

# Configuring SAP® Business Technology Platform

The Practical Guide for Administrators

- › Set up SAP Business Technology Platform in your landscape
- › Configure global accounts, subaccounts, users, authentication, and more
- › Install and activate key services such as SAP Integration Suite and SAP Build

Martin Koch  
Siegfried Zeilinger



**Rheinwerk**  
Publishing

# Contents

Preface .....	13
<b>1 Introduction to SAP BTP</b> .....	<b>17</b>
1.1 History and Positioning .....	19
1.2 License Models, Service-Level Agreements, and Important Documents .....	22
1.3 Global Accounts and Subaccounts .....	26
1.4 SAP Discovery Center .....	29
1.5 Entitlements and Service Plans .....	36
1.6 Best Practices .....	40
1.6.1 Structure of a Governance Model .....	41
1.6.2 Structure of an Account Model .....	44
1.6.3 Setting Up a Security and Compliance Model .....	50
1.6.4 Reference Architectures .....	52
1.7 Troubleshooting .....	53
1.8 Resources .....	55
1.9 Summary .....	56
<b>2 User Administration</b> .....	<b>57</b>
2.1 Security and Authorizations .....	57
2.1.1 Basics of Secure Communication .....	58
2.1.2 Authentication .....	62
2.1.3 Authorization .....	71
2.2 SAP Cloud Identity Services .....	72
2.2.1 Identity Authentication .....	72
2.2.2 Identity Provisioning .....	101
2.3 Summary .....	109

<b>3</b>	<b>Advanced Identity Authentication Service Topics</b>	<b>111</b>
<b>3.1</b>	<b>SAML 2.0</b>	<b>112</b>
<b>3.2</b>	<b>OpenID Connect</b>	<b>114</b>
<b>3.3</b>	<b>Practical Example: Identity Authentication as a Proxy to Microsoft Entra ID</b>	<b>118</b>
3.3.1	Integrate Microsoft Entra ID into Identity Authentication with SAML 2.0	118
3.3.2	Integrate Microsoft Entra ID into Identity Authentication with OpenID Connect	131
<b>3.4</b>	<b>Practical Example: Two-Factor Authentication/Risk-Based Authentication</b>	<b>144</b>
<b>3.5</b>	<b>Practical Example: Conditional Authentication</b>	<b>150</b>
<b>3.6</b>	<b>Summary</b>	<b>153</b>
<b>4</b>	<b>Global Account Administration</b>	<b>155</b>
<b>4.1</b>	<b>Access to the Global Account</b>	<b>156</b>
<b>4.2</b>	<b>Authentication and Authorization Management</b>	<b>157</b>
4.2.1	User Management	157
4.2.2	Roles and Role Collections	166
4.2.3	Practical Example: Setting Up Authentication via SAP Cloud Identity Service	169
<b>4.3</b>	<b>Directories</b>	<b>175</b>
<b>4.4</b>	<b>Boosters</b>	<b>182</b>
<b>4.5</b>	<b>System Landscape</b>	<b>188</b>
<b>4.6</b>	<b>Resource Provider</b>	<b>190</b>
<b>4.7</b>	<b>Entitlements</b>	<b>192</b>
<b>4.8</b>	<b>Usage Monitoring</b>	<b>193</b>
<b>4.9</b>	<b>Summary</b>	<b>196</b>

---

<b>5</b>	<b>Subaccount Administration</b>	199
----------	----------------------------------	-----

---

<b>5.1</b>	<b>Creating a Subaccount</b>	199
<b>5.2</b>	<b>Authentication and Authorization</b>	204
5.2.1	User Administration	206
5.2.2	Trust Configuration and Other Identity Providers	208
5.2.3	Roles and Role Collections	215
5.2.4	Practical Example: Authentication on a Subaccount with Identity Authentication	227
5.2.5	Practical Example: Subaccount with Microsoft Entra ID as the Identity Provider	233
<b>5.3</b>	<b>Organizations, Spaces, and Quotas</b>	241
<b>5.4</b>	<b>Subscriptions and Services</b>	247
<b>5.5</b>	<b>SAP Audit Log Viewer Service for SAP BTP</b>	249
<b>5.6</b>	<b>Summary</b>	250

<b>6</b>	<b>Cloud Connector</b>	253
----------	------------------------	-----

---

<b>6.1</b>	<b>Installation and Configuration</b>	253
6.1.1	Prerequisites	254
6.1.2	Installing the Cloud Connector	255
6.1.3	Initial Steps	261
6.1.4	Configuring the User Interface	264
6.1.5	Cloud Configuration	267
6.1.6	On-Premise Configuration	270
6.1.7	Reporting Configuration	274
6.1.8	Advanced Configuration	275
<b>6.2</b>	<b>Ensuring High Availability</b>	276
<b>6.3</b>	<b>SAP Connectivity Service</b>	286
<b>6.4</b>	<b>Summary</b>	295



---

<b>7</b>	<b>Activating and Setting Up SAP Business Application Studio</b>	<b>297</b>
----------	--	------------

---

7.1	Setting Up SAP Business Application Studio .....	297
7.2	Granting Authorizations .....	303
7.3	Working with Dev Spaces .....	304
7.4	Using External Systems .....	305
7.5	Versioning with Git Repositories .....	311
7.6	Summary .....	321

<b>8</b>	<b>Activating and Setting Up SAP Integration Suite</b>	<b>323</b>
----------	--	------------

---

8.1	Functions and History of SAP Integration Suite .....	323
8.2	Creating a Subaccount and Assigning Entitlements .....	326
8.3	Creating a Subscription .....	329
8.4	Activating Capabilities .....	334
8.5	Instantiating the SAP Process Integration Runtime .....	341
8.6	Create Service Key .....	344
8.7	Summary .....	347

<b>9</b>	<b>Activating and Setting Up SAP Cloud Transport Management for SAP Integration Suite</b>	<b>349</b>
----------	---	------------

---

9.1	Activating SAP Cloud Transport Management .....	350
9.2	Deploying SAP Cloud Transport Management .....	352
9.3	Creating a System Landscape in SAP Cloud Transport Management .....	361
9.4	Adding the SAP Content Agent Service to a Subaccount .....	365
9.5	Configuring SAP Cloud Transport Management in SAP Integration Suite .....	380
9.6	Summary .....	389

---

<b>10</b>	<b>Activating and Setting Up SAP Build</b>	391
<hr/>		
<b>10.1</b>	<b>SAP Build Apps</b>	391
10.1.1	Installation	393
10.1.2	Configuration	399
<b>10.2</b>	<b>SAP Build Process Automation</b>	404
<b>10.3</b>	<b>SAP Build Work Zone</b>	412
10.3.1	Initial Steps	412
10.3.2	Run the Booster	418
10.3.3	Configuring SAP Build Work Zone, Advanced Edition	422
<b>10.4</b>	<b>SAP Build Code</b>	438
<b>10.5</b>	<b>Summary</b>	444
The Authors		445
Index		447

# Chapter 4

## Global Account Administration

*When you dive into the world of SAP BTP, your journey begins with the assignment of a global account. This central element is far more than just a user account; it is the control center for cloud resources, licenses, and user management. A comprehensive understanding of global account management is essential to fully unlock the potential of SAP BTP.*

As soon as you license SAP BTP services, you receive a global account. Originally, the idea was that each organization would have exactly one global account. However, in practice, organizations may have multiple global accounts. This can happen, for example, when organizations use the integration services of SAP BTP in addition to an SaaS product like SAP SuccessFactors. You may also receive two global accounts if you acquire some services through a subscription model and others via a Cloud Platform Enterprise Agreement (CPEA). Global accounts are provided only by SAP and cannot be created independently by organizations. In general, the global account is where you consolidate your subaccounts and define overall (global) settings.

Global accounts are geographically independent, unlike the next level down—the subaccount level—where you can choose the region in which each subaccount is hosted. At the global account level, you manage the licenses available in your organization and allocate them to different environments where development takes place or where your cloud solutions are productively operated. It is the entry point for managing and grouping subaccounts and for assigning resources and licenses.

In Section 4.1, you will learn how to access your global account and switch between multiple global accounts. Section 4.2 covers user management in the global account, including roles and role collections. This topic is less complex than it is for the subaccount level, but it is important to note that admin permissions in the global account are very powerful and therefore critical. In Section 4.3, you will learn how to use directories to organize and authorize subaccounts in a structured way. Section 4.4 introduces boosters, which are used in the SAP BTP environment to speed up new subscriptions and administrative tasks. Further information about the system landscape and the resource providers as administrative units spanning subaccounts can be found in Section 4.5 and Section 4.6. How to assign resources or services using entitlements is explained in Section 4.7. Section 4.8 finally addresses the topic of usage monitoring. In

this last section, you will learn how to monitor key performance indicators and use your resources efficiently to make the most of SAP BTP.

## 4.1 Access to the Global Account

You can access your SAP BTP cockpit via `https://<region>.cockpit.btp.cloud.sap/cockpit/#/globalaccount/`, changing `<region>` to, for example, `us10`. Until recently, registration was handled at `https://hana.ondemand.com/`. This URL still works, but it will redirect the request. After successful authentication, you will be redirected to the global account you last viewed (see Figure 4.1).

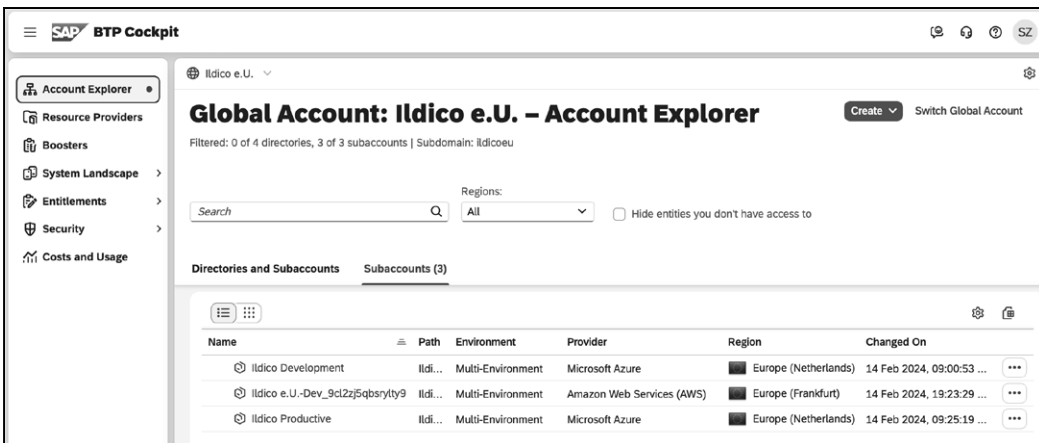


Figure 4.1 Overview of Subaccounts After Logging into Global Account

If you have more than one global account, you can switch between them by clicking the **Switch Global Account** link (see Figure 4.2).

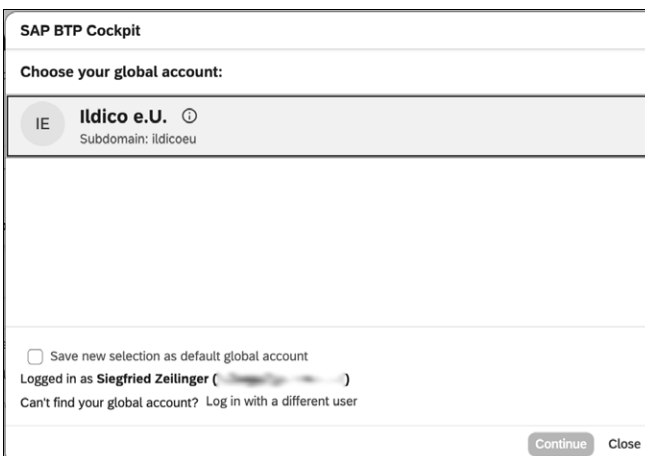


Figure 4.2 Switching Between Global Accounts

A global account can have as many subaccounts as you like, which you can create and manage yourself. The creation and management of subaccounts is described in more detail in Chapter 5.

### Lost Subaccount Privileges

From the global account, you can use the **Add Me as Admin** function in the context menu of each subaccount to get authorization for that subaccount. This is especially helpful if there has been a change in administration or if someone is suddenly unavailable. These actions are of course documented in the audit log.



## 4.2 Authentication and Authorization Management

User authentication at the global account level is first performed by the SAP ID service. You typically log on with your S-user that is defined for the global account. This S-user will be sent a welcome email and is responsible for the administration of the global account. They are the only one with initial access to Identity Authentication and is assigned the administrator role by default.

Recently, it has also become possible to use your own Identity Authentication service tenant for authentication in the SAP BTP cockpit. We will introduce this in Section 4.2.1 and will demonstrate a practical example in Section 4.2.3 by setting up a platform identity provider. Section 4.2.2 will cover roles and collective roles for granting permissions within the global account.

### 4.2.1 User Management

You can find the users of your global account under **Security • Users** in your SAP BTP cockpit (see Figure 4.3).

User Name	Identity Provider	Last Name	First Name	E-Mail	Last Updated	Last Logon	Actions
[Avatar]	Default identity provider	Zeilinger	Siegfried	[Avatar]	19 Feb 2023, 18:35:21 (GMT+01:00)	3 Mar 2025, 20:14:53 (GMT+01:00)	[Icons]

Figure 4.3 Users in Global Account



We recommend that you use at least two administrators as it's possible to be locked out of SAP BTP for an hour if you enter the wrong password. It is also useful to have a substitute in case of illness or vacation.



#### Who Needs Access to the Global Account?

From our point of view, only users who are involved in creating new subaccounts or monitoring and configuring existing ones, similar to the SAP Basis department, need access to the global account.

Users who develop or use an application in a subaccount do not need access to the global account as these users can be authorized in the subaccount and access to the global account does not provide any added value.

Persons from the auditing department, the internal audit department, and the works council may be granted read-only access to the global account (see Section 4.2.2).

The **Default Identity Provider** setting, as shown in Figure 4.3, means that the SAP ID service is configured. Authentication using this identity provider is sufficient. However, you can also use *SAP Cloud Identity Services*. This includes, among other elements, *Identity Authentication*, which can store data individually. This means that users who are authenticated using Identity Authentication do not necessarily need an account with SAP but can be created directly in Identity Authentication. Identity Authentication can also be used to pass the authentication to your local directory server (e.g., Microsoft Entra ID or Microsoft Active Directory on-premise). The decisive advantage of such a configuration is that the users exist in the lifecycle of your organization; that is, the validity data is transferred from your company servers and changes are therefore reflected in the global account administration.

Another aspect of setting up SAP Cloud Identity Services is that the included Identity Authentication service becomes a platform identity provider. It can be used in all subaccounts.

Identity Authentication is discussed in detail at the subaccount level in Chapter 5, Section 5.2.2, including an example of connecting Identity Authentication to a subaccount. Therefore, we abbreviate the content here. Connecting the global account is a side issue at this point.



#### Differences in Trust Configuration Between Subaccount and Global Account

In the global account, you have the following trust configuration options:

- SAP ID
- Identity Authentication tenant as a platform provider

In the subaccount, you can choose from among the following options:

- SAP ID
- Identity Authentication tenant
- SAML configuration

In the global account, you *cannot configure SAML directly*. However, doing so is possible via Identity Authentication. An important advantage of this is that all authentication methods involved in the global account are under SAP's control, and therefore you can get better help from SAP in case of a SAML error or a hack in your trusted system.

To add users, you can create a new user with **Create** (see Figure 4.4).

Figure 4.4 Creating New User

As shown in Figure 4.5, enter the mail address of the new user. The underlying S-user or P-user must be associated with the email address entered.

