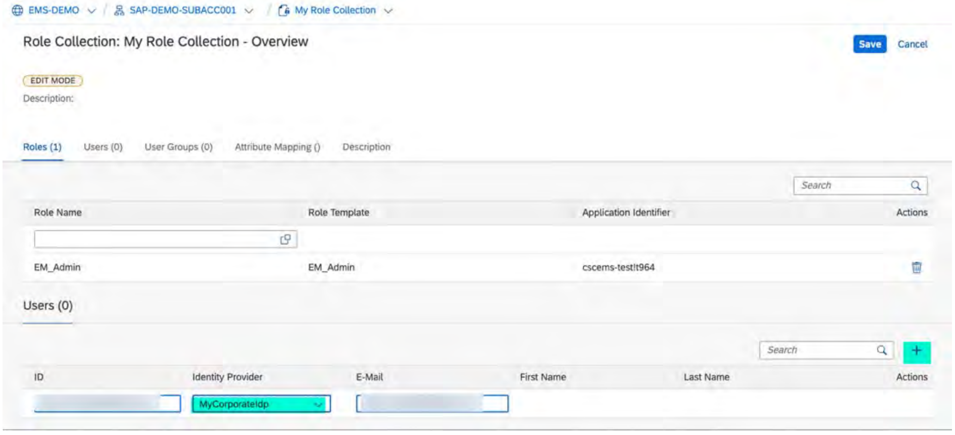


Role Collection: My Role Collection - Overview

Description:

Role Name	Role Template	Application Identifier
EM_Admin	EM_Admin	cscems-testlt964

2. Under **Users**, enter the ID of the user and choose the identity provider in the first row. Then select the plus (**+**) icon.



Role Collection: My Role Collection - Overview

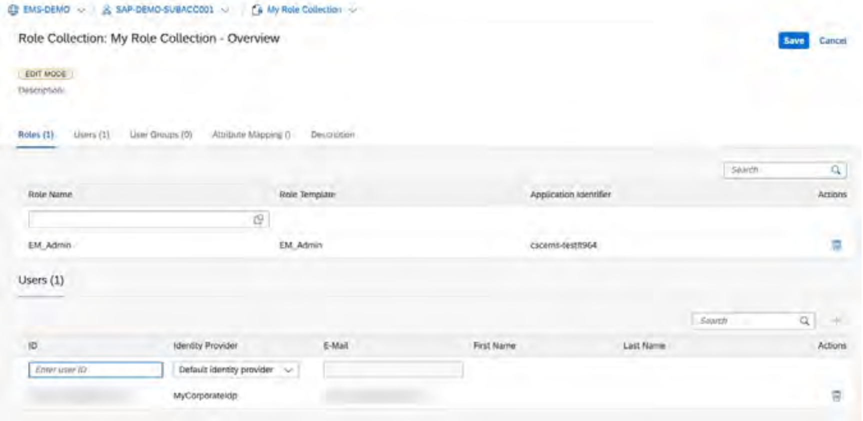
Description:

Role Name	Role Template	Application Identifier	Actions
EM_Admin	EM_Admin	cscems-testlt964	

Users (0)

ID	Identity Provider	E-Mail	First Name	Last Name	Actions
[redacted]	MyCorporateIdp	[redacted]			

3. The user is now added. Repeat the previous step to add further users to the collection.



Role Collection: My Role Collection - Overview

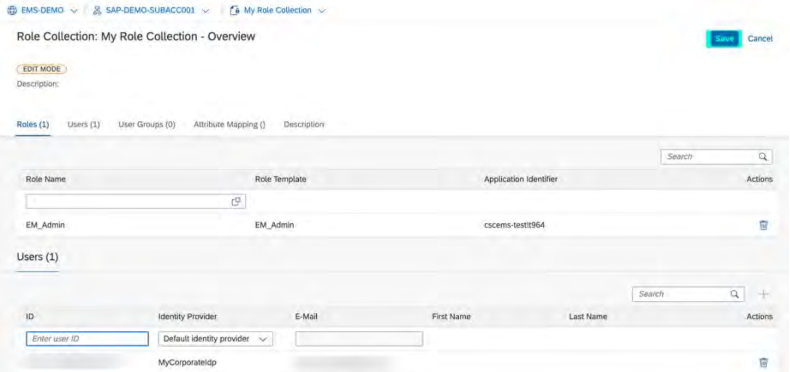
Description:

Role Name	Role Template	Application Identifier	Actions
EM_Admin	EM_Admin	cscems-testlt964	

Users (1)

ID	Identity Provider	E-Mail	First Name	Last Name	Actions
Enter user ID	Default identity provider				
[redacted]	MyCorporateIdp	[redacted]			

4. Select **Save** to close the edit mode.



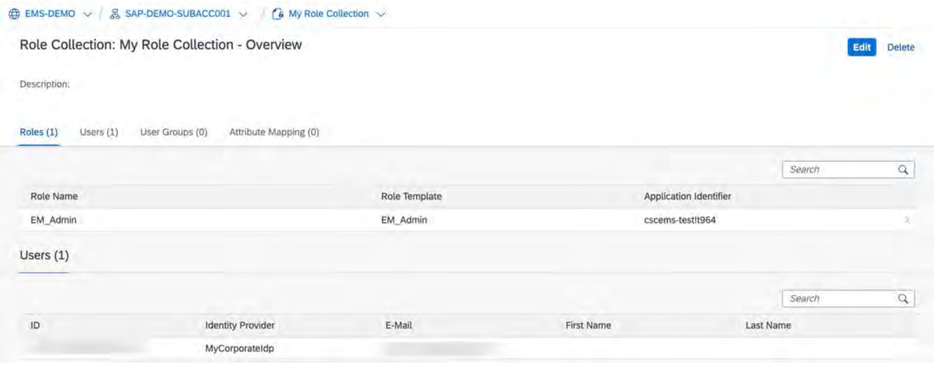
Role Collection: My Role Collection - Overview

Description:

Role Name	Role Template	Application Identifier	Actions
EM_Admin	EM_Admin	cscems-testlt964	

Users (1)

ID	Identity Provider	E-Mail	First Name	Last Name	Actions
Enter user ID	Default identity provider				
[redacted]	MyCorporateIdp	[redacted]			

