**7 Security**

Use the security features and functions of SAP BTP to support the security policies of your organization.

**Security Recommendations**

We provide a list with our recommendations for the configuration of our services. These recommendations help

you to meet your compliance goals and secure your business.

See SAP BTP Security Recommendations.

Our customer success organization uses these recommendations as a base to create a security baseline

template.

For more information, go to https://support.sap.com/sos and choose *Media Library SAP CoE Security*

*Services - Security Baseline Template* .

**User Model**

SAP BTP distinguishes between platform users (account management, custom development, and operations)

and business users (for the applications).

See User and Member Management [page 121].

**Authorizations**

You can configure authorizations using roles and role collections for your global account, subaccount,

directory, or individual applications.

See Security Administration: Managing Authentication and Authorization [page 2278].

**Identity Providers**

All users of SAP BTP are stored in identity providers, either in the default or in a custom identity provider. SAP

BTP needs a copy of the user, sometimes called a shadow user. You assign the shadow user authorizations

to access resources in SAP BTP. When a user authenticates, SAP BTP forwards the request to the identity

provider.

For more information, see Trust and Federation with Identity Providers [page 2280].

**3178** PUBLIC

SAP Business Technology Platform

**Security**

 Note

For the China (Shanghai) region, a different default identity provider is used.

For more information, see this blog article on *SAP Community*.

**Default Identity Provider**

We provide a default identity provider for both platform users and business users (in applications) at SAP BTP.

The default identity provider enables single sign-on to your SAP applications and services.

Use the default identity provider as a preconfigured user store in your starter scenarios or for testing. You can

also use the default identity provider as a backup identity provider if access to your custom identity provider

fails.

See Default Identity Provider [page 2335].

**Identity Authentication Service**

Identity Authentication service provides authentication and single sign-on in the cloud.

We recommend that you configure the Identity Authentication service as the identity provider and connect

Identity Authentication to your own corporate identity provider. Identity Authentication provides features that

the default identity provider doesn't, such as the ability to connect your corporate identity provider or to define

security policies.

See Trust and Federation with Identity Providers [page 2280].

For more information about Identity Authentication, see SAP Cloud Identity Services - Identity Authentication.

**Transport Layer Security (TLS) Connectivity Support**

SAP BTP uses encrypted communication channels based on HTTPS/TLS, supporting TLS version 1.2 or higher.

 Note

TLS versions 1.0 and 1.1 are no longer supported.

Make sure you use HTTP clients (such as web browsers) that support TLS version 1.2 or higher for connecting

to SAP BTP.

 Note

You can optionally use TLS 1.3 in the Custom Domain Manager. This option allows the use of TLS 1.3 with

applications running on SAP BTP. It's not allowed to use TLS 1.3, for example for the SAP BTP cockpit or

SAP Cloud Identity Services. These services are still using TLS 1.2.

SAP Business Technology Platform

**Security** PUBLIC **3179**

See What Is Custom Domain.

**Audit Logging**

Use the Audit Log Retrieval API to view the audit logs stored for your subaccount. Use the audit log viewer

to display the audit logs for your Cloud Foundry account, produced by SAP applications and services you’ve

subscribed to. See Audit Logging in the Cloud Foundry Environment [page 2595].

**Credential Store**

SAP Credential Store provides a repository for passwords and keys for applications that are running on

SAP BTP, Cloud Foundry environment. It enables the applications to retrieve credentials and use them for

authentication to external services, or to perform cryptographic operations and TLS communication.

See SAP Credential Store.

**Malware Scanning**

Use the SAP Malware Scanning service to scan business documents for malware. Integrate this service

with your custom-developed apps running on the Cloud Foundry runtime. When your apps upload business

documents, your apps can call the SAP Malware Scanning service to check for viruses or other malware.

For more information, see SAP Malware Scanning Service.