User Name	Identity Provider	Last Name	First Name	E-Mail	Last Updated	Last Logon	Actions
testaccount@ildico.com	Default identity provider			testaccount@ildico.com	3 Mar 2025, 20:22:05 (GMT+01:00)		[Edit] [Delete]
Zeilinger Siegfried	Default identity provider	Zeilinger	Siegfried		19 Feb 2023, 18:35:21 (GMT+01:00)	3 Mar 2025, 20:14:53 (GMT+01:00)	[Edit] [Delete]

**testaccount@ildico.com**

Identity Provider: Default identity provider

Last Logon: [Edit] [Delete]

**Overview** **Role Collections**

E-Mail: testaccount@ildico.com

Created: 3 Mar 2025, 20:22:05 (GMT+01:00)

ID: cb58a395-e95c-4563-b69a-0045adcb0026

Last Updated: 3 Mar 2025, 20:22:05 (GMT+01:00)

**Role Collections**

[Search] [Assign Role Collection]

Name	Description	Action
No role collections have been assigned to this user yet		

Figure 4.5 Created User with User Details Opened

After creating the user, you can select a **Role Collection** in the lower-right area. For more information about role collections, see Section 4.2.2.

For test purposes, click **Assign Role Collection** and assign the **Global Account Viewer** role to the new user (see Figure 4.6).

**Assign Role Collection**

Search

Name	Description
<input type="checkbox"/> Directory Admin	
<input type="checkbox"/> Global Account Administrator	Administrative access to the global account
<input checked="" type="checkbox"/> Global Account Viewer	Read-only access to the global account

Global Account Viewer

Figure 4.6 Assigning Role Collection to User

Click **Assign Role Collection** again to assign the collection role. Figure 4.7 shows the assigned composite role in the user overview under **Role Collections**.

**SAP BTP Cockpit**

Global Account: Ildico e.U. - Users

Search  Last Updated: All Hasn't Logged On: All

User Name	Identity Provider	Last Name	First Name	E-Mail	Last Updated	Last Logon	Actions
testaccount@ildico.com	Default identity provider			testaccount@ildico.com	3 Mar 2025, 20:22:05 (GMT+01:00)		<input type="button" value="Edit"/>
	Default identity provider	Zellinger	Siegfried		19 Feb 2023, 18:35:21 (GMT+01:00)	3 Mar 2025, 20:14:53 (GMT+01:00)	<input type="button" value="Edit"/>

**testaccount@ildico.com**

Identity Provider: Default identity provider  
Last Logon:

**Role Collections**

Search  Assign Role Collection

Name	Description	Action
Global Account Viewer	Read-only access to the global account	<input type="button" value="X"/>

Figure 4.7 Result: User with Assigned Role Collection

## Users in SAP ID

Users that you assign with an SAP ID authentication type must also be known in your company with the same email address. To ensure this, you can register an SAP Universal ID (a P-user) or—and this is what we recommend—register an S-user via your company. This way, you have the account validity under control.

If you have not yet created the selected user in your company, go to <https://me.sap.com/userscontacts/usermanagement> and log onto SAP for Me as a user administrator. Once there, click **Users & Contacts** (see Figure 4.8).

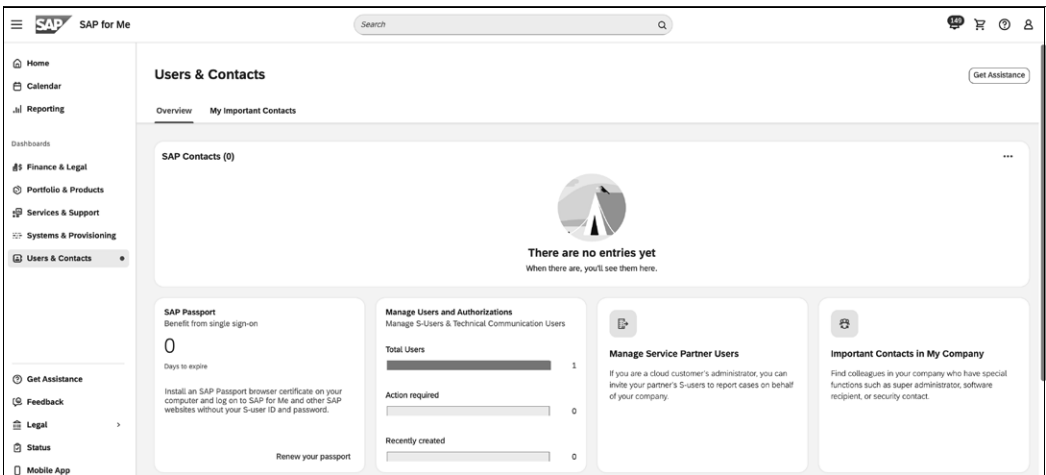


Figure 4.8 Logging onto SAP Support User Management

On the next screen (see Figure 4.9), create a new user for your company by choosing **Request User**.

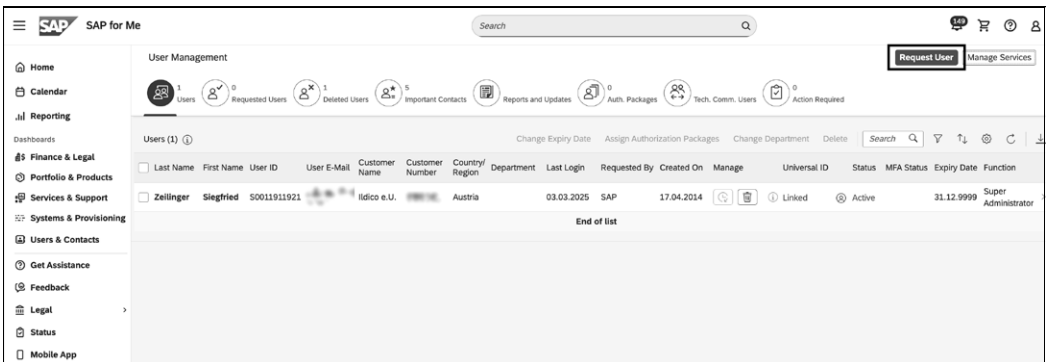



Figure 4.9 User Overview in SAP for Me

On the **Request User** screen, enter your **First Name**, **Last Name**, and **Email** address, then click **Submit** (see Figure 4.10).

**Figure 4.10** SAP for Me: User Request Screen

Now you will receive a success message and after a certain activation period (typically about 60 minutes, depending on the time of day), the user is ready for login.

In a new browser window, you can enter the link to your new global account and log on with the email address of the newly created user.

After logging in (see Figure 4.11), you can immediately see from the lock icon  beside the **Subaccount** label that you have read-only access to the global account (because you have only assigned the Global Account Viewer role).

Back in the user overview, you can see that the newly created user now shows a date in the **Last Logon** field, which works as expected (see Figure 4.12).



### Difference Between S-Users and P-Users

Note another difference between S-users and P-users: S-users expire after two years and must be renewed by a user administrator in SAP for Me. P-users and the assignments in the default identity provider never expire; the role collection must be removed from them at least, but in fact we recommend deleting them from the global account. You can still use the audit log to see who accessed the global account and when.



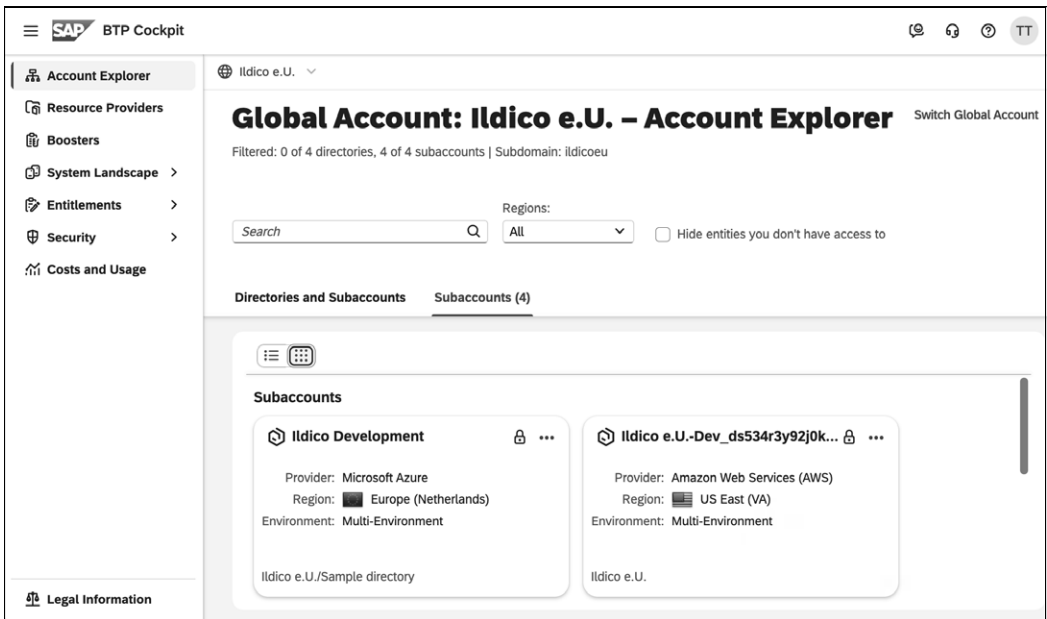


Figure 4.11 Read-Only Access with Test User Just Created

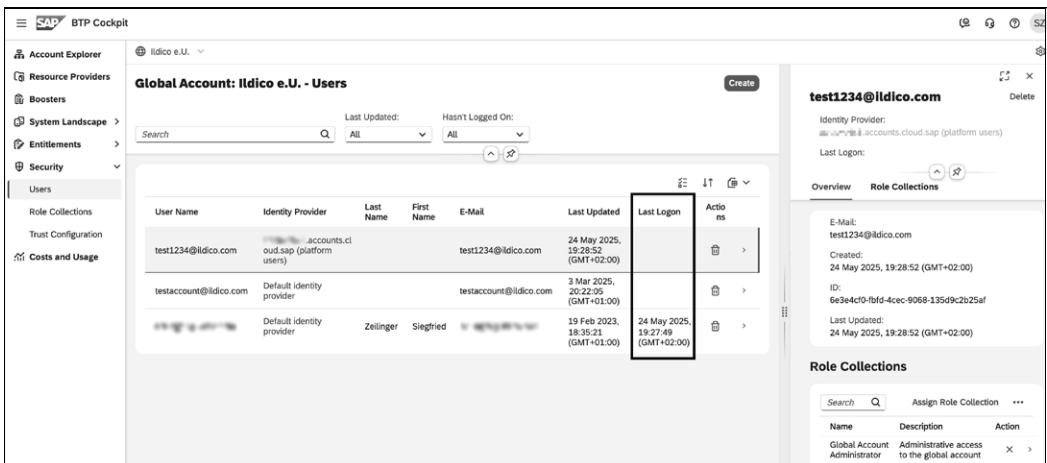


Figure 4.12 Last Login Date in User Overview

We have already written several times about the default identity provider. In the SAP BTP cockpit of your global account, click **Security • Trust Configuration**. There you will see the linked identity providers, as shown in Figure 4.13.

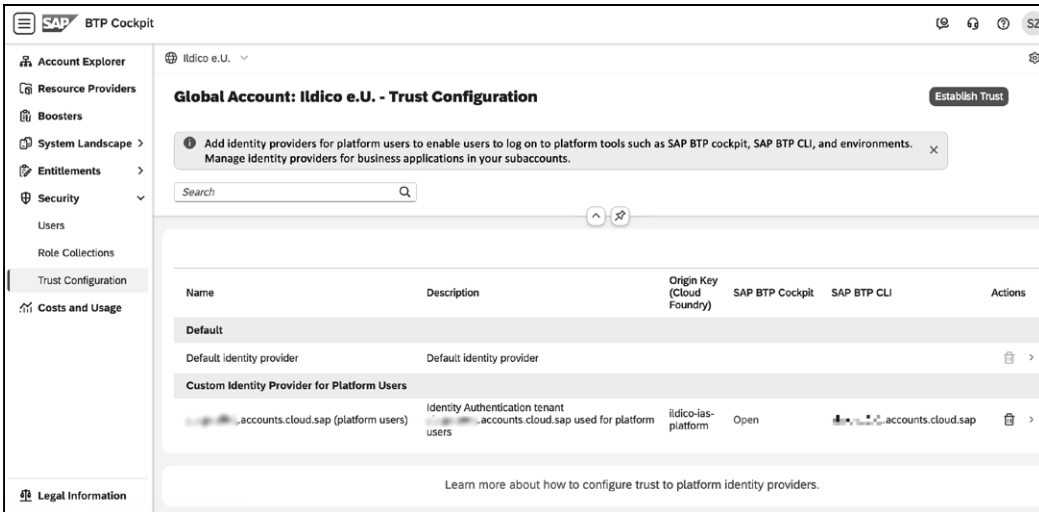


Figure 4.13 Trust Configuration with SAP ID: Default Identity Provider

Below the default identity provider, you can see a custom identity provider. (Section 4.2.3 describes how to create this identity provider.) You can also authorize users of this identity provider in your SAP BTP cockpit. You also can also jump to the provider (the underlying tenant of the Identity Authentication service) using the **Open** button.

Because we will discuss this in more detail later in this chapter, we have added a user from Identity Authentication as the global administrator in this example (see Figure 4.14).

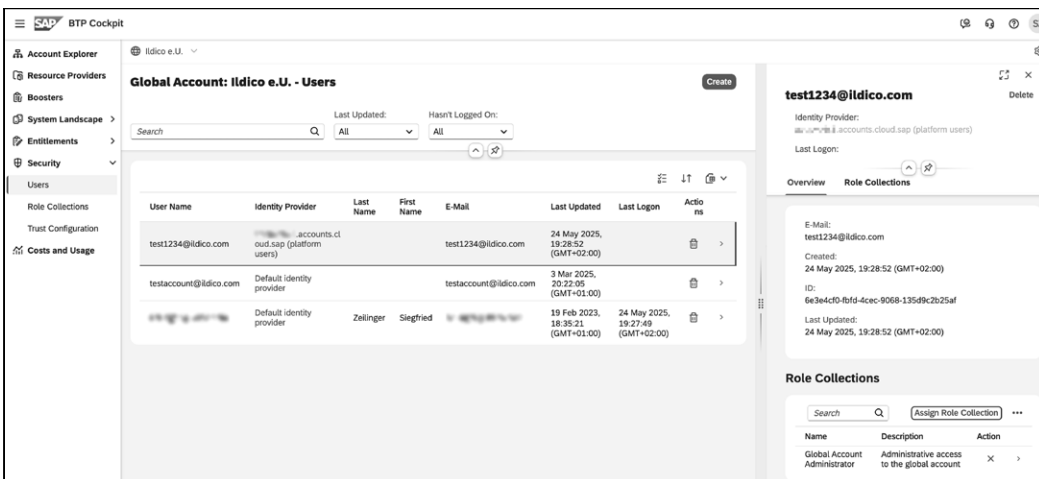


Figure 4.14 Example of Identity Authentication User in User List of Global Account

As you can see in Figure 4.15, you can now configure multifactor authentication (via the **Multi-Factor Authentication** menu item) in Identity Authentication and also define a user lifecycle with start and end dates (**Valid From** and **Valid To**, shown in Figure 4.16).