5. Now your role collection should have at least one user.	

EMS-DEMO / SAP-DEMO-SUBACC001 / My Role Collection

Role Collection: My Role Collection - Overview

Description:

Role Name	Role Template	Application Identifier
EM_Admin	EM_Admin	cscems-test!t964

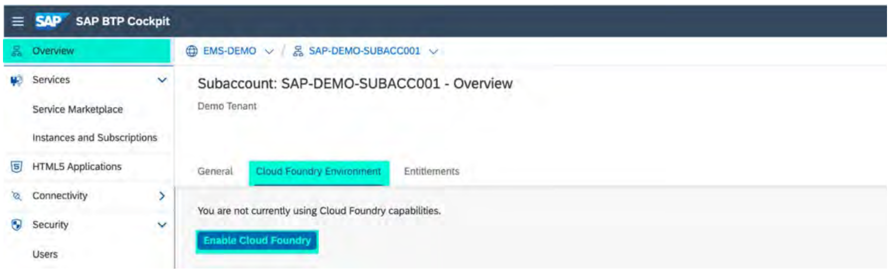
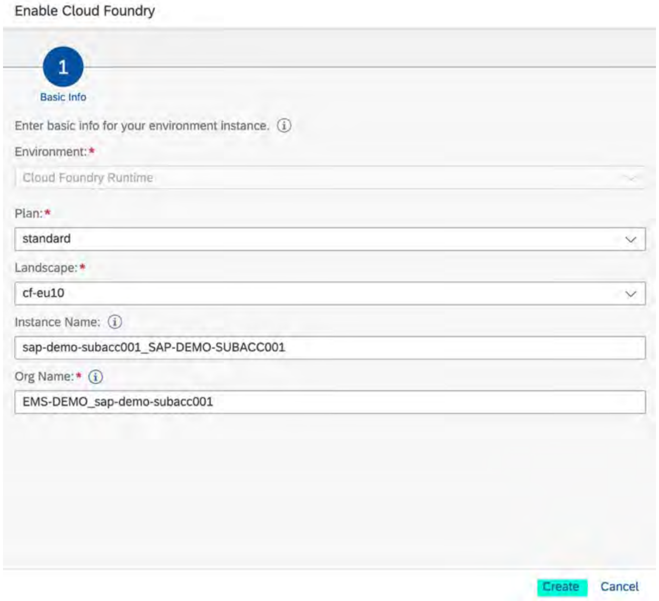
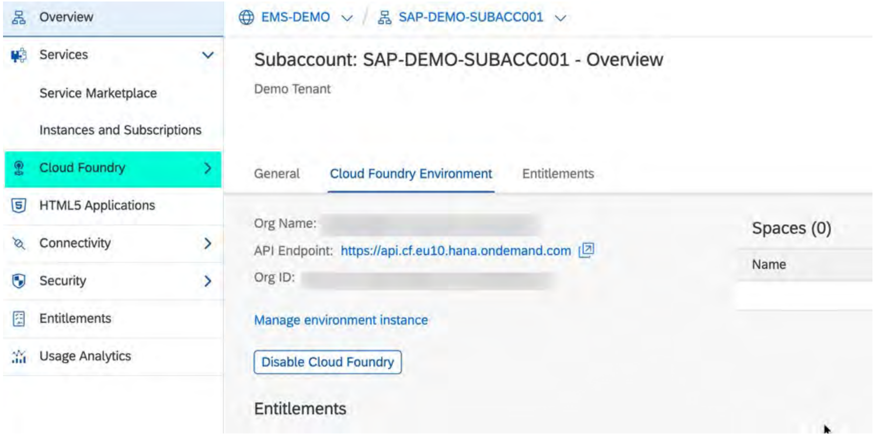
Users (1)

ID	Identity Provider	E-Mail	First Name	Last Name
[redacted]	MyCorporateIdp	[redacted]		

3. ENABLE API ACCESS

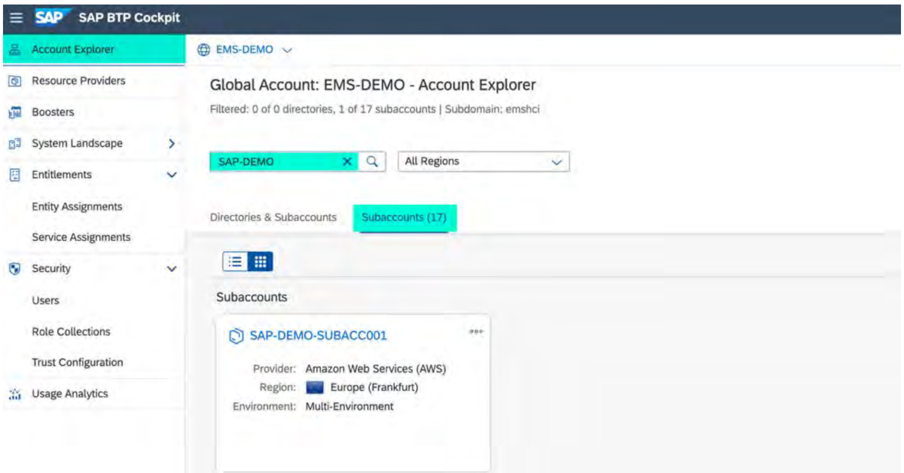
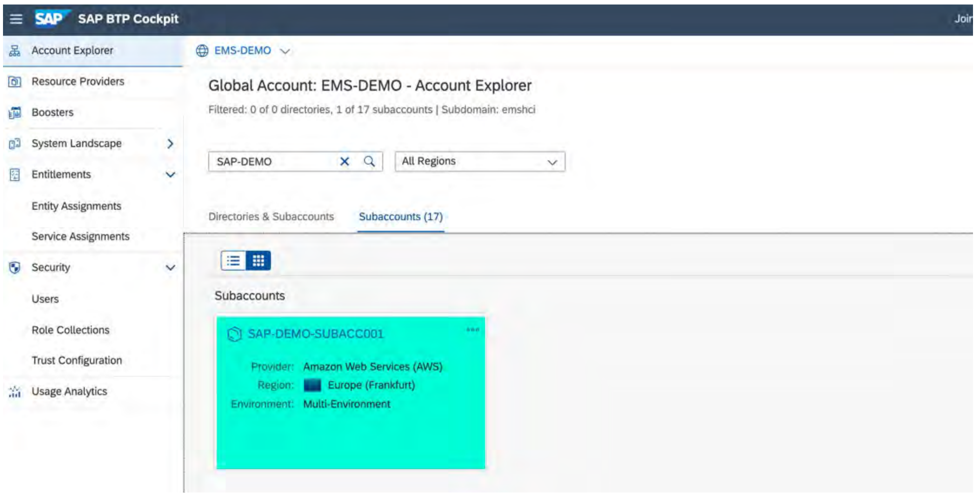
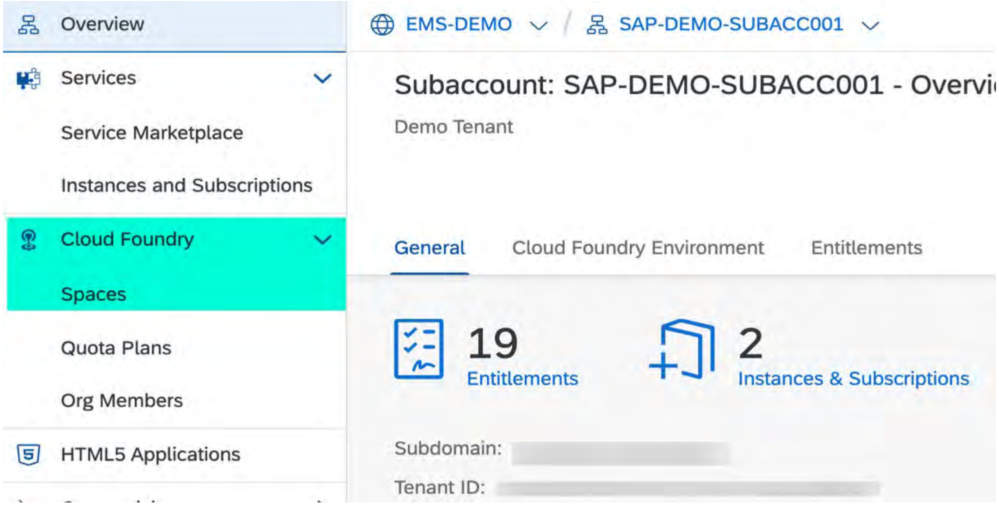
3.1 Enable Cloud Foundry