**Related Information**

SAP Authorization and Trust Management Service [page 3180]

Audit Logging in the Cloud Foundry Environment [page 2595]

Principal Propagation [page 3257]

Data Protection and Privacy [page 3273]

Security in the Kyma Environment [page 3284]

**7.1 SAP Authorization and Trust Management Service**

The global account and subaccounts get their users from identity providers. Administrators make sure that

users can only access their dedicated subaccount by making sure that there is a dedicated trust relationship

**3180** PUBLIC

SAP Business Technology Platform

**Security**

only between the identity providers and the respective subaccounts. Developers configure and deploy

application-based security artifacts containing authorizations, and administrators assign these authorizations

using the SAP BTP cockpit.

 Note

Before you start, make yourself familiar with the sections about authentication and authorization of the

SAP BTP Planning and Lifecycle-Management Guide. See the Setting Up Your Security and Compliance

Model section.

• #unique\_390/unique\_390\_Connect\_42\_subsection-im1 [page 3182]

• #unique\_390/unique\_390\_Connect\_42\_subsection-im2 [page 3182]

• #unique\_390/unique\_390\_Connect\_42\_subsection-im3 [page 3183]

• #unique\_390/unique\_390\_Connect\_42\_subsection-im4 [page 3184]

• #unique\_390/unique\_390\_Connect\_42\_subsection-im5 [page 3185]

• #unique\_390/unique\_390\_Connect\_42\_subsection-im6 [page 3186]

• #unique\_390/unique\_390\_Connect\_42\_subsection-im7 [page 3187]

Hold your pointer over a box for a description. Select a box to display more information.

SAP Business Technology Platform

**Security** PUBLIC **3181**

**Overview of the SAP Authorization and Trust Management Service**

Get a high-level overview of the concepts that underpin the SAP Authorization and Trust Management service

for SAP BTP in the Cloud Foundry environment.

For more information, see What Is the SAP Authorization and Trust Management Service? [page 3187].

**Tutorials for the SAP Authorization and Trust Management Service**

Follow the tutorials below to get familiar with the SAP Authorization and Trust Management service in the

Cloud Foundry environment of SAP BTP.

Tutorials for the SAP Authorization

and Trust Management service in the

Cloud Foundry environment Language / Framework Link

Learn how to secure a basic single-tenant

Node.js application. Start with a

Node.js application that uses the express

framework and SAPUI5 to display

a list of products and add the security

components step by step.

Node.js SAP Developers

Learn how to secure a basic java application.

This tutorial starts with a Hello

World Java application built with SAP

Cloud SDK.

Java, SAP Cloud SDK SAP Developers

Learn how to build a cloud-native

Node.js application that features secured

service-to-service communication.

The application shows you two different

ways of securing service-to-service-

communication (by propagating a

business user or using a technical

user).

Node.js GitHub

Learn how to secure microservices in

SAP BTP using spring-xsuaa and

Spring security. Furthermore, learn how

to test the secured application using

the java-security-test utilities.

Spring (Boot) GitHub

Learn how to add multitenancy to a

node.js application and make it available

for other subaccounts using the

SaaS Provisioning service and the

XSUAA.

Node.js SAP Developers

**3182** PUBLIC

SAP Business Technology Platform

**Security**

Tutorials for the SAP Authorization

and Trust Management service in the

Cloud Foundry environment Language / Framework Link

Learn how to secure microservices in

SAP BTP. This sample provides J2EE

Configuration using web.xml and uses

the SAP Java Buildpack.

J2EE, SAP Java Buildpack GitHub (SAP Java Buildpack version

>=1.26.1)

GitHub (SAP Java Buildpack version <=

1.26.0)

Learn how to use the java-security

library to perform JWT Validation as

part of your Java application. Furthermore,

learn how to test the secured

application using the java-securitytest

utilities.

Java GitHub

Learn how to validate OAuth tokens using

a Python library. Use this library to

add authentication in your Python application.

 Note

This library isn't part of an SAP BTP

license. However, it belongs to a related

open source project.

Python GitHub

Learn in this reference application how

the service fits into a complete architecture

of microservices that interact

with each other propagating user information.

Java GitHub

**Principal Propagation**

Exchange user ID information between systems or environments in SAP BTP.