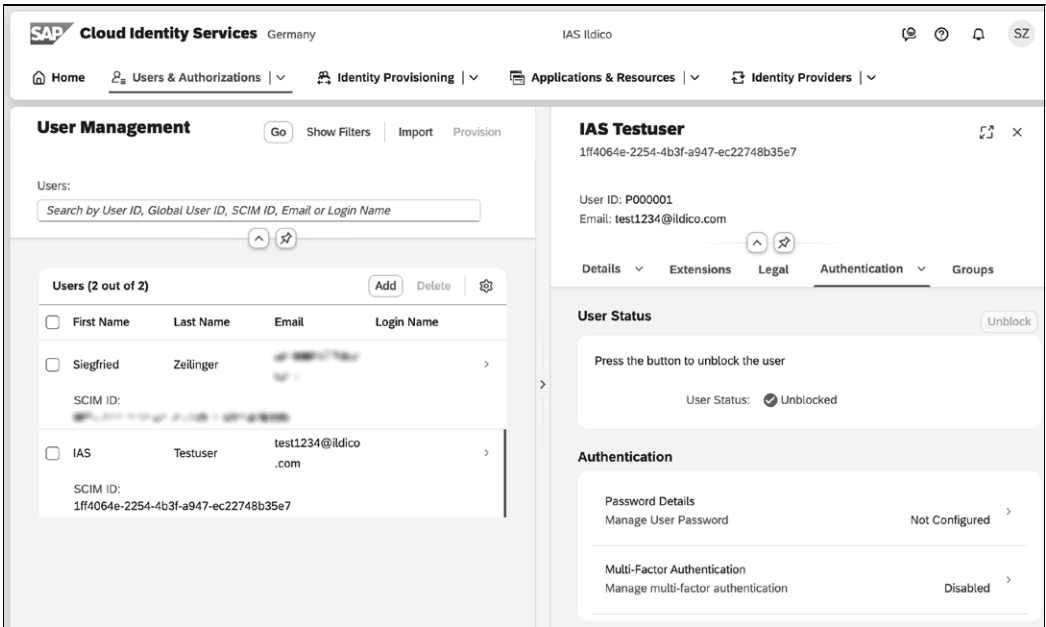


Figure 4.15 Test User in Identity Authentication Tenant

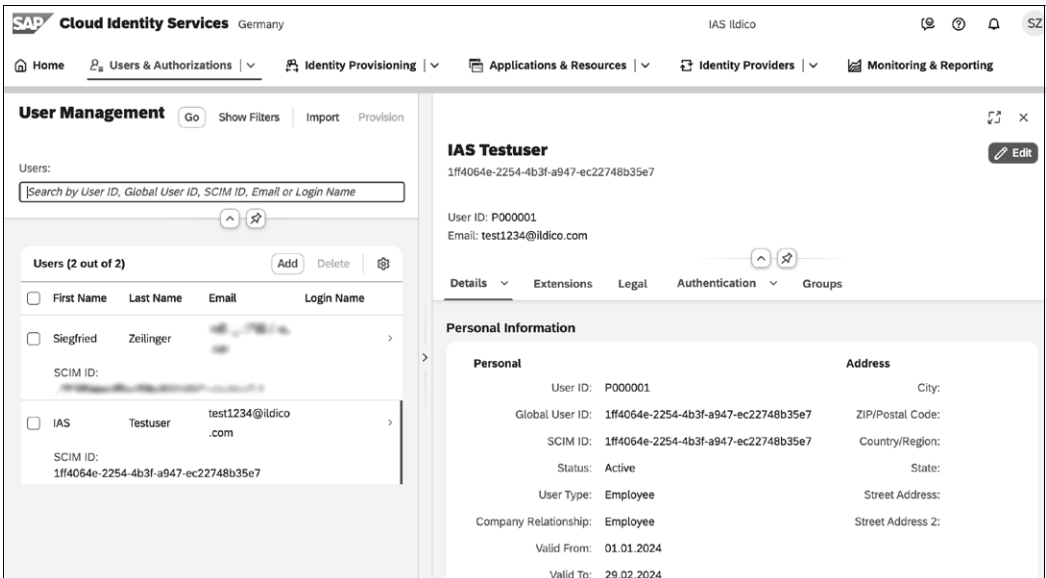


Figure 4.16 User Details with Test User Start and End Dates



### Practical Considerations for Using Identity Authentication and Global Accounts

We recommend connecting global account administration users via Identity Authentication and using two-factor authentication. We also recommend deactivating SAP ID because it does not provide two-factor authentication and because it locks accounts for one hour if a password is entered incorrectly. This is very important in case of an attack.

Some administrators store a *break glass* account (i.e., an emergency access account) in SAP ID and keep the password safe. If you wish to do so, please make sure that the break glass account mailbox is forwarded and checked. If you receive any suspicious messages (e.g., login attempts or attempted password resets), change the username.

For particularly tricky scenarios, you can also consider having a separate domain that is not associated with your company, which you can then use for administrative users (e.g., *domain1.dev*). This prevents dictionary attacks with well-known company names in the critical infrastructure in the cloud.

## 4.2.2 Roles and Role Collections

In the global account, SAP delivers collections of roles. In a standard installation, the following three role collections are available for selection:

### ■ Global Account Administrator

This role collection provides full access to the global account. You can manage users; create, modify, and delete subaccounts; and manage technical settings such as quotas and permissions (more on technical topics in Section 4.7). This kind of user also has the right to act as administrator for any of the subaccounts.

### ■ Global Account Viewer

This can be used to view the entire global account in read-only mode.

### ■ Directory Admin

This role allows the administration of directories, which group the subaccounts. These are described in more detail in Section 4.3.

The role collections contain roles, also called *single roles*. You can copy these roles and create new ones to model your own permissions. Figure 4.17 shows the access to the role collections via the **Security • Role Collections** menu path. Here you can see the default roles we just mentioned.

If you click the > icon at the end of the line, you can see the roles contained in the collection and the users assigned to them. Figure 4.18 shows the **Directory Admin** role, which contains an **Admin** role for editing, a **Viewer** role for viewing, and a **Usage Reporting Viewer** role for running reports.

Figure 4.19 shows the contents of the **Global Account Administrator** collection role, which contains all the individual roles for the global account, the system landscape administrator, and the user administration.

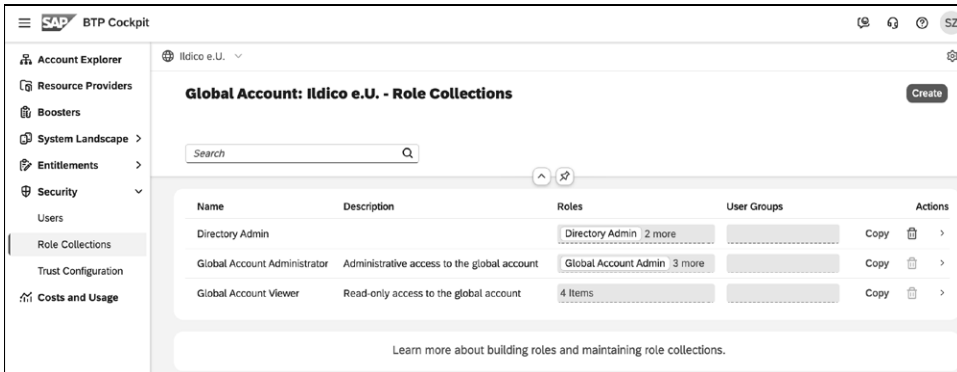


Figure 4.17 Overview of Role Collections in Global Account

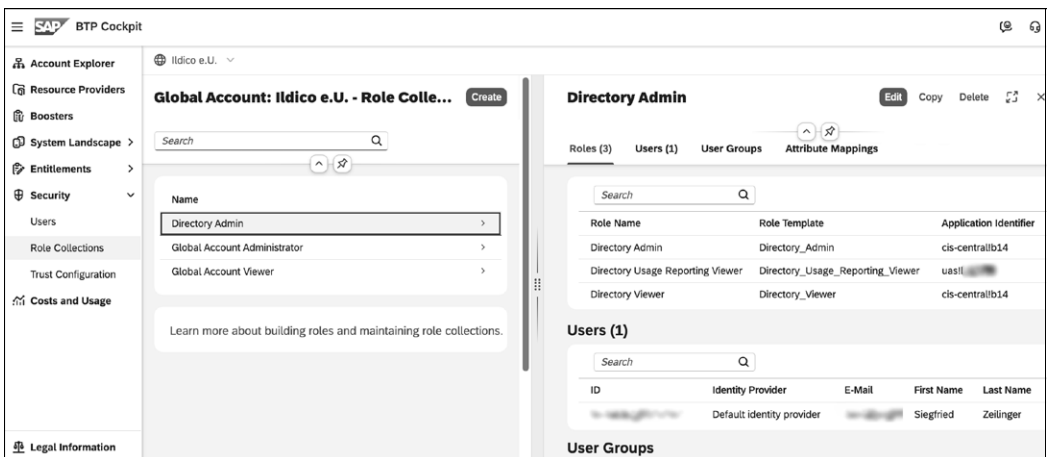


Figure 4.18 Individual Roles Assigned to Composite Role and Overview of Assigned Users

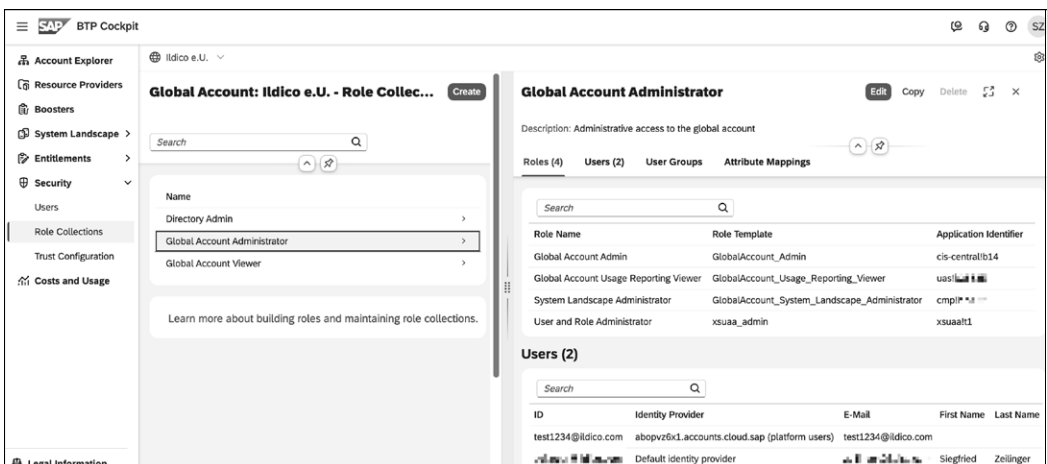


Figure 4.19 Contents of Global Account Administrator Role



Finally, Figure 4.20 shows the permissions contained in the **Global Account Viewer** role.

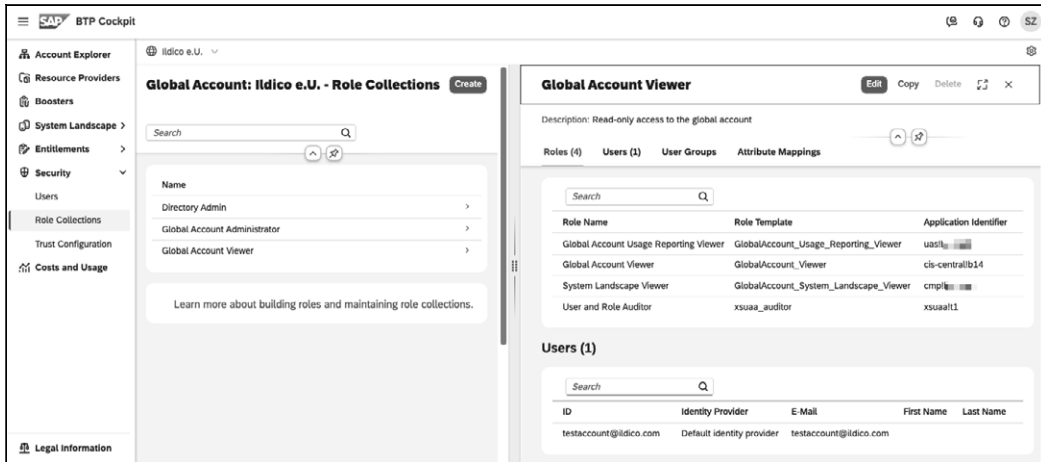


Figure 4.20 Global Account Viewer Composite Role

If you want to create your own role collection, click **Create** in the overview of the composite roles. A dialog opens (see Figure 4.21), in which you must enter a unique **Name**. Click **Create** when you're finished.

The 'Create Role Collection' dialog box is shown. It has a title bar 'Create Role Collection'. Inside, there are two input fields: 'Name: \*' and 'Description:'. The 'Name' field contains the text 'Ildico Admin'. Below the 'Description' field, there are two buttons: 'Create' and 'Cancel'.

Figure 4.21 Creating Role Collection

You will now see an empty role in the overview (see Figure 4.22), which you can edit by clicking the > icon and the **Edit** button.

Now you can assign individual roles to each other in the edit mode under **Role Name** and—if desired—to users under **Users** (see Figure 4.23).

You cannot create single roles yourself. However, new single roles are created when services are added or when directories are created, which you can copy to your own single roles.

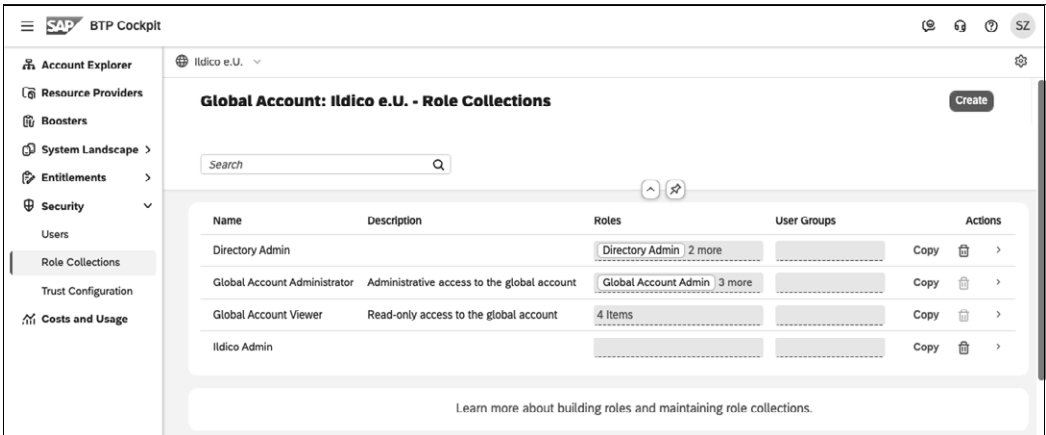


Figure 4.22 Display of Roles, Including Newly Created Composite Role

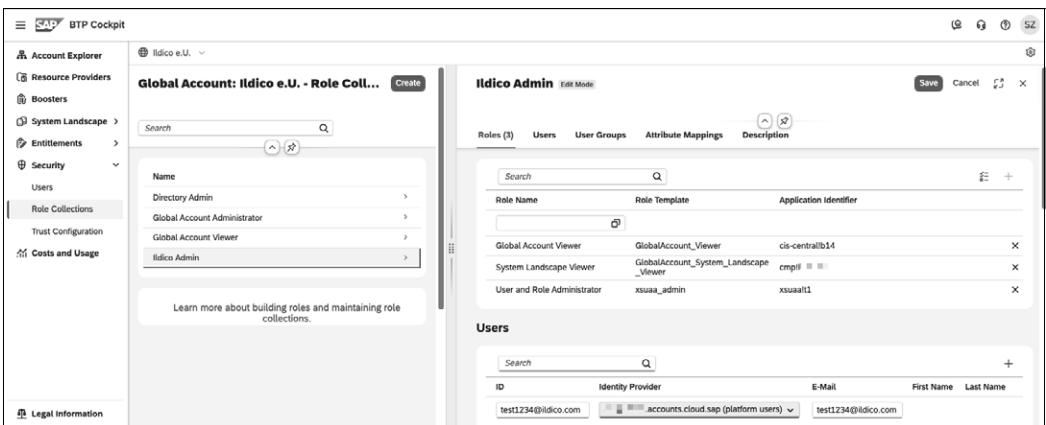


Figure 4.23 Edit Mode for Composite Role

When naming new roles, note that they should not start with the same name as the SAP default roles (e.g., do not use Global Account Editor for your own role). This is for protection in case SAP wants to extend its collection of roles. Including a company name is recommended, rather than having the roles start with Y or Z as in old ABAP times.

### 4.2.3 Practical Example: Setting Up Authentication via SAP Cloud Identity Service

In this practical example, we will show you how to set up authentication via SAP Cloud Identity Services, which Identity Authentication is a part of, in the global account. A more detailed explanation of SAP Cloud Identity Services can be found in Chapter 5, Section 5.2.4, where this topic is described in more detail for subaccounts, and the initial setup is also described in more detail.

First create a new subaccount in the SAP BTP cockpit in the global account under **Account Explorer** using **Create • Subaccount** (see Figure 4.24).