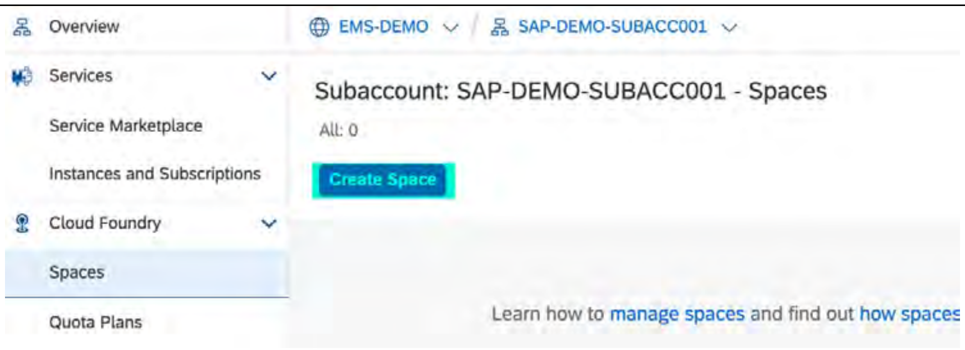
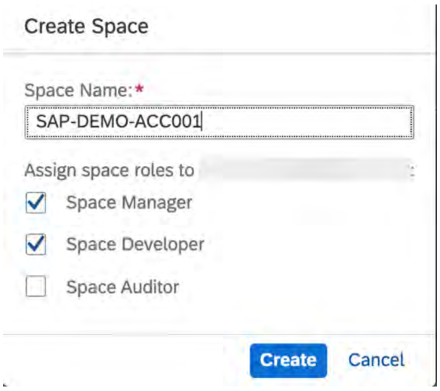
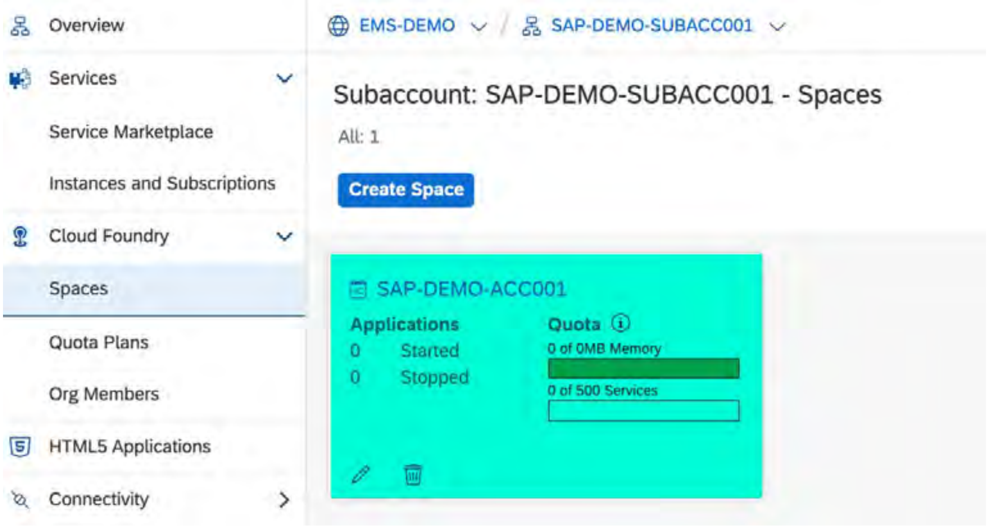
You need to set up the Cloud Foundry environment for your subaccount if you want to call **SAP Entitlement Management** OAuth APIs, develop your own applications, and process extensions on SAP BTP Cloud Foundry.