In This Section

• Principal Propagation from the Multi-Cloud Foundation to the Neo Environment [page 3264]

• Principal Propagation from the Neo Environment to the Multi-Cloud Foundation [page 3257]

Other Principal Propagation Scenarios

• On-Premise User Store

• Principal Propagation to OAuth-Protected Applications

• Connectivity in the Cloud Foundry Environment: Principal Propagation

• Connectivity in the Neo Environment: Principal Propagation

SAP Business Technology Platform

**Security** PUBLIC **3183**

**Trust and Federation**

When setting up accounts you need to assign users. While we provide you with your first users from the default

identity provider to get you started, your organization has identity providers that you want to integrate.

SAP BTP supports identity federation, a concept of linking and reusing digital identities of a user base across

loosely coupled systems. Identity federation frees applications on SAP BTP as well as the platform itself

from the need to obtain and store the credentials of users and to authenticate them. Instead, the user base

is reused from identity providers, which support the administration of digital user identities, authentication,

and authorizations in a centralized and decoupled manner. To enable communication between SAP BTP

and identity providers, you must cross-configure the communication endpoints of the involved systems,

establishing a trust relationship between them.

 Recommendation

We strongly recommend that you use a custom tenant of SAP Cloud Identity Services. Using SAP Cloud

Identity Services eases integration with other SAP solutions. When setting up accounts you need to assign

users. We provide you with your first users from the default identity provider. By using SAP Cloud Identity

Services as a proxy to your corporate identity provider and hosting your users there, you gain a number of

advantages:

• Integrate the management of these users with your broader identity management strategy, hosted

on your own identity providers. You control your own user lifecycle and single sign-on strategies

throughout the entire landscape.

• Enforce your own password and authentication policies, such as stronger passwords or multifactor

authentication.

For platform users, the use of SAP Cloud Identity Services is mandatory. If you don't have a tenant yet,

check Getting a Tenant.

To connect your corporate identity provider to SAP Cloud Identity Services, see Corporate Identity

Providers and Configure Conditional Authentication for an Application in What Is Identity Authentication

and SAP Cloud Identity Services

Identity Provider and XSUAA in SAP BTP Architecture

**3184** PUBLIC

SAP Business Technology Platform

**Security**

SAP Cloud Identity Services is a multitenancy-enabled identity provider for all SAP cloud applications

and optionally on-premise applications. The service provides capabilities for authentication, single sign-on,

authorizations, identity lifecycle management, and on-premise integration as well as self-services like selfregistration

or password reset.

SAP has its own SAP Cloud Identity Services tenant, SAP ID service. SAP ID service is the default identity

provider of SAP BTP and where you register to get initial access to SAP BTP. Trust to SAP ID service is

preconfigured by default.

We recommend that you request your own SAP Cloud Identity Services tenant (see Getting a Tenant). To

establish trust with your identity provider, proceed as follows.

For business users:

• Establish Trust and Federation Between SAP Authorization and Trust Management Service and SAP Cloud

Identity Services [page 2282]

• Manually Establish Trust and Federation Between SAP Authorization and Trust Management Service and

SAP Cloud Identity Services [page 2302]

• Establish Trust and Federation with UAA Using Any SAML Identity Provider [page 2306]

For platform users:

• Establish Trust and Federation of Custom Identity Providers for Platform Users [page 2316]

For default identity provider:

• Default Identity Provider

 Note

How you assign users to their authorizations depends on the type of trust configuration. If you’re using

the default trust configuration via SAP ID service, you can assign users directly to role collections. For

more information, see Default Identity Provider [page 2335].

However, if you’re using a custom trust configuration as described in this topic, you can assign

individual users or groups to role collections. Assigning users to their authorizations is part

of application administration, which is described here. For more information, see Mapping Role

Collections [page 2358].

**Administration: Managing Authentication and Authorization**

Application developers create and deploy application-based authorization artifacts for business users.

Administrators use this model to manage roles, build role collections, and assign these collections to users

or user groups. In this way, they control the users' permissions.