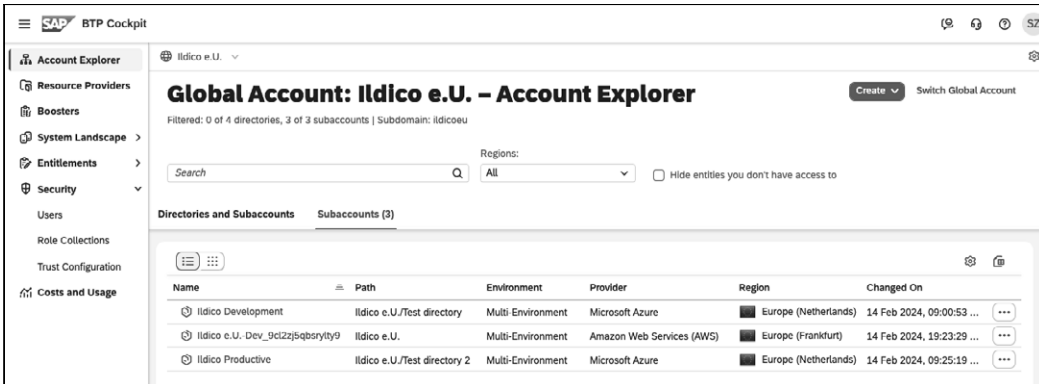


Figure 4.24 Account Explorer in SAP BTP Cockpit

Figure 4.25 shows an example of a creation dialog. Chapter 5 describes which regions are options for SAP Cloud Identity Services—and almost all of them are. Enter a descriptive name (**Display Name**). You may also change the **Subdomain** to a more convenient term (e.g., “prod\_ids\_customername”) and set the **Parent** directory (more information on directories will be shown in Section 4.3). Create the subaccount with **Create**.

**Create Subaccount**

Display Name \*  
Ildico IDS|Subaccount

Description  
Subaccount for Cloud Identity Services

Region \*  
US East (VA)

Subdomain \* ⓘ  
ildico-ids-subaccount-89v22b10

Parent \*  
Ildico e.U.

> **Advanced**

Cockpit supports 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**.

Create Cancel

Figure 4.25 Subaccount Creation Dialog

During the creation of the subaccount, you will see a waiting icon, then the name will turn blue and you can log into the subaccount (see Figure 4.26). You will be taken to the **Overview** page (see Figure 4.27).

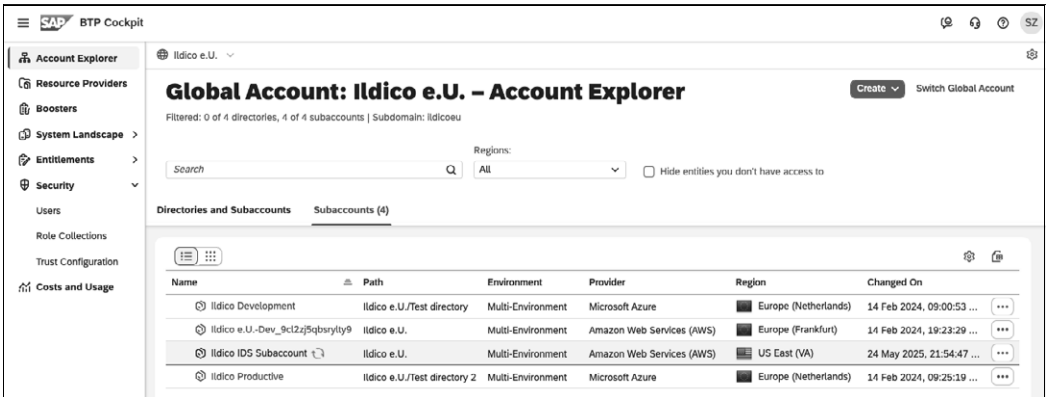


Figure 4.26 Subaccount Setup Progress Indication

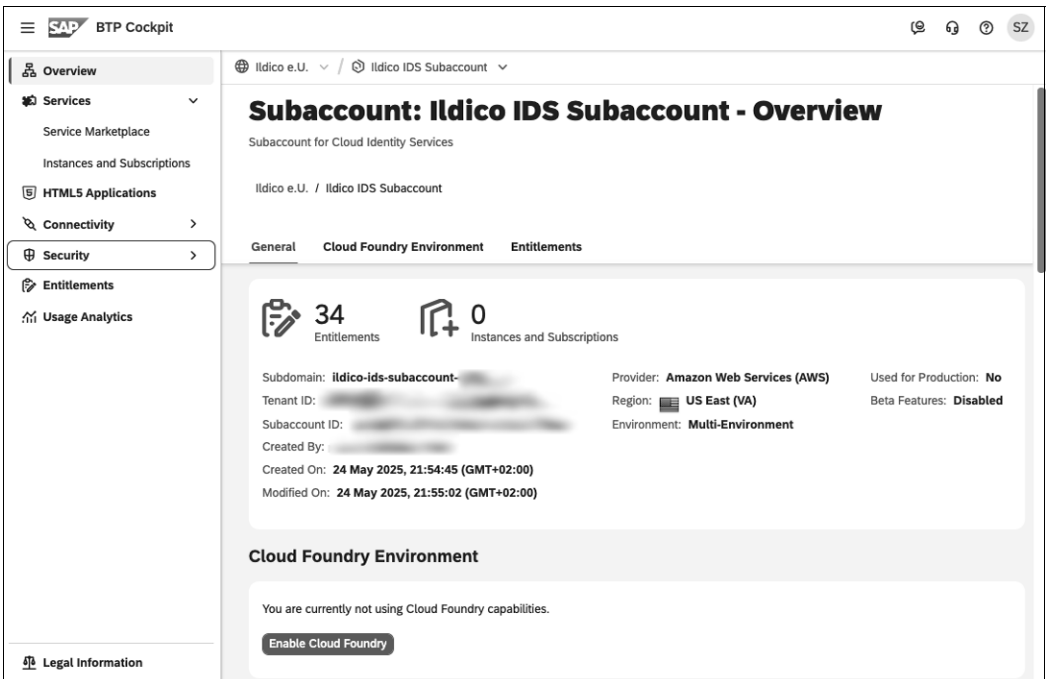


Figure 4.27 New Subaccount Overview Page

The first time you log into the subaccount, you can access the **Service Marketplace** directly from the home page of the subaccount via **Services • Service Marketplace**, as shown in Figure 4.28.

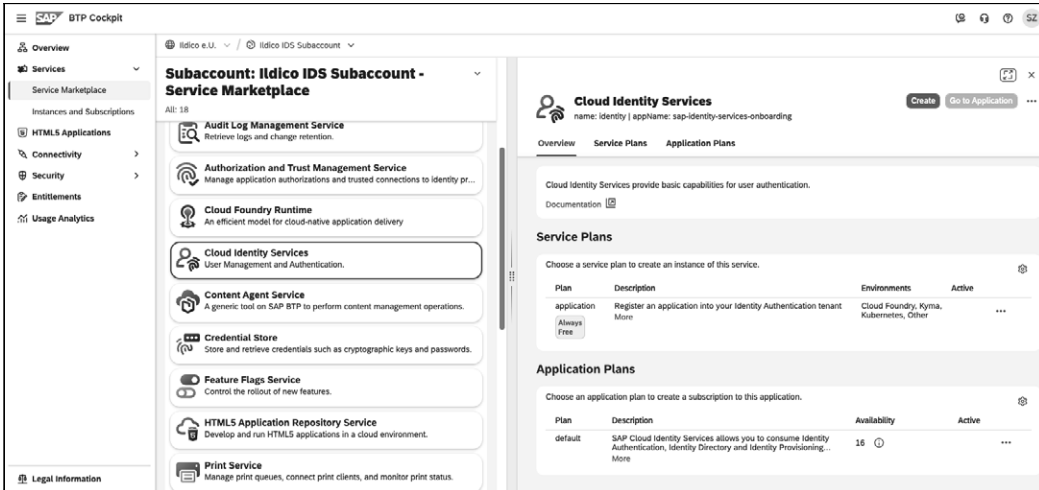


Figure 4.28 SAP Service Marketplace

To create a new instance of SAP Cloud Identity Services in the SAP Service Marketplace, click **Create** (see Figure 4.28) and fill out the form, selecting **Cloud Identity Services** under **Service** (see Figure 4.29). Currently, the default plan option (**default** in the **Plan** dropdown) is the correct choice. This choice depends on your license agreement with SAP. To our knowledge, default is the only option for most organizations.

New Instance or Subscription

1

Basic Info

2

Parameters

3

Review

Enter basic info for your instance or subscription.

Some services are not shown because Cloud Foundry is not enabled. To enable it, select it from the Service dropdown menu and create an instance of it.

Service: \*

Cloud Identity Services

Can't find what you're looking for?

Plan: \*

default

☒

I understand that enabling a service might result in costs, depending on the plan selected. See Services Catalog

Next >

Create

Cancel

Figure 4.29 Creating Identity Authentication Tenant

Click **Create** to create the SAP Cloud Identity Services instance.

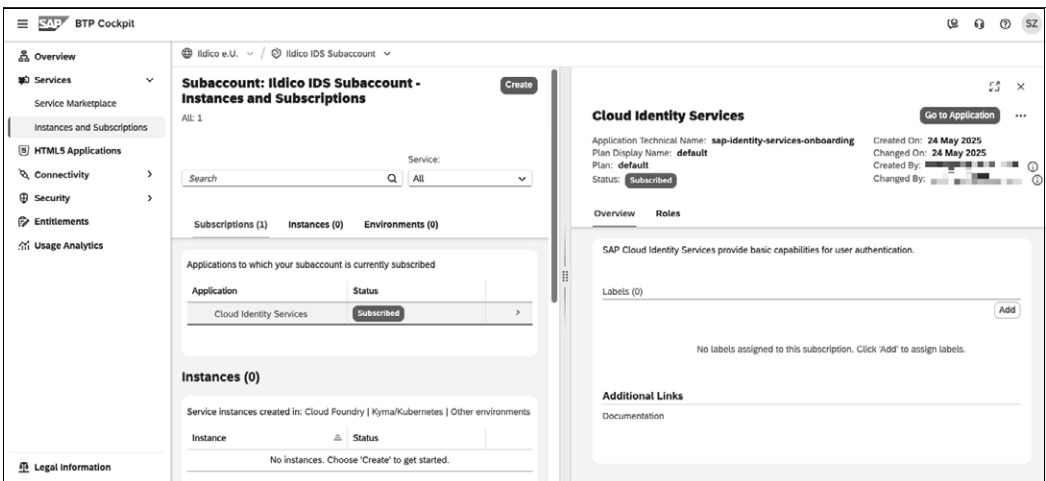


### SAP Cloud Identity Services Instance

The creation screen differs if you have already activated Cloud Foundry in your tenant. Compare Figure 4.29 with Figure 9.11 in Chapter 9: The difference is in the choice of space and runtime environment.

Also note that using SAP Cloud Identity Services means that a corresponding tenant for each global account is created once as a shared instance. This sharing means that creation happens only once and is then only shared. Our screenshots may not be 100% accurate at this point as an SAP Cloud Identity Services instance was already created on the training tenant beforehand.

You can view this instance in the SAP BTP cockpit under **Services • Instances and Subscriptions**, as shown in Figure 4.30.



**Figure 4.30** Overview of Instances and Subscriptions with Open SAP Cloud Identity Services Instance

This setup is sufficient for use with the global account. Additional options on the sub-account level are explored in Chapter 5.

Now navigate back to the SAP BTP cockpit of your global account under **Security • Trust Configuration**. Use **Establish Trust** to select the SAP Cloud Identity Service tenant to be used in the global account (see Figure 4.31).

Select your Identity Authentication tenant and click **Next**. On the next screen, select the internet domain under **Domain**. As shown in Figure 4.32, this should match the link in the browser and should end in *cloud.sap*. Click **Next**.

**Configure Tenant**

1 Choose Tenant — 2 Choose Domain — 3 Configure Parameters — 4 Review

### Choose Tenant

Choose the SAP Cloud Identity tenant for users when logging on to BTP cockpit and similar tools.

Search  Q | ↓↑

Status	Default Domain	Type	Data Center	Display Name	Custom Domain
	...accounts.ondemand.com	Productive	EU2_PROD	IDS Ildico	

Next Cancel

Figure 4.31 Selecting Identity Authentication Tenant

**Configure Tenant**

1 Choose Tenant — 2 Choose Domain — 3 Configure Parameters — 4 Review

### Choose Domain

For a good single sign-on experience, choose the same domain for all BTP accounts and non-BTP applications. Your choice applies to all global accounts that use this tenant.

Domain: \*  ▼

Previous Next Cancel

Figure 4.32 Browser Link and Domain Selection

Now enter the parameters (see Figure 4.33), ideally using a self-explanatory key for **Origin Key**. Click **Next** to get to the final overview, where you can complete the setup of the platform identity provider by clicking **Finish**.

**Configure Tenant**

1 Choose Tenant — 2 Choose Domain — 3 Configure Parameters — 4 Review

### Configure Parameters

Choose an origin key that is clear and easy for developers and operators to remember. They need the origin key when logging on to Cloud Foundry CLI or service dashboards. You can't change it later.

Name: \*

Description:

Origin Key: \*  -platform

Previous Next Cancel

Figure 4.33 Identity Authentication Connection Parameters

Pay attention to the final message shown in Figure 4.34: The configuration setup now is not only valid for the global account but is also available for *all* subaccounts (but does not have to be used).

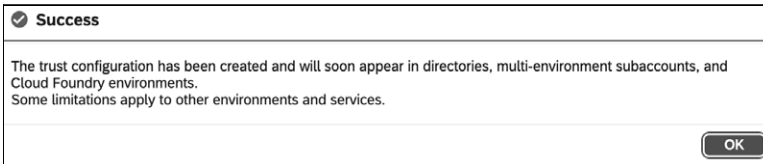


Figure 4.34 Final Message: Platform Identity Provider Has Been Set Up

The target screen is shown in Figure 4.35.

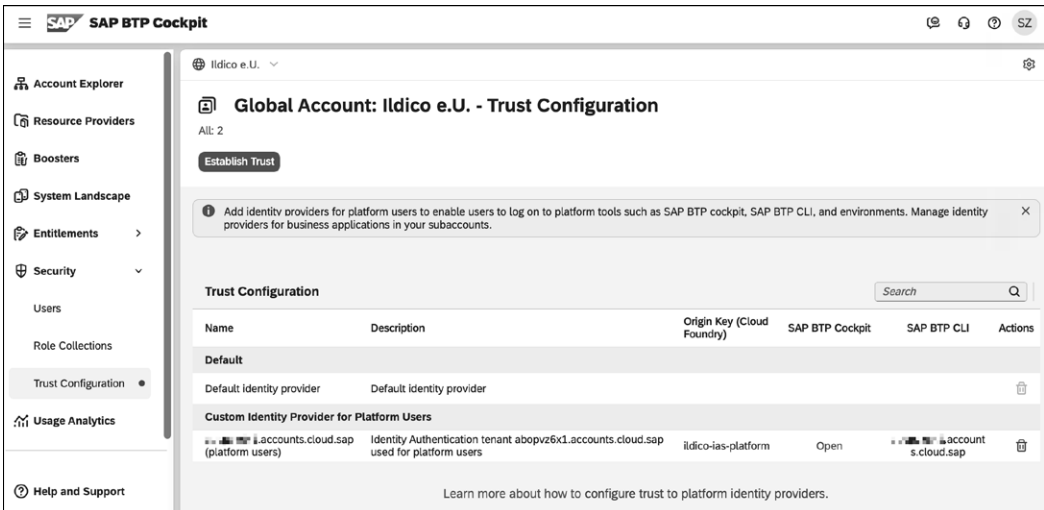


Figure 4.35 Trust Configuration with Platform Identity Provider Setup

In this practical example, we configured the platform identity provider based on identity authentication. You can now use and authorize users in your global account based on this configuration.