1. In your global account, open the subaccount. In the overview, select **Enable Cloud Foundry**.	 SAP BTP Cockpit Overview Services Service Marketplace Instances and Subscriptions HTML5 Applications Connectivity Security Users EMS-DEMO / SAP-DEMO-SUBACC001 General Cloud Foundry Environment Entitlements Enable Cloud Foundry Subaccount: SAP-DEMO-SUBACC001 - Overview Demo Tenant You are not currently using Cloud Foundry capabilities.
2. Enter an organization name and select **Create**. ⓘ In this guide, we use the automatic suggestion as the example name.	 Enable Cloud Foundry Enter basic info for your environment instance. Environment:* Cloud Foundry Runtime Plan:* standard Landscape:* cf-eu10 Instance Name: sap-demo-subacc001_SAP-DEMO-SUBACC001 Org Name:* EMS-DEMO_sap-demo-subacc001
3. Cloud Foundry is enabled.	 Overview Services Service Marketplace Instances and Subscriptions Cloud Foundry HTML5 Applications Connectivity Security Entitlements Usage Analytics EMS-DEMO / SAP-DEMO-SUBACC001 General Cloud Foundry Environment Entitlements Manage environment instance Disable Cloud Foundry Subaccount: SAP-DEMO-SUBACC001 - Overview Demo Tenant Org Name: [redacted] API Endpoint: https://api.cf.eu10.hana.ondemand.com Org ID: [redacted] Spaces (0) Name Entitlements

3.2 Create a Space

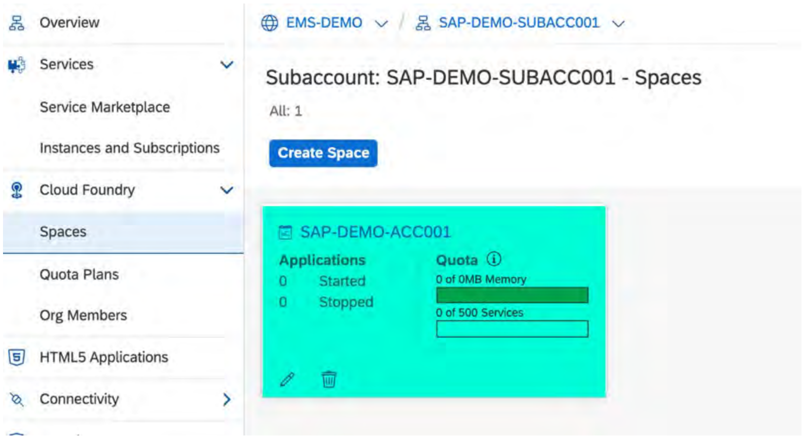
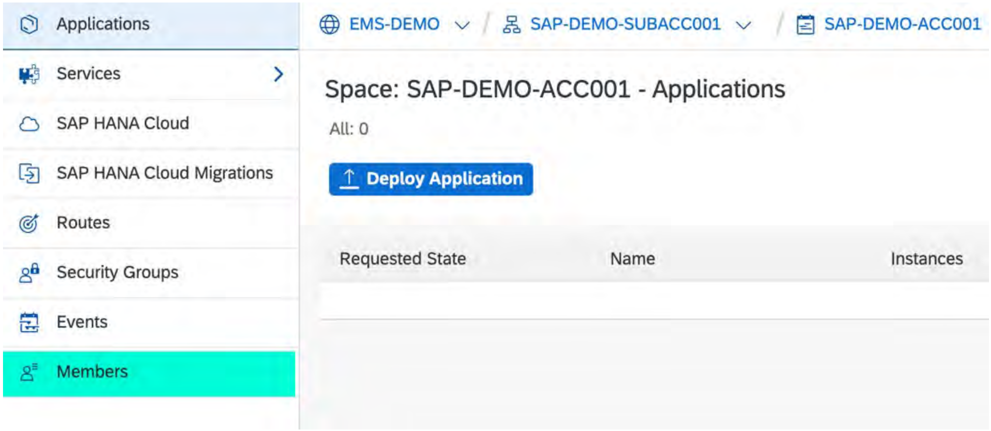
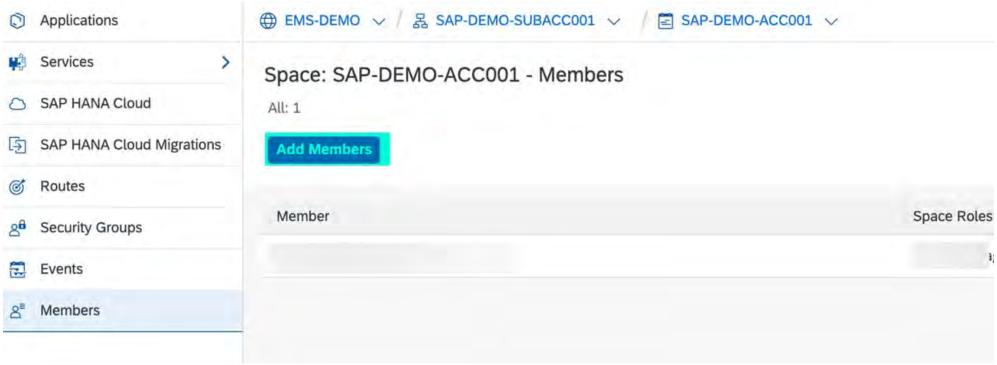
The Cloud Foundry environment uses spaces within subaccounts to allow you to deploy applications or services. You need at least one space to create the service instance that provides credentials for access to the **SAP Entitlement Management** OAuth APIs and enables further integration capabilities.