Setting Up Authorization Artifacts (Account Administrators)

Task Links

Assign the role collection to the users provided by an identity

provider

Working with Role Collections [page 2351]

(If you do use a custom identity provider) Assign the role collections

to user groups

Map Role Collections to User Groups [page 2358]

SAP Business Technology Platform

**Security** PUBLIC **3185**

Task Links

Assign the role collections to users and user groups, manage

attribute mappings

Mapping Role Collections [page 2358]

Create a role collection and assign roles to it Define a Role Collection [page 2352]

Use an existing role or create a new one using role templates Add Roles to Role Collections on the Application Level

[page 2370]

**Troubleshooting**

This section provides information on troubleshooting-related activities for the SAP Authorization and Trust

Management service in the Cloud Foundry environment.

 Tip

We also recommend that you regularly check the SAP Notes and Knowledge Base for component BC-CPCF-

SEC-IAM in the SAP Support Portal . These contain information about program corrections and

provide additional information.

To help you troubleshoot your issue, we also recommend increasing the log verbosity of your application

and application router. We provide a script to help you. If for some reason you can't use this script,

increase the log verbosity manually, see related link.

To troubleshoot problems with tokens from SAP Cloud Identity Services, see Logging OpenID Connect

Tokens in the documentation for SAP Cloud Identity Services.

Our troubleshooting information can be found in Troubleshooting for the SAP Authorization and Trust

Management service in the Cloud Foundry environment . Check the individual troubleshooting topics for

your error message. If you can't find your problem, create an incident in the component BC-CP-CF-SEC-IAM.

For more information, see the related link.

• The Security Tab Is Missing in the Subaccount

• Access Is Denied or Forbidden

• Identity Provider Could Not Process Authentication Request

• Logon Screen Shows "SAP HANA XS Advanced"

• Requested Route Does Not Exist

• Subdomain Does Not Map to a Valid Identity Zone

• No Client with Requested ID

• Login Issues

• Cannot Add Role Templates to Predefined Role Collections

• 502 Error: Call to /oauth/token Was Not Successful

• Unexpected AuthnResponse : Existing authentication - <User>

• AuthnRequest expired - ID: <RequestId> Destination: <IdPDestination>

• InResponseToField of Response doesn‘t correspond to the sent message

• Response issue time is either too old or with date in the future. Sync IdP to match skew <skew>

• Trust establishment issues

• Token retrieval fails with status code 401

**3186** PUBLIC

SAP Business Technology Platform

**Security**

• Cockpit displays HTTP status 500 error on logon with custom IdP user

• IAS application reference isn't created in your IAS tenant

• User base doesn't appear in existing Neo subaccounts

• User from corporate IdP can't log on to Neo subaccount

• 409 error code on deleting a custom identity provider

• Share Authorization and Trust Management service instances

• Invalid "redirect\_uri"

**Adding Authentication and Authorization**

Developers create authorization information for business users in their environment and deploy this

information in an application. They make this available to administrators, who complete the authorization

setup and assign the authorizations to business users.

Developers store authorization information as design-time role templates in the xs-security.json security

descriptor file. Using the cockpit, administrators of the environment assign the authorizations to business

users.

The following sections contain the process of adding authentication and authorization checks for protecting

your applications, links to a number of associated tutorials, extended tasks for creating authorization artifacts,

as well as reference information, including the syntax required to set the properties and values defined in the

application security descriptor file.

• Protecting Your Application [page 533]

• Tutorials for the SAP Authorization and Trust Management Service [page 558]

• Application Security Descriptor Configuration Syntax [page 576]

**7.1.1 What Is the SAP Authorization and Trust Management**

**Service?**

Get a high-level overview of the concepts that underpin the SAP Authorization and Trust Management service

for SAP BTP in the Cloud Foundry environment.

The SAP Authorization and Trust Management service lets you manage user authorizations and trust to

identity providers. Identity providers are the user base for applications. We recommend that you use an

SAP Cloud Identity Services tenant, an SAP on-premise system, or a custom corporate identity provider.

User authorizations are managed using technical roles at the application level, which can be aggregated into

business-level role collections for large-scale cloud scenarios.