## 4.3 Directories

Directories help you to better structure your accounts in your account explorer. You are completely free to determine the division of the directories. For example, whether you separate development and quality assurance from production tenants in one directory or whether you group them by projects, is your individual decision.

SAP distinguishes between two different types of directories, as follows:

### ■ Simple directories

Simple directories are used for structuring purposes only. You can create simple tree structures with them. This is also explained in Chapter 5, Section 5.1. Simple directories are recommended, for example, if you want to subdivide similar subaccounts and need to centrally manage a set of up to 20 subaccounts.

### ■ Managed directories

For larger cloud scenarios, administration is required. Cloud data centers need to be managed from a regional and application perspective, but also from a system resource perspective for specific groups of subaccounts. In addition, there may be a need to grant individual users access to specific directory levels. At this point, it is time to look into managed directories.

You can find the directories in the SAP BTP cockpit of your global account, in the account explorer. In Figure 4.36, we have created three test directories for testing purposes. **Sample Directory** is a normal directory without any further properties; the other two are managed, one with user management and one with resource management. Only the managed and unmanaged directories differ visually.

The screenshot shows the SAP BTP Cockpit interface. The left sidebar contains navigation links: Account Explorer, Resource Providers, Boosters, System Landscape, Entitlements, Security, and Costs and Usage. The main area is titled 'Global Account: Ildico e.U. – Account Explorer'. Below the title, it says 'Alt: 3 directories, 4 subaccounts | Subdomain: ildicoeu'. There are search and filter options. The main content is a table of 'Directories and Subaccounts'.

Name	Type	Environment	Provider	Region	Changed On	
▼ Ildico e.U.	Global Account				20 Feb 2025, 01:12:04 ...	...
□ Sample directory	Directory				24 May 2025, 23:35:45 ...	...
□ Sample directory 2	Directory (Managed)				1 Jun 2025, 10:03:15 (...)	...
□ Sample directory 3	Directory (Managed)				1 Jun 2025, 10:03:30 (...)	...
🔗 Ildico Development	Subaccount	Multi-Environment	Microsoft Azure	Europe (Netherlands)	1 Jun 2025, 10:02:37 (...)	...
🔗 Ildico e.U.-Dev_9cl2zj5qbsytl9	Subaccount	Multi-Environment	Amazon Web Services (AWS)	Europe (Frankfurt)	14 Feb 2024, 19:23:29 ...	...
🔗 Ildico IDS Subaccount	Subaccount	Multi-Environment	Amazon Web Services (AWS)	Europe (Frankfurt)	24 May 2025, 22:14:30 ...	...
🔗 Ildico Productive	Subaccount	Multi-Environment	Microsoft Azure	Europe (Netherlands)	24 May 2025, 23:30:47 ...	...

Figure 4.36 Example Directories in Account Explorer



### Splitting Directories

Note that there can only be one managed directory in a directory hierarchy. Things like inherited permissions that overlap and the like currently are not possible.

To create a directory, select **Create • Directory** to reach the creation screen shown in Figure 4.37.

Click **Advanced** to display the additional options at the bottom of the screen. You can enter a name under **Display Name** and a root node under **Parent**. If you click the icon beside the directory name, a selection dialog for the object's root node opens.

**Create Directory**

Display Name\*  Description

Parent\*

**Advanced**

☒ Enable entitlement management ☒ Enable user management

Labels

Figure 4.37 Directory Creation Screen

If you do not specify anything else, you will create a default directory node. With the **Enable Entitlement Management** and/or **Enable User Management** checkbox, you can make the new directory a managed directory. Click **Create** to create the directory. Figure 4.38 shows the created directory.

**Global Account: Ildico e.U. – Account Explorer**

All: 4 directories, 4 subaccounts | Subdomain: Ildicoeu

Search  Regions:  ☐ Hide entities you don't have access to

Name	Type	Environment	Provider	Region	Changed On
Sample Directory 4	Directory (Managed)				1 Jun 2025, 10:15:00 (...)
Sample directory 2	Directory (Managed)				1 Jun 2025, 10:03:15 (...)
Sample directory 3	Directory (Managed)				1 Jun 2025, 10:03:30 (...)
Ildico Development	Subaccount	Multi-Environment	Microsoft Azure	Europe (Netherlands)	1 Jun 2025, 10:02:37 (...)
Ildico e.U.-Dev_9d12zf5qbsrty9	Subaccount	Multi-Environment	Amazon Web Services (AWS)	Europe (Frankfurt)	14 Feb 2024, 19:23:29 (...)
Ildico IDS Subaccount	Subaccount	Multi-Environment	Amazon Web Services (AWS)	Europe (Frankfurt)	24 May 2025, 22:14:30 (...)
Ildico Productive	Subaccount	Multi-Environment	Microsoft Azure	Europe (Netherlands)	24 May 2025, 23:30:47 (...)

Figure 4.38 Subaccounts in Account Explorer with Updated Directory Structure

Now you can move the subaccounts into the directories by simply clicking and dragging the subaccount row, then releasing the mouse button. You can see an example result in Figure 4.39.

If you now click a directory, you will see its details. If it is a managed directory, as shown in Figure 4.40, you will see the **Users** and **Entitlements** navigation nodes in the left pane.

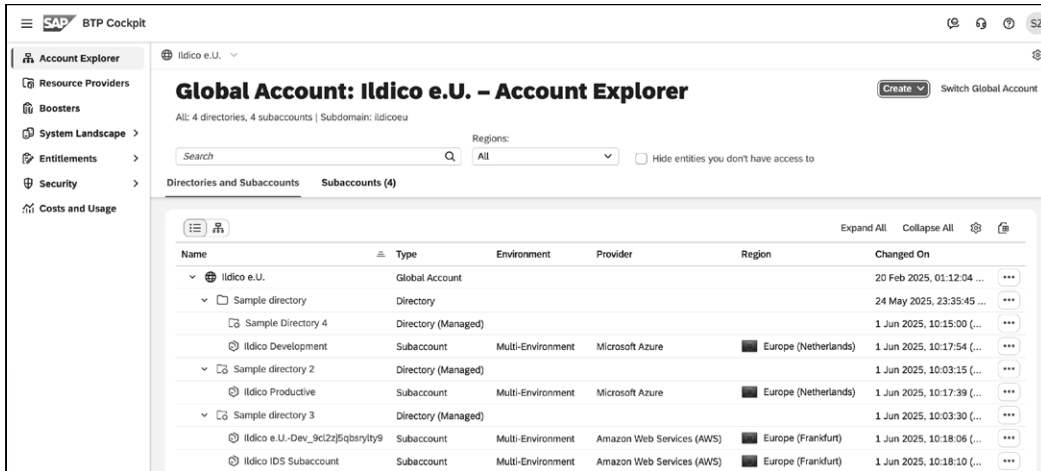


Figure 4.39 Subaccounts in Directories

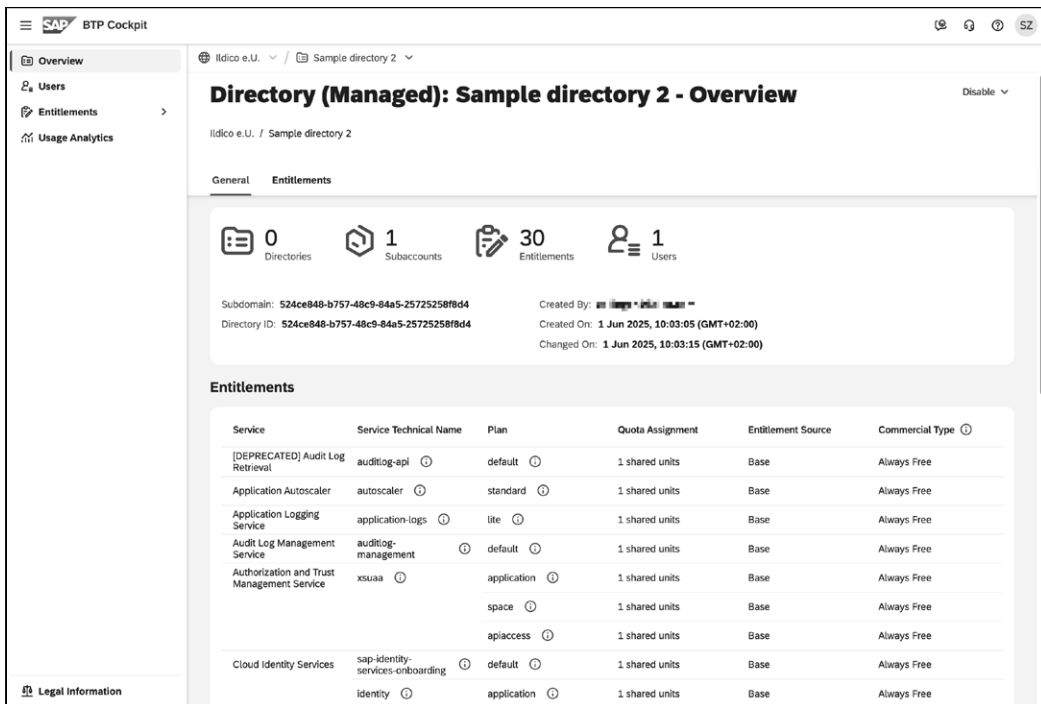


Figure 4.40 Detailed View of Directory

The example Sample Directory 2 was configured for entitlement management only. Figure 4.41 shows what happens when you navigate to an inactive item such as this. By clicking **Enable User Management**, you can easily configure user management for the directory.

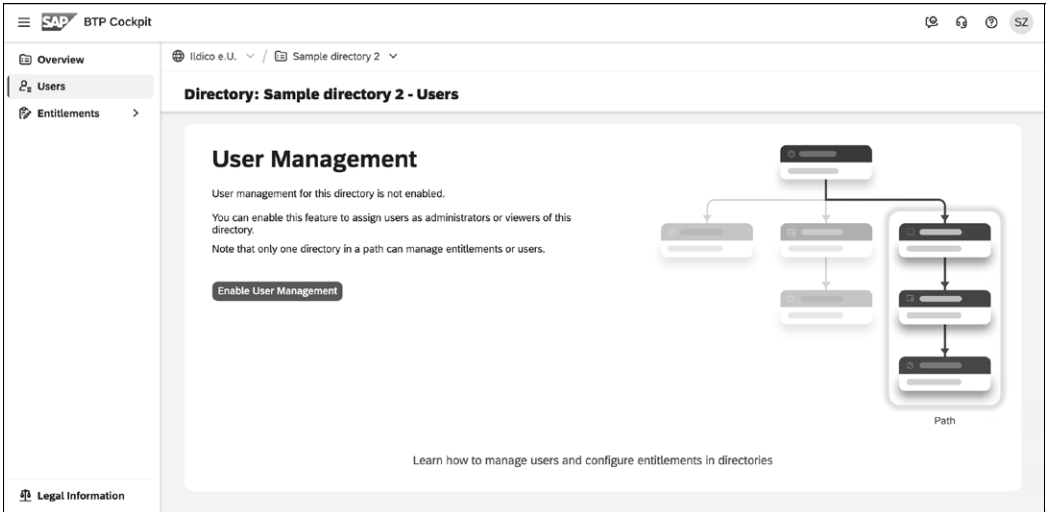


Figure 4.41 Access to User Management in Directory


In user management, users can be created with **Create User** in the same way as in the global account. These users are then specifically authorized for a directory. Figure 4.42 shows an example of a user creation screen.

The 'Create User' form has the following fields and values:

- User Name:** \* sample\_directory\_user@ildico.com
- Identity Provider:** \* Default identity provider (dropdown menu)
- E-Mail:** \* sample\_directory\_user@ildico.com

At the bottom right, there are two buttons: 'Create' and 'Cancel'.

Figure 4.42 Creating Directory User

For the user to receive permissions, a few steps are necessary. First, navigate from the user overview via the  icon to the user details (Figure 4.43). At the bottom right, you will find the assigned **Role Collections**.

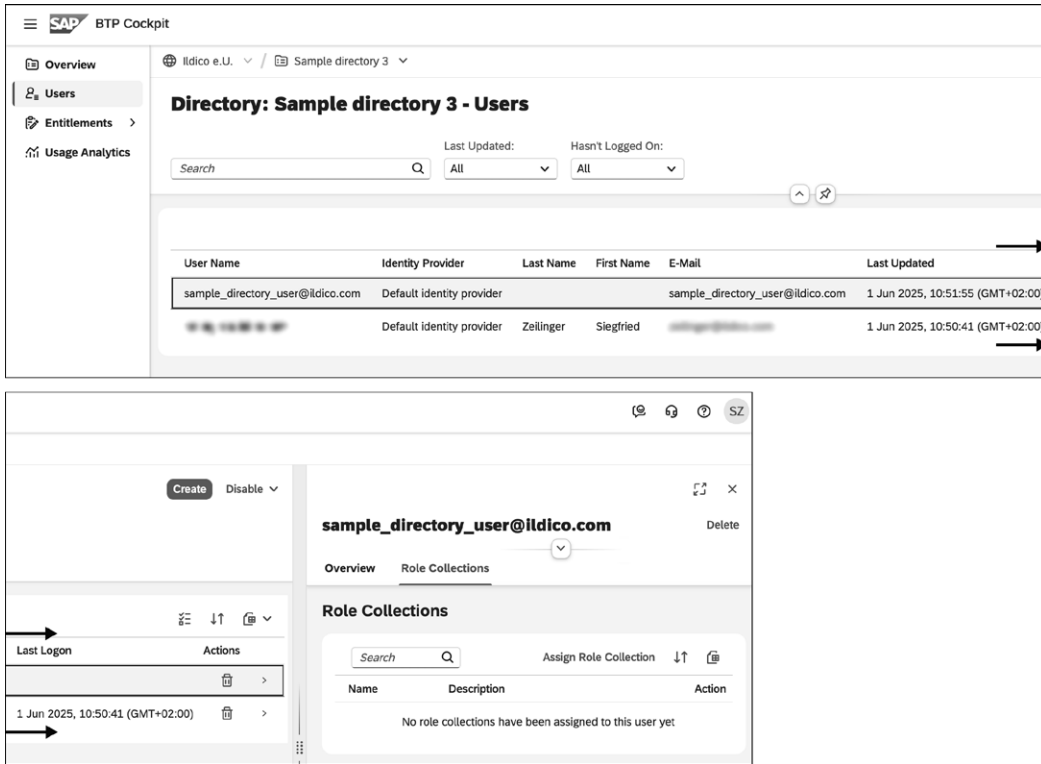


Figure 4.43 User Detail View At Directory

Click the **Assign Role Collection** link and choose whether the selected person may administrate (**Directory Administrator**) or only view (**Directory Viewer**) the directory, as shown in Figure 4.44.

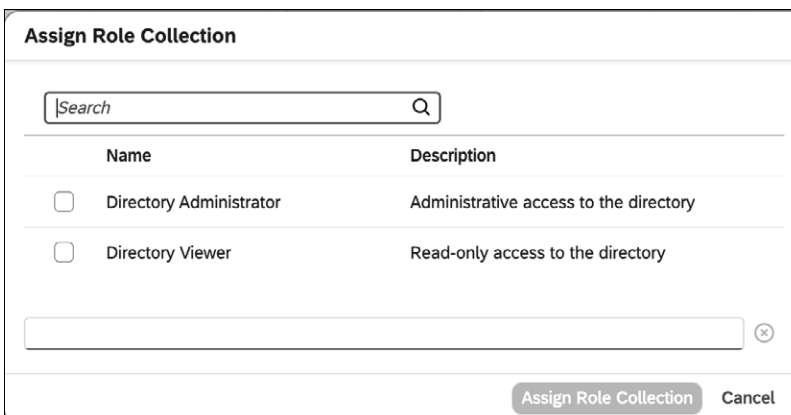


Figure 4.44 Directory Role Assignments



The entitlements, which we will discuss in the Section 4.7, can also be analyzed at the directory level in the corresponding menu item. This can be used to determine which assignments exist at the directory level. You will also find these mappings in the global account, but they are not broken down. Figure 4.45 shows the filtered selection of subaccounts in the directory.