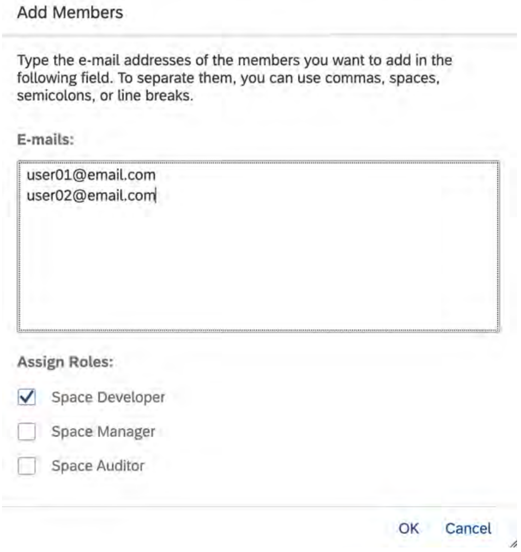
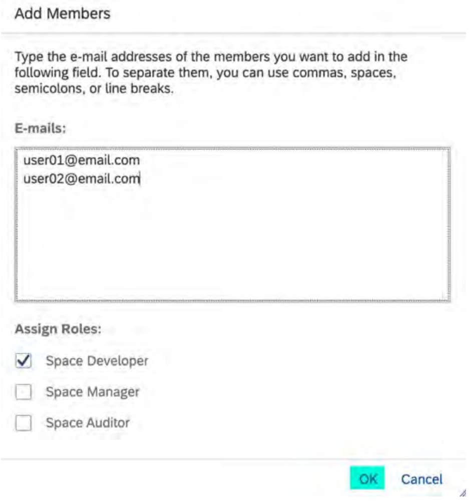
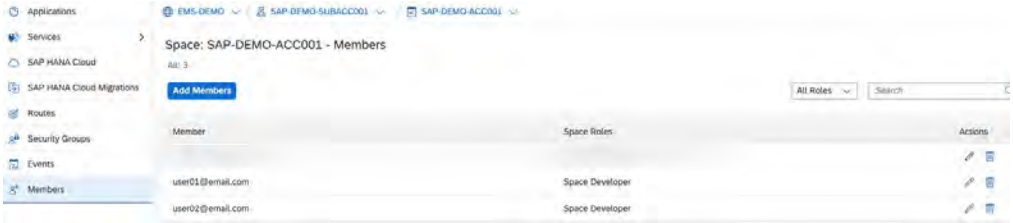
1. Choose **Subaccounts** in the navigation panel.	 SAP BTP Cockpit Account Explorer Resource Providers Boosters System Landscape Entitlements Entity Assignments Service Assignments Security Users Role Collections Trust Configuration Usage Analytics EMS-DEMO Global Account: EMS-DEMO - Account Explorer Filtered: 0 of 0 directories, 1 of 17 subaccounts | Subdomain: emshci SAP-DEMO All Regions Directories & Subaccounts Subaccounts (17) Subaccounts SAP-DEMO-SUBACC001 Provider: Amazon Web Services (AWS) Region: Europe (Frankfurt) Environment: Multi-Environment
2. Choose the subaccount that contains the Cloud Foundry organization in which you'd like to create a space. ⓘ Subaccounts and orgs have a 1:1 relationship. They have the same name and therefore also the same navigation level in the cockpit.	 SAP BTP Cockpit Joir Account Explorer Resource Providers Boosters System Landscape Entitlements Entity Assignments Service Assignments Security Users Role Collections Trust Configuration Usage Analytics EMS-DEMO Global Account: EMS-DEMO - Account Explorer Filtered: 0 of 0 directories, 1 of 17 subaccounts | Subdomain: emshci SAP-DEMO All Regions Directories & Subaccounts Subaccounts (17) Subaccounts SAP-DEMO-SUBACC001 Provider: Amazon Web Services (AWS) Region: Europe (Frankfurt) Environment: Multi-Environment
3. Select **Cloud Foundry** → **Spaces** in the navigation panel.	 Overview Services Service Marketplace Instances and Subscriptions Cloud Foundry Spaces Quota Plans Org Members HTML5 Applications EMS-DEMO SAP-DEMO-SUBACC001 Subaccount: SAP-DEMO-SUBACC001 - Overvi Demo Tenant General Cloud Foundry Environment Entitlements 19 Entitlements 2 Instances & Subscriptions Subdomain: [redacted] Tenant ID: [redacted]

4. Select **Create Space**.	 Overview Services Service Marketplace Instances and Subscriptions Cloud Foundry Spaces Quota Plans EMS-DEMO SAP-DEMO-SUBACC001 Create Space Subaccount: SAP-DEMO-SUBACC001 - Spaces All: 0 Learn how to manage spaces and find out how spaces
5. Enter a space name, check the permissions you'd like to assign to your user, and then select **Create**. ⓘ In this guide, we use the same name as the subaccount for the space example.	 Create Space Space Name:* SAP-DEMO-ACC001 Assign space roles to [redacted] ☑ Space Manager ☑ Space Developer □ Space Auditor
6. Your space is created.	 Overview Services Service Marketplace Instances and Subscriptions Cloud Foundry Spaces Quota Plans Org Members HTML5 Applications Connectivity EMS-DEMO SAP-DEMO-SUBACC001 Create Space Subaccount: SAP-DEMO-SUBACC001 - Spaces All: 1 SAP-DEMO-ACC001 Applications 0 Started 0 Stopped Quota 0 of 0MB Memory 0 of 500 Services

3.3 Add members to spaces and assign roles

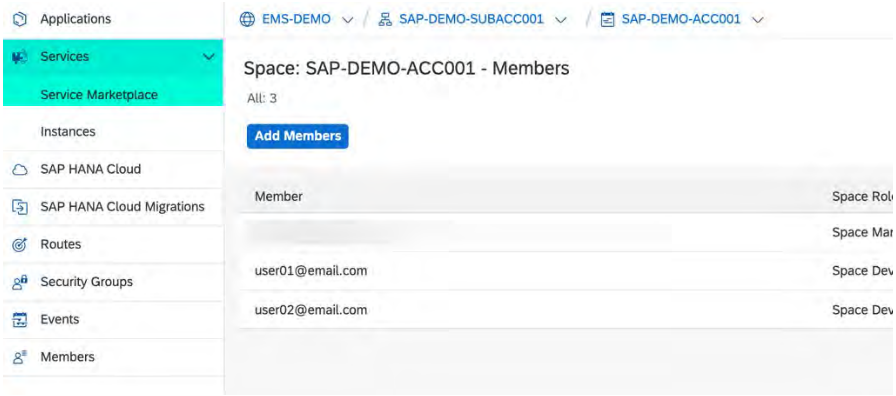
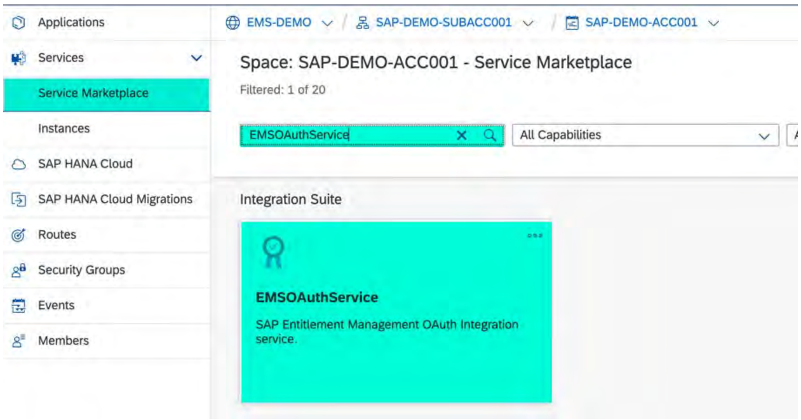
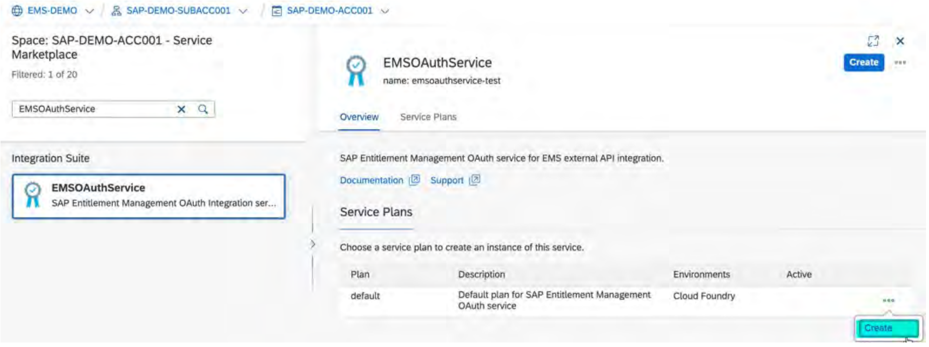
To allow users to configure access to SAP Entitlement Management APIs, you need to add them as members to your spaces and assign the relevant roles for authorization. Access configuration is described in the section Enable API Access in this guide.