**Environment**

The SAP Authorization and Trust Management service is available for consumption in the following SAP BTP

environments:

• Cloud Foundry

• Kyma

SAP Business Technology Platform

**Security** PUBLIC **3187**

• Neo

 Note

This documentation refers to SAP BTP for multi-environment subaccounts.

If you're looking for documentation about the Neo environment, see Authorization and Trust Management

in the Neo Environment.

**Features**

Use your corporate or a

default IdP

Enable user management for your applications by handling authentication to

an external identity provider. Start with SAP ID service as a pre-configured

easy-to-use identity provider. Switch to your corporate identity provider for

customized user management.

Enable role-based access to

applications

Enable different privileges to users accessing your applications based on roles.

**Overview**

The following figure shows a high-level overview of components, which comprise an SAP BTP business web

applications and how these applications are embedded in the Cloud Foundry environment. Further details have

been omitted for the sake of simplicity. It’s further assumed that the Cloud Foundry environment is set up with

basic configuration (that is, container-to-container networking isn’t configured). The components and their

interactions are depicted in the following block-diagram.

**Application, Microservice, and App**

The components and their interactions are depicted in the previous block-diagram. It shows a runtime platform

for business web applications. These are referred to as applications. An SAP BTP application is implemented

**3188** PUBLIC

SAP Business Technology Platform

**Security**

in an architectural style that structures the application as a collection of loosely coupled components, termed

microservices. Microservices can be deployed independently from one another. This eliminates the need to

deploy the complete application if only a subset of its microservices have received new features or a bug fix. In

the terminology of the Cloud Foundry environment of SAP BTP, microservices are referred to as apps.

**Application Architecture**

The application consists of a distinct gateway app with at least one or more resource apps. The gateway serves

as a reverse-proxy and provides functionality for security and session management. The application router app

is a standard implementation of the gateway and is used as the single point-of-entry for the application. It also

serves static content, initiates the authentication process, checks on cross-site request forgery (XSRF) attacks,

and forwards requests to the resource apps while propagating user information.

The resource apps can use the security client library, which also provides security functionality. As stated in

the previous section, all apps represent microservices, in the meaning of an app engineered and operated

according to the 12-factor paradigm. All apps run in their dedicated runtime containers, which are hosted on

the Cloud Foundry runtime platform.

**OAuth 2.0, Resource Owner, Client, Resource Server, and the SAP Authorization and Trust**

**Management Service**

The security functionality of SAP BTP is based on the OAuth 2.0 specification. OAuth 2.0 defines how a user -

the OAuth 2.0 resource owner - can delegate all or a subset of the authorizations to a third-party application -

the OAuth 2.0 client - without the third-party application needing to know the credentials of the user.

The Cloud Foundry environment uses a standard implementation of OAuth 2.0 to protect its platform

resources (orgs, spaces, and platform operations on those entities).

However, the OAuth 2.0 specification is reused for SAP BTP with a proprietary implementation to protect

the resources of business web applications powered by the Cloud Foundry environment. The proprietary

implementation exchanges the responsibilities of the OAuth 2.0 entities, client and resource owner: the OAuth

2.0 client - represented by the application - holds all the authorizations. A set or sub-set of these authorizations

is assigned to the user after authentication in the system. The application also acts as the OAuth 2.0 resource

server because it contains the resource apps. All apps of an application operate under the same OAuth 2.0

client.

The SAP Authorization and Trust Management service (XSUAA) provides functionality for administrating and

assigning application authorizations. It acts as the OAuth 2.0 authorization server and represents a typical

reuse service. The SAP Authorization and Trust Management servicebroker creates a service instance for each

application. Each app that wants to enforce authorizations with the security client library is then bound to this

SAP Authorization and Trust Management service instance of the corresponding application.

 Note

The Cloud Foundry environment also supports the following token grant types of Cloud Foundry.

• Authorization code grant

• Client credentials grant

• SAML 2.0 bearer grant

Refresh tokens are supported as well.

For more information, see the Cloud Foundry environment's API reference of the User Account and

Authentication and the related link.