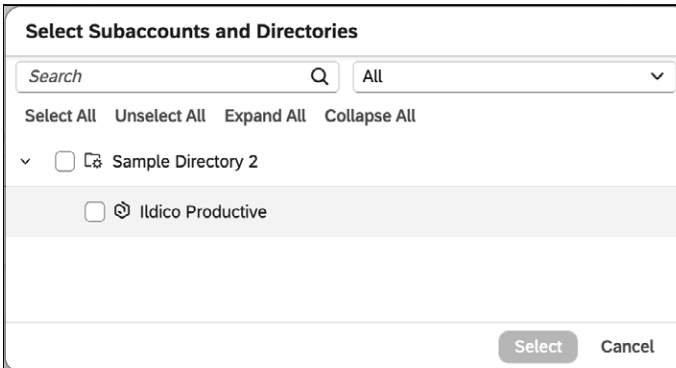


Figure 4.45 Selection in Subaccount Field

The **Service Assignments** in the directories are also filtered and prepared according to the assigned subaccounts (see Figure 4.46).

Service	Service Technical Name	Plan	Assigned To	Quota Assignment	Global Quota	Licensed Quantity	Entitlement Source	Commercial Type
[DEPRECATED] Audit Log Retrieval	auditlog-api	default	1 entity	Assigned	1	1	Base	Always Free
Application Autoscaler	autoscaler	standard	1 entity	Assigned	1	1	Base	Always Free
Application Logging Service	application-logs	lite	1 entity	Assigned	1	1	Base	Always Free
Audit Log Management Service	auditlog-management	default	1 entity	Assigned	1	1	Base	Always Free
Authorization and Trust Management Service	xsuaa	application	1 entity	Assigned	1	1	Base	Always Free
		space	1 entity	Assigned	1	1	Base	Always Free
		apiaccess	1 entity	Assigned	1	1	Base	Always Free
Cloud Identity Services	identity	application	1 entity	Assigned	1	1	Base	Always Free
	sap-identity-services-onboarding	default (Application)	1 entity	Assigned	1	1	Base	Always Free

Figure 4.46 Service Assignments in Directory

Another tool to help with the administration of directories is **Usage Analytics**, which we will discuss in Section 4.8 and which you can see a preview of in Figure 4.47.

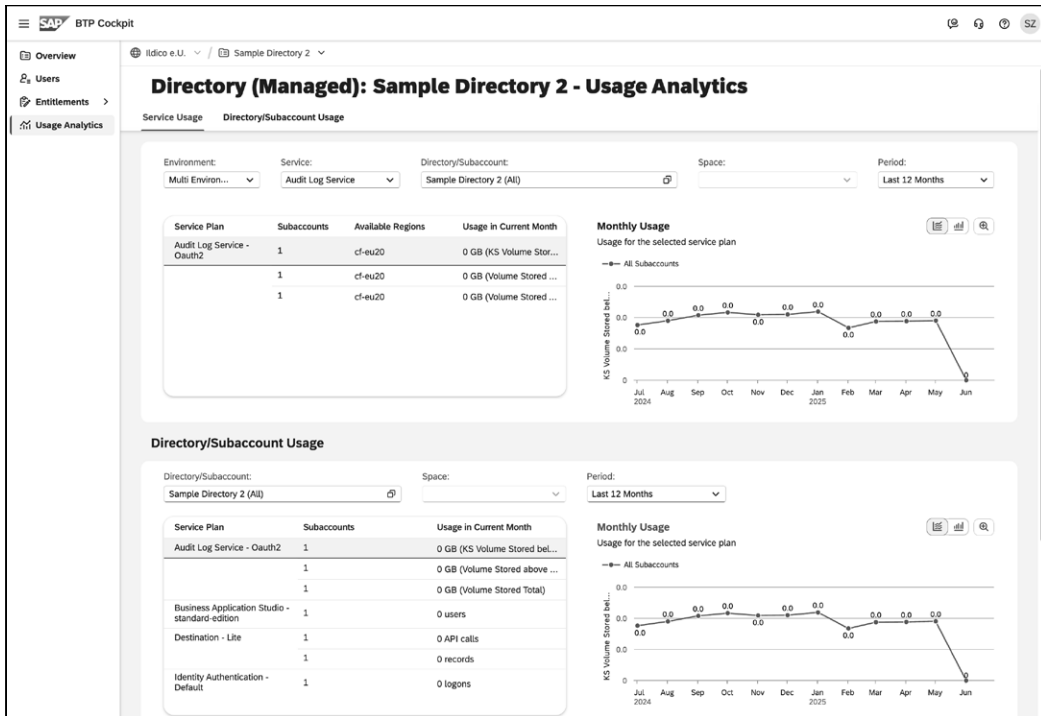


Figure 4.47 Usage Analytics for Directory

In summary, directories are very useful for organizing complex subaccount landscapes, and we recommend using them at least for organizing productive and nonproductive subaccounts.

## 4.4 Boosters

SAP uses ready-made configuration templates for the administration of its solutions in many areas. Especially in complex system landscapes and with new products, as well as with longer sequences of configuration settings, this is the preferred option.

SAP has also created such configuration templates in SAP BTP with boosters. *Boosters* automate many of the steps required to make certain functions or solutions quickly available, such as integrating data, setting up authentication mechanisms, or configuring connectivity services.

Boosters are offered in SAP BTP in your global account in the navigation under **Boosters**. They are subdivided into a filterable overview of tiles (see Figure 4.48), and detailed representations (see Figure 4.49). All configurations can be performed using a wizard-based interface, which reduces the complexity of administration.

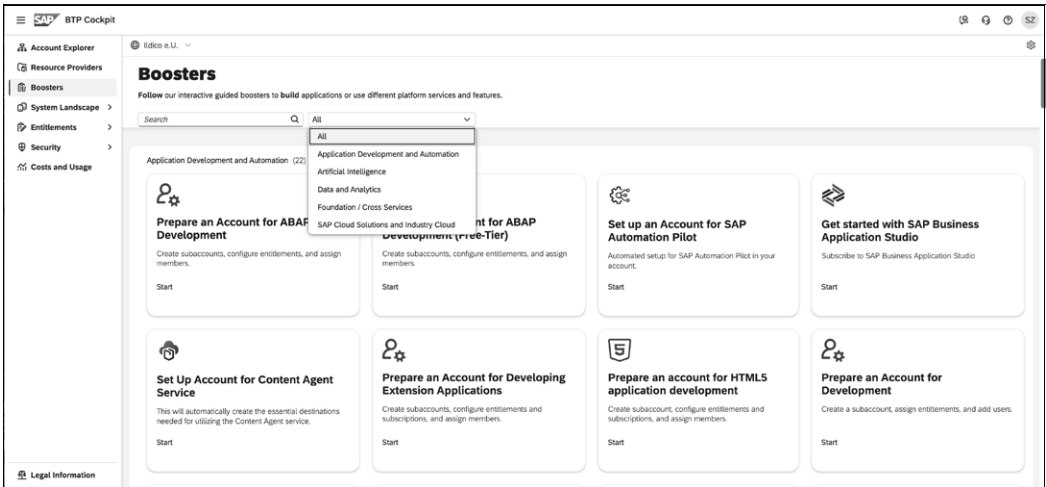


Figure 4.48 Filterable Entry to Boosters

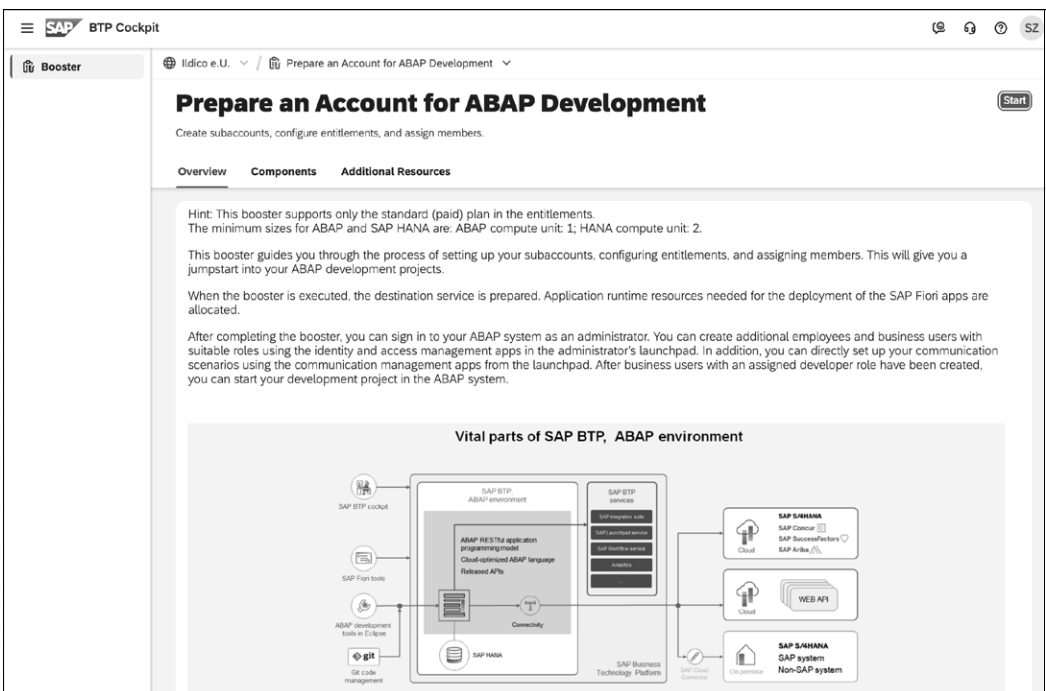


Figure 4.49 Details of Sample Booster

The following example walks through the steps to set up a (free) booster in SAP BTP. Start the booster via the **Start** button (as shown in Figure 4.49). The remaining steps, each completed by clicking **Next**, are as follows:

### 1. Checking the prerequisites (see Figure 4.50)

The system will check if you have the necessary permissions and privileges.

The screenshot shows the 'Set up account for SAP Build Process Automation (Free)' wizard. The progress bar at the top indicates five steps: 1. Check Prerequisites (active), 2. Select Scenario, 3. Configure Subaccount, 4. Add Users, and 5. Review. Below the progress bar, a message states 'All required prerequisites are met. Rerun' with a close button. The main section is titled 'Check Prerequisites' and contains the text 'We're checking if you meet all the prerequisites required for this booster.' followed by two status indicators: 'Checking Authorizations: DONE' and 'Checking Entitlements: DONE'. At the bottom right, there are 'Next' and 'Cancel' buttons.

Figure 4.50 Step 1: Checking Prerequisites

### 2. Scenario selection (see Figure 4.51)

In this step, you can choose whether to use an existing subaccount or create a new one.

The screenshot shows the 'Set up account for SAP Build Process Automation (Free)' wizard. The progress bar at the top indicates five steps: 1. Check Prerequisites, 2. Select Scenario (active), 3. Configure Subaccount, 4. Add Users, and 5. Review. Below the progress bar, the main section is titled 'Select Scenario' and contains the text 'Select subaccount mode for the booster.' followed by two radio button options: 'Create Subaccount' (selected) and 'Select Subaccount'. Each option has a descriptive text below it. At the bottom right, there are 'Previous', 'Next', and 'Cancel' buttons.

Figure 4.51 Step 2: Selecting Scenario

### 3. Subaccount settings (see Figure 4.52)

This is where you specify how the subaccount will be included in your global account.

**Set up account for SAP Build Process Automation (Free)**

1 Check Prerequisites — 2 Select Scenario — **3 Configure Subaccount** — 4 Add Users — 5 Review

### Configure Subaccount

Configure your Cloud Foundry Subaccount and Space. ⓘ

Entitlements: Reset

Service	Plan	Required Quota	Remaining Quota
SAP Build Process Automation *	free	— 1 +	1
	standard	1	unlimited

The service plans that are required for running this project and their required quota. The required quota is deducted from the available quota for each service in your global account.

Subaccount Name: \*

The name for your new subaccount can contain up to 255 characters.

Provider: \*

Select the infrastructure provider of the new subaccount.

Region: \*

Select the region in which to create the new subaccount.

Subdomain: \*

The subdomain of your subaccount must be unique and can contain up to 63 letters (a-z or A-Z), digits (0-9), and hyphens (not at the start or end).

Org Name: \*

The name for the Cloud Foundry org can contain up to 255 characters.

Space Name: \*

The name for the Cloud Foundry space can contain up to 255 characters.

Previous Next Cancel

**Figure 4.52** Step 3: Subaccount Settings

#### 4. Identity provider and user (see Figure 4.53)

In the last step, you specify the identity provider and can also specify authorized users.

#### 5. Summary (see Figure 4.54)

On the last screen, the summary, you can check all your settings and start the booster by clicking **Finish**.

**Set up account for SAP Build Process Automation (Free)**

1 Check Prerequisites — 2 Select Scenario — 3 Configure Subaccount — **4 Add Users** — 5 Review

## Add Users

Enter the details of additional users who will work on your development project and assign them to the relevant roles. ⓘ

**ⓘ** The **Platform Identity Provider** displays all the **Custom Identity Authentication Service (IAS) tenants** configured in your global account. The booster will use it to assign cockpit platform roles like "Subaccount Administrator". Similarly, the **Application Identity Provider** displays all the Custom IAS tenants associated with the selected subaccount. This IAS tenant will be used by application users having application roles like "BuildAppsDeveloper".

Custom Identity Provider for Platform Users:

Custom Identity Provider for Applications:

Administrators:

Administrators will be assigned to the org manager, space manager roles and Subaccount Administrator role collection(s). The logged in user '...' will be added by default as an Administrator.

Developers:

Developers will be assigned to the space developer role and ProcessAutomationDeveloper, ProcessAutomationAdmin, ProcessAutomationParticipant, Subaccount Viewer role collection(s). The logged in user '...' will be added by default as a Developer.

Previous Next Cancel

Figure 4.53 Step 4: Identity Provider and User

**Set up account for SAP Build Process Automation (Free)**

1 Check Prerequisites — 2 Select Scenario — 3 Configure Subaccount — **4 Add Users** — 5 Review

## Select Scenario

Subaccount Mode: Create Subaccount

## Configure Subaccount

Subaccount: Ildico e.U.-Dev\_ds534r3y92j0kmbm  
 Provider: Amazon Web Services (AWS)  
 Region: US East (VA)  
 Subdomain: ds534r3y92j0kmbm  
 Org: Ildico\_e.U.\_ds534r3y92j0kmbm  
 Space: dev

## Add Users

Cloud Foundry Origin: sap.ids  
 XSUAA Origin: sap.default  
 Application Origin: sap.custom  
 Application IdP Host URL: accounts.ondemand.com  
 Administrators: ...  
 Developers: ...

Previous **Finish** Cancel

Figure 4.54 Step 5: Summary

Now you will see a progress screen, and when it completes, everything will be prepared for you (see Figure 4.55).

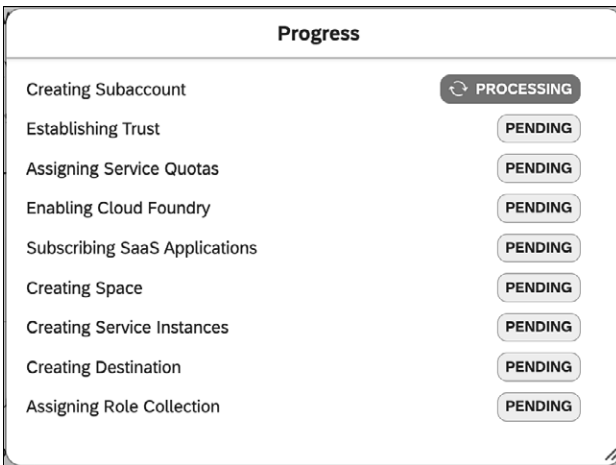


Figure 4.55 Wizard Execution: Progress Bar

The final **Success** screen (see Figure 4.56) allows you to navigate directly to the new subaccount using the **Navigate to Subaccount** link.