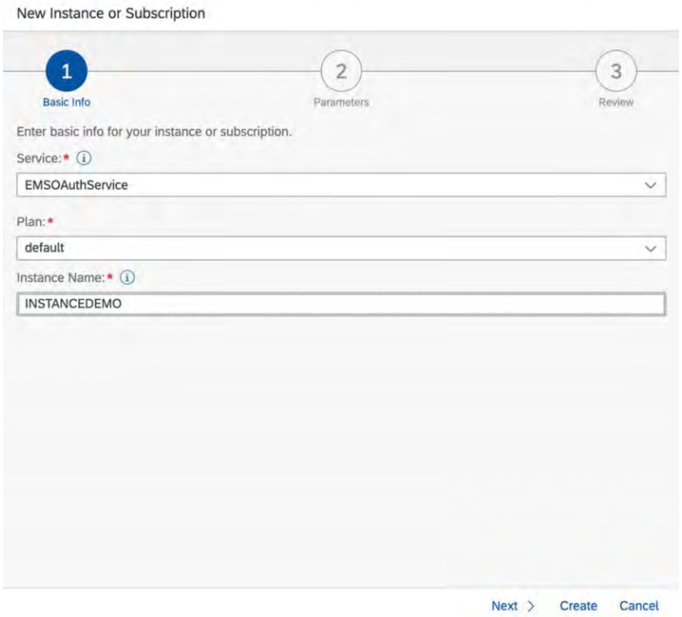
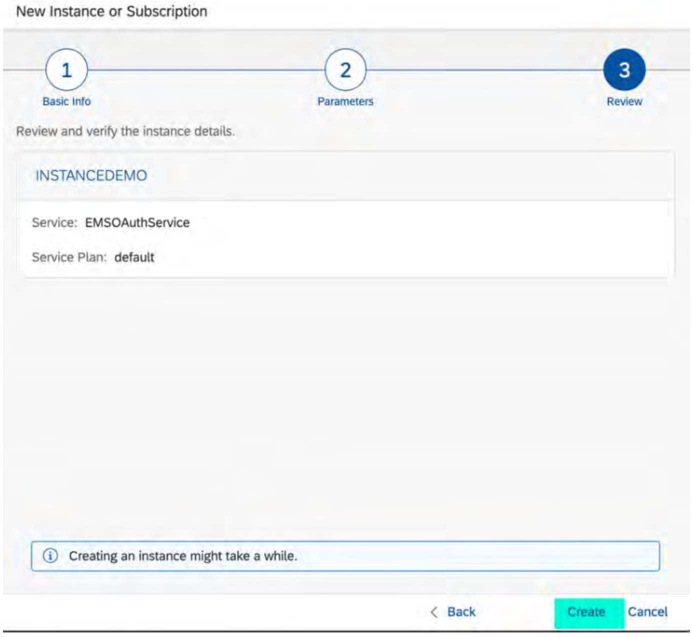
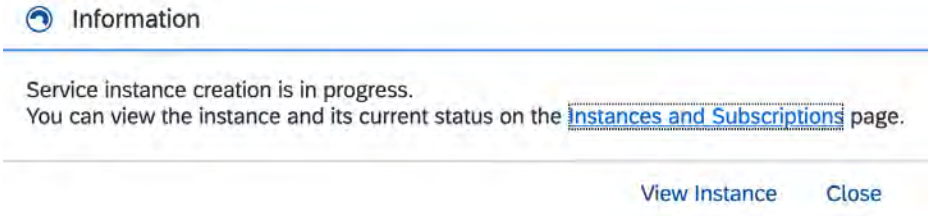
1. Access your **space**.	 Overview Services Service Marketplace Instances and Subscriptions Cloud Foundry Spaces Quota Plans Org Members HTML5 Applications Connectivity EMS-DEMO SAP-DEMO-SUBACC001 Subaccount: SAP-DEMO-SUBACC001 - Spaces All: 1 Create Space SAP-DEMO-ACC001 Applications 0 Started 0 Stopped Quota 0 of 0MB Memory 0 of 500 Services
2. To assign members and roles to instances, choose **Members** in the navigation panel.	 Applications Services SAP HANA Cloud SAP HANA Cloud Migrations Routes Security Groups Events Members EMS-DEMO SAP-DEMO-SUBACC001 SAP-DEMO-ACC001 Space: SAP-DEMO-ACC001 - Applications All: 0 Deploy Application Requested State Name Instances
3. Select **Add Members**.	 Applications Services SAP HANA Cloud SAP HANA Cloud Migrations Routes Security Groups Events Members EMS-DEMO SAP-DEMO-SUBACC001 SAP-DEMO-ACC001 Space: SAP-DEMO-ACC001 - Members All: 1 Add Members Member Space Roles