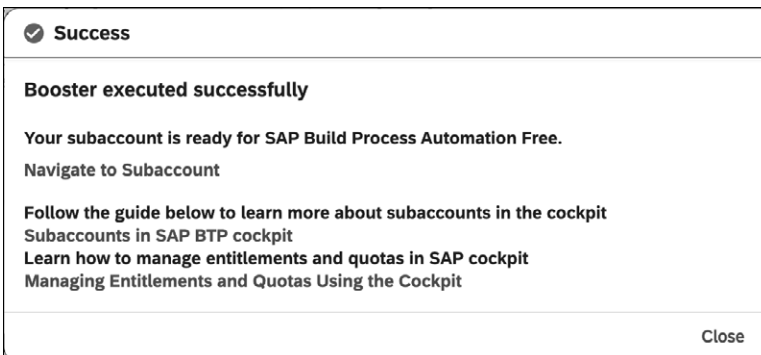


Figure 4.56 Success Message After Booster Execution

If you go to the subaccount and then navigate to **Services • Instances and Subscriptions**, you will see that the Cloud Foundry runtime, the corresponding service instance, and the corresponding application have been added and set up in this process (see Figure 4.57).

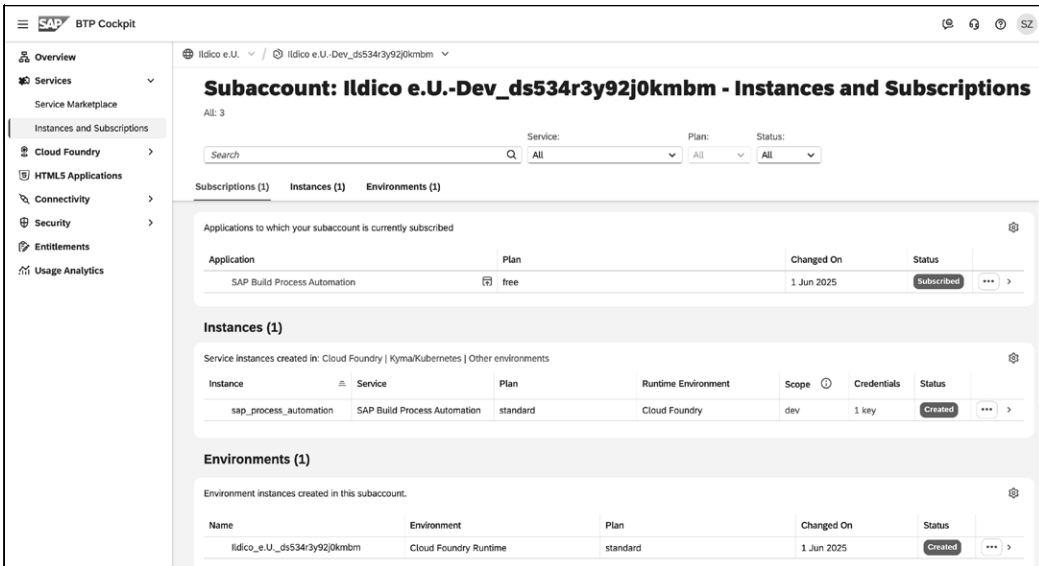


Figure 4.57 SAP BTP Cockpit of Created Subaccount

The benefits of an SAP BTP booster are, in a nutshell, as follows:

- **Simplification**  
Boosters reduce the complexity of setting up services and applications by providing a step-by-step process and preconfigured settings.
- **Time savings**  
By automating setup and configuration, organizations can start development and get to market faster.
- **Error reduction**  
Standardization and automation help minimize human error in service configuration.
- **Learning support**  
For new users of SAP BTP, boosters offer a learning tool to better understand the platform and its capabilities.

Boosters cover a wide range of use cases, including the integration of SAP and non-SAP applications, the development of new applications, the implementation of security and authentication mechanisms, and much more.

## 4.5 System Landscape

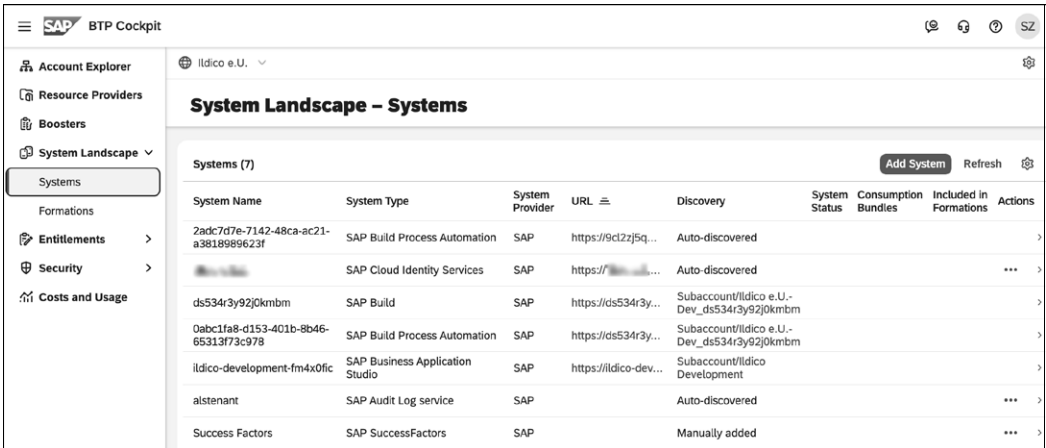
If you want to connect an SAP cloud solution such as SAP SuccessFactors or SAP Marketing Cloud to your global account, you can do so using an integration token. The



integration takes place in the SAP BTP cockpit of your global account under the **System Landscape** menu item. The following SAP solutions can be connected:

- SAP S/4HANA Cloud
- SAP Marketing Cloud
- SAP SuccessFactors
- SAP Commerce Cloud
- SAP Cloud for Customer
- SAP Field Service Management

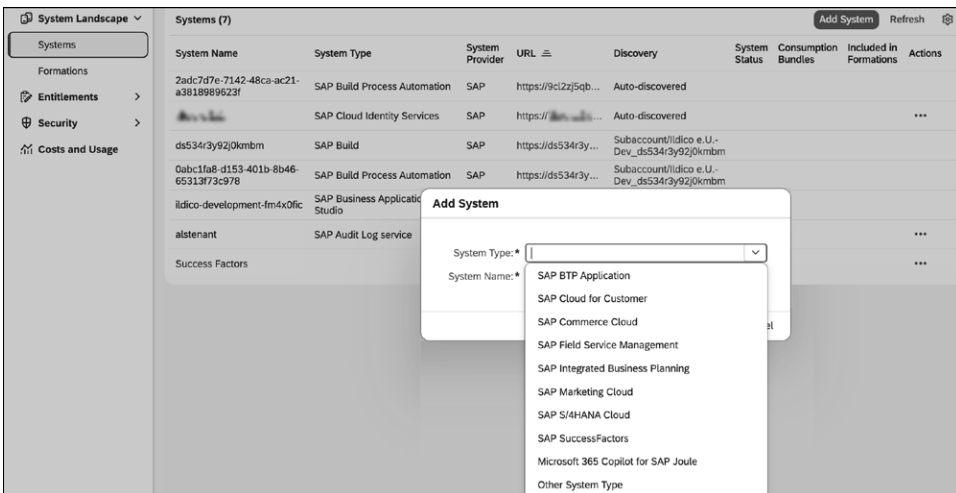
The basic procedure is as follows: First, under **System Landscape • Systems**, click **Add System** (see Figure 4.58).



System Name	System Type	System Provider	URL	Discovery	System Status	Consumption Bundles	Included in Formations	Actions
2adc7d7e-7142-48ca-ac21-a3818989623f	SAP Build Process Automation	SAP	https://9cl2zj5q...	Auto-discovered				
...	SAP Cloud Identity Services	SAP	https://...	Auto-discovered				...
ds534r3y92j0kmbm	SAP Build	SAP	https://ds534r3y...	Subaccount/ildico e.U.-Dev_ds534r3y92j0kmbm				
0abc1fa8-d153-401b-8b46-65313f73c978	SAP Build Process Automation	SAP	https://ds534r3y...	Subaccount/ildico e.U.-Dev_ds534r3y92j0kmbm				
ildico-development-fm4x0fic	SAP Business Application Studio	SAP	https://ildico-dev...	Subaccount/ildico Development				
alstenant	SAP Audit Log service	SAP		Auto-discovered				...
Success Factors	SAP SuccessFactors	SAP		Manually added				...

Figure 4.58 Accessing System Landscape

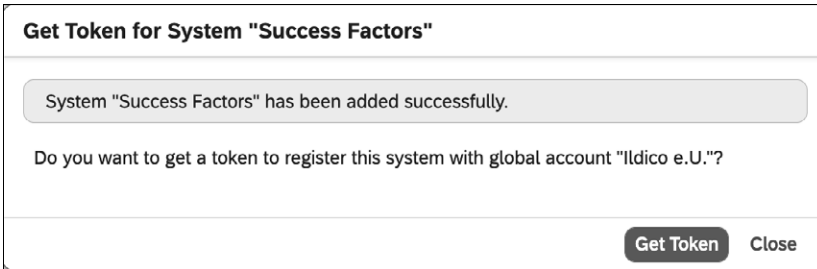
In the next step, select the **System Type** and enter a **System Name** (see Figure 4.59). In this example, we have chosen **SAP SuccessFactors**.



System Name	System Type	System Provider	URL	Discovery	System Status	Consumption Bundles	Included in Formations	Actions
2adc7d7e-7142-48ca-ac21-a3818989623f	SAP Build Process Automation	SAP	https://9cl2zj5q...	Auto-discovered				
...	SAP Cloud Identity Services	SAP	https://...	Auto-discovered				...
ds534r3y92j0kmbm	SAP Build	SAP	https://ds534r3y...	Subaccount/ildico e.U.-Dev_ds534r3y92j0kmbm				
0abc1fa8-d153-401b-8b46-65313f73c978	SAP Build Process Automation	SAP	https://ds534r3y...	Subaccount/ildico e.U.-Dev_ds534r3y92j0kmbm				
ildico-development-fm4x0fic	SAP Business Application Studio	SAP	https://ildico-dev...	Subaccount/ildico Development				
alstenant	SAP Audit Log service	SAP		Auto-discovered				...
Success Factors	SAP SuccessFactors	SAP		Manually added				...

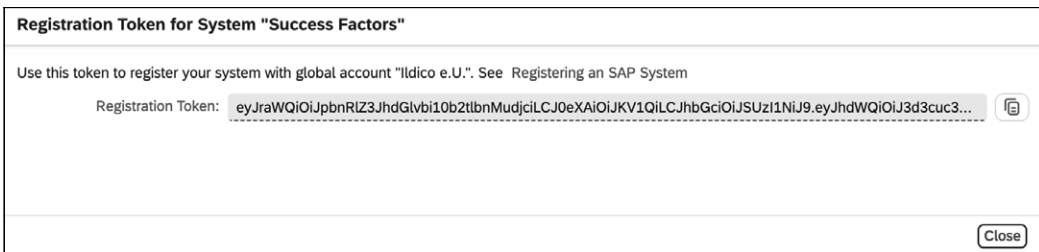
Figure 4.59 Selecting System Type

Now you can directly create the token for the authentication in the target system (see Figure 4.60) by clicking **Get Token**.



**Figure 4.60** Get Token

You can then copy the token as shown in Figure 4.61 and add it to your cloud product according to the installation guide. In the system overview, you can see that the trust setting has been confirmed on the other side.



**Figure 4.61** Receiving SAP BTP Token for Target System

These scenarios are especially important if, for example, you want to rely on custom developments and extensions for your SAP SuccessFactors installation.

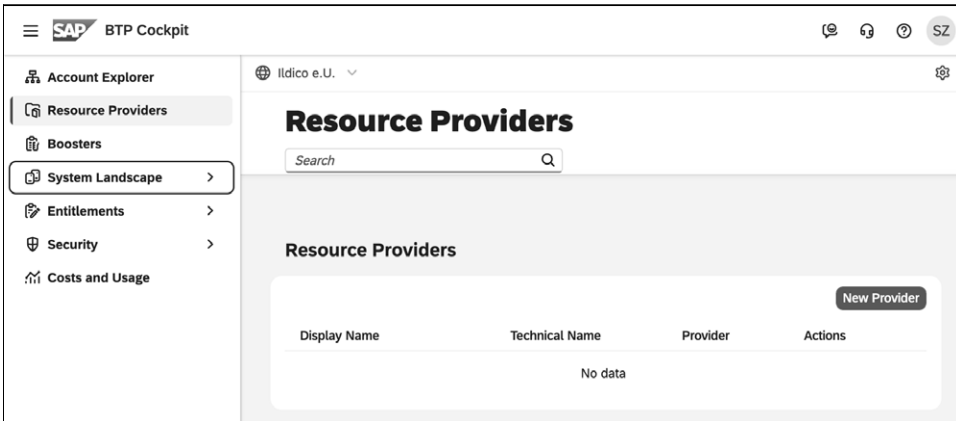
## 4.6 Resource Provider

If you have already subscribed to resources from one of the cloud providers supported by SAP, you can integrate these resources into SAP BTP. Examples might include databases that are located at a cloud provider and should be accessed by your applications. Currently, only two use cases are supported, as shown in Table 4.1.

Cloud Vendor	Supported Services
Amazon Web Services	Amazon Relational Database Service (RDS) — PostgreSQL
Microsoft Azure	Azure Database for PostgreSQL

**Table 4.1** Services Supported by Cloud Providers

To create a resource provider, navigate to **Resource Providers** in your global account in the SAP BTP cockpit (see Figure 4.62). Now use the **New Provider** button to access the creation dialog.



**Figure 4.62** Overview of Resource Providers in Global Account

The resources received from the providers are now entered in the configuration dialog (see Figure 4.63).

**Figure 4.63** Resource Provider Registration Dialog

## 4.7 Entitlements

Entitlements can be thought of as *rights*; they determine the allocation of resources and services made available to an organization or user. These entitlements define which specific services and resource quantities a customer has access to based on his subscription or license. You must distribute your company's entitlements among your subaccounts.

There are two aspects of entitlements in SAP BTP in the global account:

### ■ Entity allocations

These are the resources included in your licenses and plans and their limits. Many services are shared entities and can be used multiple times. Otherwise, you can set a quota limit on a global level—for example, to specify that a service may only exist three times in all subaccounts.

### ■ Service allocation

This determines which services are assigned and active in which subaccounts.

The management of entitlements is an essential part of administration as it allows you to use and control cloud resources efficiently and can save you a lot of money. You can manage your entitlements via the SAP BTP cockpit under the **Entitlements** menu option. There, you can view your current allocations, make adjustments, and monitor the usage of your subscribed services.



### Configuring Entitlements in Practice

In practice, you start the distribution of permissions in the global account. Using the optional directories, you then distribute the permissions first to subaccounts, and then to spaces.

Figure 4.64 shows the allocations of an example global account. With **Edit**, you can change the quotas. Note that in our test tenant, all units are *shared units*, which is why they are difficult to see in the example.

Figure 4.65 shows an example of the assignment of the SAP Business Application Studio service in our example tenant.



### Common Issues Related to Entitlements

People often forget to assign entitlements to subaccounts, but this is relatively easy to fix. If you are using a usage-based model, be sure to check your license terms and conditions; you will quickly incur costs if you increase your allocations. That leads into the next topic, usage monitoring, which will help you keep your costs under control.

Service	Service Technical Name	Plan	Set Quota Limit	Quota Assignment	Remaining Quota	Actions
[DEPRECATED] Audit Log Retrieval	auditlog-api	default		Assigned (1 unit)		
Application Autoscaler	autoscaler	standard		Assigned (1 unit)		
Application Logging Service	application-logs	lite		Assigned (1 unit)		
Audit Log Management Service	auditlog-management	default		Assigned (1 unit)		
Audit Log Viewer Service	auditlog-viewer	free (Application)		Assigned (1 unit)		
Authorization and Trust Management Service	xsuaa	application		Assigned (1 unit)		
		space		Assigned (1 unit)		
		apiaccess		Assigned (1 unit)		
Cloud Identity Services	identity	application		Assigned (1 unit)		
	sap-identity-services-onboarding	default (Application)		Assigned (1 unit)		
Cloud Integration Automation	cias	oauth2		Assigned (1 unit)		

Figure 4.64 Entity Assignments

Name	Type	Plan	Quota Assignment
Ildico Development	Subaccount	standard-edition	Assigned (unlimited units)
Sample Directory 2	Directory	standard-edition	Assigned (unlimited units)

Figure 4.65 Service Assignments

## 4.8 Usage Monitoring

With the **Costs and Usage** menu of the SAP BTP cockpit, you can monitor cloud resources and services and also get an overview of the (forecasted) running costs. If you navigate to the **Costs and Usage** menu in the SAP BTP cockpit, you will find different sources of information.

First, on the top level under **Global Account Info** (see Figure 4.66), you can see facts about your global account such as the **Account ID**, along with a high-level summary of monthly costs, the selected time range, and your contract information. This area provides a clear summary of current and projected costs.

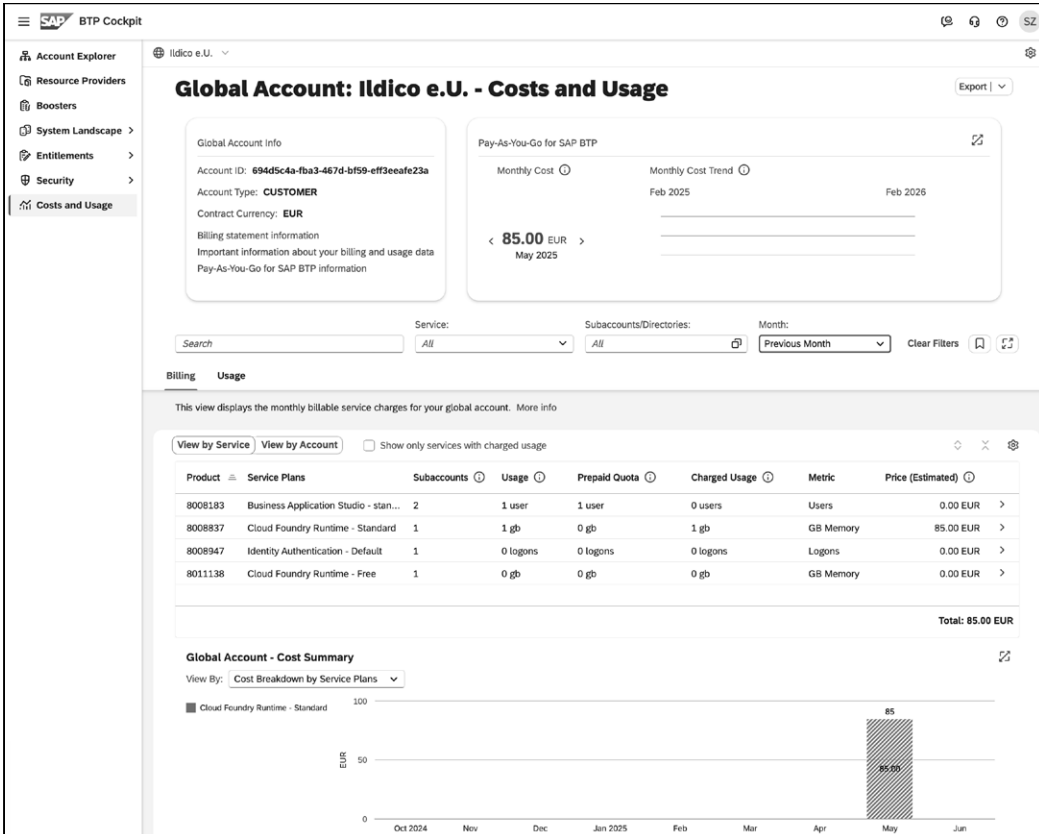


Figure 4.66 Usage Analysis: Global Account Info

Below, when you filter by **Service**, you will see a table under the main **Usage** section that shows resource usage grouped by service plan. This table includes information like **Service Plan**, **Usage**, and **Metric**. This helps identify which services and plans are consuming the most resources (see Figure 4.67).

If you drill down into a particular service plan from the usage table, you'll see detailed consumption data by subaccount or directory for that service. This provides insights into how the service is being used across different parts of your organization (see Figure 4.68).

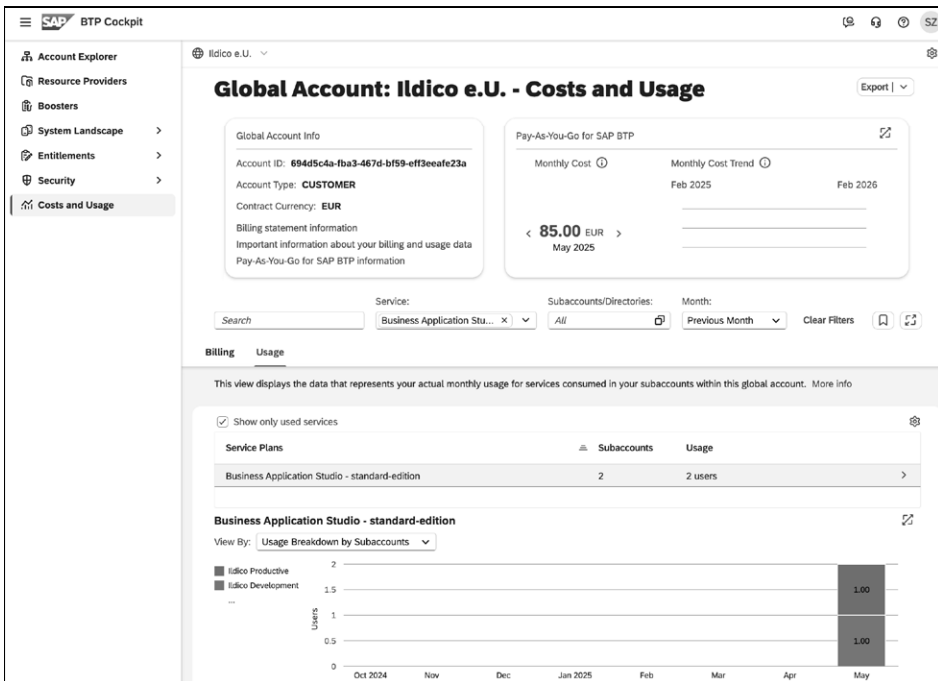


Figure 4.67 Usage Analysis: Service Plans

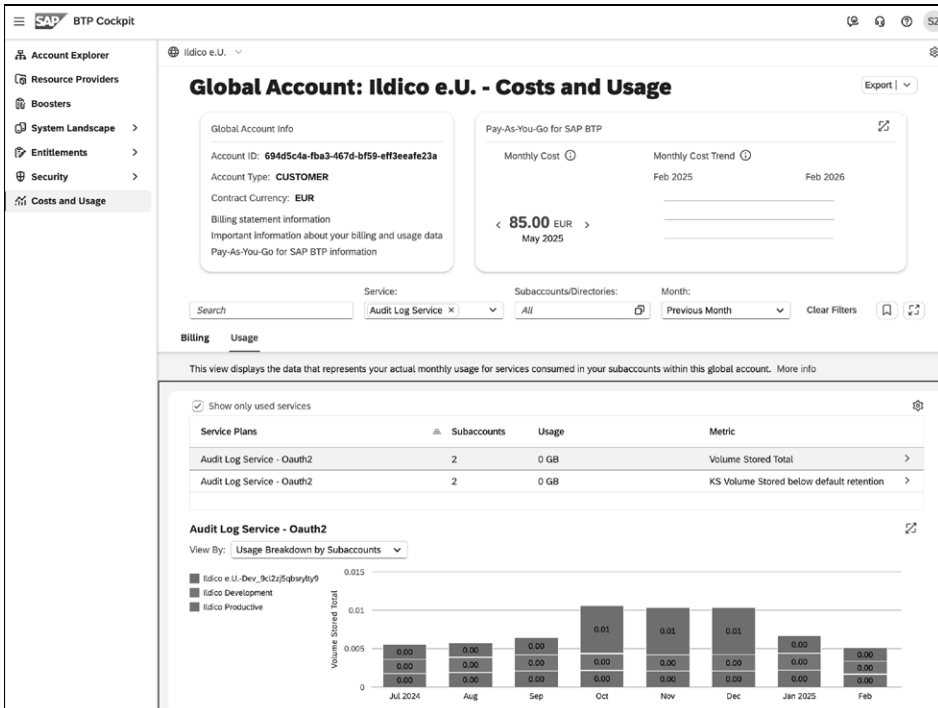


Figure 4.68 Usage Analysis: Service Usage

Finally, when you select the **Billing** tab (see Figure 4.69), you will see a subaccount-based breakdown of SAP BTP costs, followed by a timeline diagram.

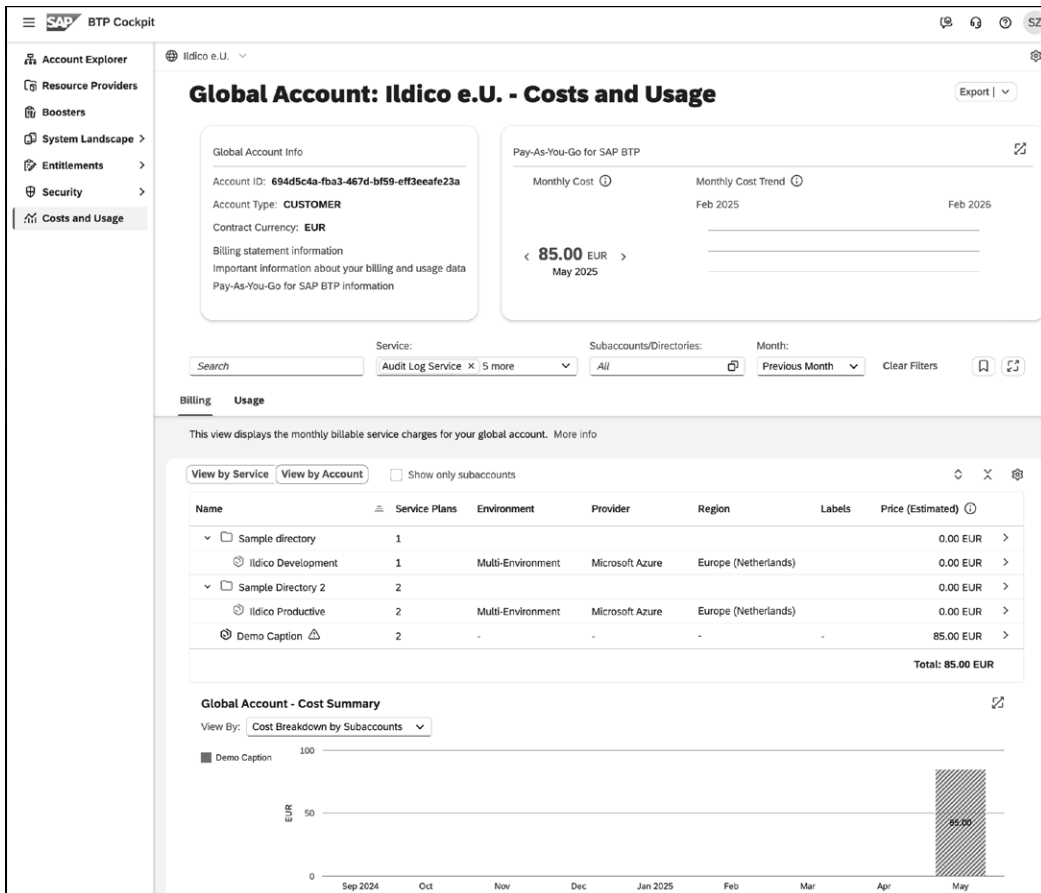


Figure 4.69 Subaccount and Directory Usage

We recommend that you regularly monitor the costs and usage of your cloud services—not least for cost and management reasons as resources can be saved in virtually inactive subaccounts, and these can be added back on demand.

## 4.9 Summary

Global account administration is the foundation of managing cloud resources within SAP BTP. Every organization receives a global account from SAP, which serves as the central control hub for licenses, subaccounts, user access, and platform-wide configuration. Access to the global account is managed via the SAP BTP cockpit. Users typically authenticate using SAP ID, but Identity Authentication can be integrated for advanced scenarios, such as connecting to corporate identity stores and enabling multifactor



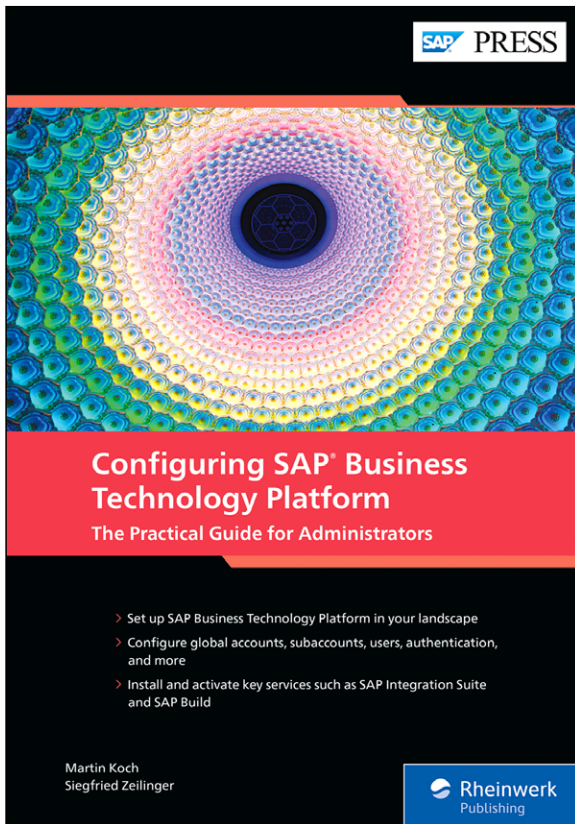
authentication. Managing users, assigning role collections, and controlling access is crucial for maintaining secure administration.

Role collections in the global account—such as administrator, viewer, or directory admin—determine user capabilities. These can be customized to suit organizational needs. Directories help in structuring and organizing subaccounts logically, either for purely visual grouping or for managed control of entitlements and user permissions across large landscapes.

Boosters are SAP's wizard-based tools to quickly configure and deploy common SAP BTP scenarios, automating many setup tasks and reducing errors.

The system landscape feature allows integration of other SAP cloud solutions (e.g., SAP SuccessFactors or SAP Marketing Cloud) by using authentication tokens, thus simplifying centralized administration. SAP BTP also supports integrating cloud infrastructure resources via resource providers, expanding flexibility in hybrid deployments.

Entitlements determine which services and resources are allocated to which subaccounts. Managing entitlements effectively is key to optimizing usage, avoiding unnecessary costs, and staying within license limits. Finally, usage monitoring tools offer visibility into service consumption and cost trends, enabling better governance and cost control across the cloud environment.



Martin Koch, Siegfried Zeilinger

# Configuring SAP Business Technology Platform

## The Practical Guide for Administrators

- Set up SAP Business Technology Platform in your landscape
- Configure global accounts, subaccounts, users, authentication, and more
- Install and activate key services such as SAP Integration Suite and SAP Build



[www.sap-press.com/6080](http://www.sap-press.com/6080)

We hope you have enjoyed this reading sample. You may recommend or pass it on to others, but only in its entirety, including all pages. This reading sample and all its parts are protected by copyright law. All usage and exploitation rights are reserved by the author and the publisher.

Martin Koch is the managing director of CloudDNA GmbH, an SAP partner in Austria. Siegfried Zeilinger is a freelancer and the managing director of a small management consultancy.

ISBN 978-1-4932-2707-5 • 450 pages • 09/2025

E-book: \$84.99 • Print book: \$89.95 • Bundle: \$99.99



**Rheinwerk**  
Publishing