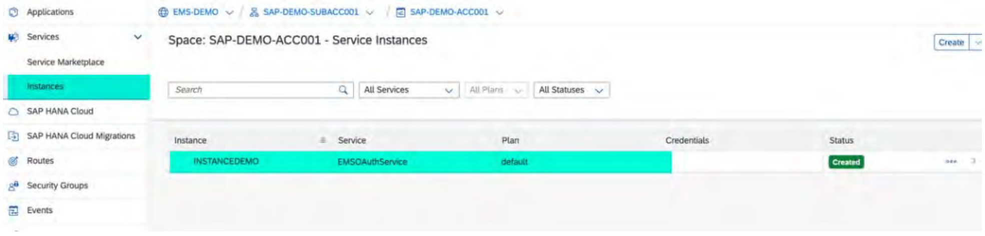
4. Enter the email addresses of the users that you want to add. ⓘ Members need the role “Space Developer” to read the credentials for the service instance. For more information about the Cloud Foundry roles, see the Cloud Foundry Documentation.	 Add Members Type the e-mail addresses of the members you want to add in the following field. To separate them, you can use commas, spaces, semicolons, or line breaks. E-mails: user01@email.com user02@email.com Assign Roles: ☑ Space Developer □ Space Manager □ Space Auditor OK Cancel
5. Select **OK** to save your changes.	 Add Members Type the e-mail addresses of the members you want to add in the following field. To separate them, you can use commas, spaces, semicolons, or line breaks. E-mails: user01@email.com user02@email.com Assign Roles: ☑ Space Developer □ Space Manager □ Space Auditor OK Cancel
6. The users are now members of your space.	 Applications Services SAP HANA Cloud SAP HANA Cloud Migrations Routes Security Groups Events Members EMS-DEMO SAP-DEMO-SUBACC001 SAP-DEMO-ACC001 Add Members All Roles Search Space: SAP-DEMO-ACC001 - Members All: 3 Member / Space Roles / Actions user01@email.com / Space Developer user02@email.com / Space Developer

3.4 Create a Service Instance

When you create an instance of the **SAP Entitlement Management** OAuth API service, you provide a set of scopes that define which of the APIs can be called and which activities can be done using service keys created for the instance.

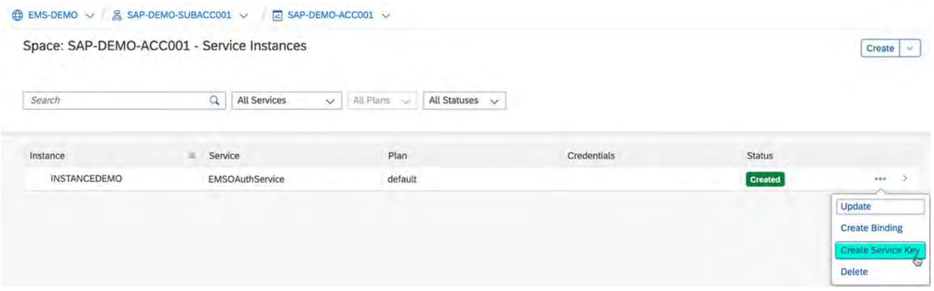
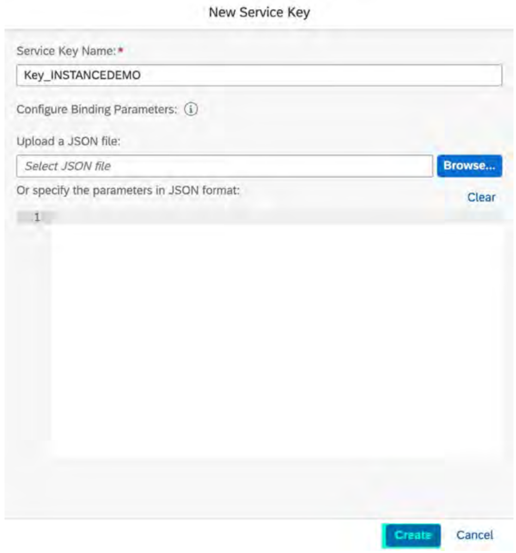
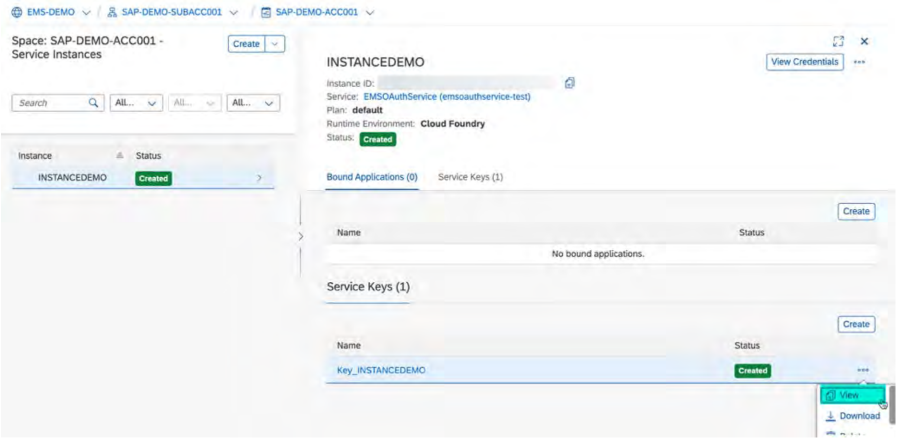
1. In your space, choose **Services → Service Marketplace** in the navigation panel.	 Applications Services Service Marketplace Instances SAP HANA Cloud SAP HANA Cloud Migrations Routes Security Groups Events Members EMS-DEMO SAP-DEMO-SUBACC001 SAP-DEMO-ACC001 Add MembersSpace: SAP-DEMO-ACC001 - Members All: 3 Member / Space Rol Space Mar user01@email.com — Space Dev user02@email.com — Space Dev
2. You will see all the services that are available to you. Search for and select the service **EMSOAuthService.**	 Applications Services Service Marketplace Instances SAP HANA Cloud SAP HANA Cloud Migrations Routes Security Groups Events Members EMS-DEMO SAP-DEMO-SUBACC001 SAP-DEMO-ACC001 All Capabilities Integration SuiteSpace: SAP-DEMO-ACC001 - Service Marketplace Filtered: 1 of 20 EMSOAuthService **EMSOAuthService** SAP Entitlement Management OAuth Integration service.
3. Under **Service Plans**, display the action menu of the plan for which you want to create an instance and select **Create**. ⓘ In this guide, we use the default plan for the example.	 EMS-DEMO SAP-DEMO-SUBACC001 SAP-DEMO-ACC001 Integration Suite Create Overview Service Plans Documentation Support CreateSpace: SAP-DEMO-ACC001 - Service Marketplace Filtered: 1 of 20 EMSOAuthService **EMSOAuthService** SAP Entitlement Management OAuth Integration ser... EMSOAuthService name: emsoauthservice-test SAP Entitlement Management OAuth service for EMS external API integration. Service Plans Choose a service plan to create an instance of this service. Plan: default — Description: Default plan for SAP Entitlement Management OAuth service — Environments: Cloud Foundry — Active

4. Name the instance and select **Next**. ⓘIn this guide, we use “INSTANCEDEMO” as the example name.	 New Instance or Subscription Enter basic info for your instance or subscription. Service:* EMSOAuthService Plan:* default Instance Name:* INSTANCEDEMO 1 Basic Info 2 Parameters 3 Review Next > Create Cancel
5. Check that everything is correct and select **Create**.	 New Instance or Subscription Review and verify the instance details. INSTANCEDEMO Service: EMSOAuthService Service Plan: default ⓘ Creating an instance might take a while. 1 Basic Info 2 Parameters 3 Review < Back Create Cancel
6. The creation process starts. Select **View Instance** to switch to the **Instances** screen.	 Information Service instance creation is in progress. You can view the instance and its current status on the Instances and Subscriptions page.

7. Your instance is created.	 Applications Services Service Marketplace Instances SAP HANA Cloud SAP HANA Cloud Migrations Routes Security Groups Events EMS-DEMO / SAP-DEMO-SUBACC001 / SAP-DEMO-ACC001 Create Search All Services All Plans All Statuses Space: SAP-DEMO-ACC001 - Service Instances Instance: INSTANCEDEMO Service: EMSOAuthService Plan: default Credentials: Status: Created

3.5 Create a Service Key

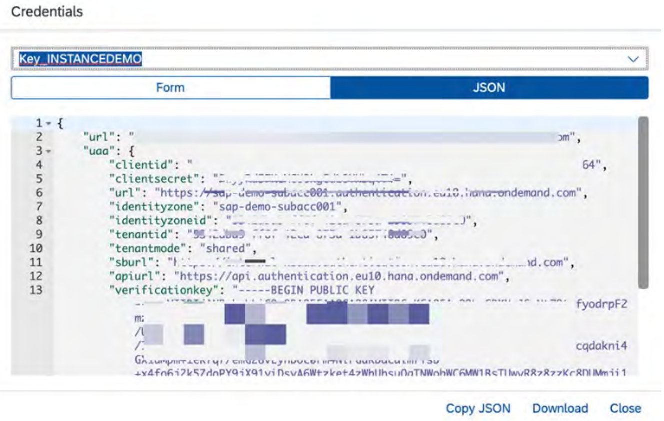
To access APIs, technical users need a service key to get an access token.

1. In the **Instances** screen, display the action menu of the instance and choose **Create Service Key**.	 EMS-DEMO / SAP-DEMO-SUBACC001 / SAP-DEMO-ACC001 Create Search All Services All Plans All Statuses Update Create Binding Create Service Key Delete Space: SAP-DEMO-ACC001 - Service Instances Instance · Service · Plan · Credentials · Status INSTANCEDEMO · EMSOAuthService · default · · Created
2. Name the service key and select **Create**.	 New Service Key Service Key Name:* Key_INSTANCEDEMO Configure Binding Parameters: Upload a JSON file: Select JSON file Or specify the parameters in JSON format: 1
3. To see the newly created service key, display its action menu and select **View**.	 EMS-DEMO / SAP-DEMO-SUBACC001 / SAP-DEMO-ACC001 Create Search All... View Credentials Bound Applications (0) Service Keys (1) Create View Download Space: SAP-DEMO-ACC001 - Service Instances Instance · Status INSTANCEDEMO · Created INSTANCEDEMO Instance ID: [redacted] Service: EMSOAuthService (emsoauthservice-test) Plan: default Runtime Environment: Cloud Foundry Status: Created Name · Status No bound applications. Service Keys (1) Name · Status Key_INSTANCEDEMO · Created

4. The details of the service key are displayed.

ⓘ The service key contains the information needed to generate an access token to access the APIs of **SAP Entitlement Management**.

For information on generating a token, see Generate an Access Token in the *API Guide*.



Credentials

Key_INSTANCEDEMO

```
{
    "url": "[redacted]om",
    "uaa": {
        "clientid": "[redacted]64",
        "clientsecret": "[redacted]",
        "url": "https:/[redacted]ondemand.com",
        "identityzone": "sap-demo-subacc001",
        "identityzoneid": "[redacted]",
        "tenantid": "[redacted]",
        "tenantmode": "shared",
        "sburl": "[redacted]d.com",
        "apiurl": "https://api.authentication.eu10.hana.ondemand.com",
        "verificationkey": "-----BEGIN PUBLIC KEY
            [redacted] fyodrpF2
            m[redacted]
            /[redacted]
            /[redacted] cqdakni4
            G[redacted]
            +x4fo6j2k57doPY9jX91viDsvA6Wtzket4zWhUhsuQqTNWohWC6MW1RsTUwvR8z8zzKc8DUMmjj1
```

4. Demo Videos

SAP Entitlement Management Test Tenant Onboard(US)
SAP Entitlement Management Production Tenant Onboard(US)

SAP Entitlement Management Test Tenant Onboard(EU)
SAP Entitlement Management Production Tenant Onboard(EU)

SAP Entitlement Management Addon Test Tenant Onboard(EU)

MORE INFORMATION

If you need more details, including explanations of the SAP BTP concepts, refer to the documentation Getting Started with an Enterprise Account in the Cloud Foundry Environment, where you can use the interactive graphics to navigate to more information.

www.sap.com/contactsap

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

THE BEST RUN SAP