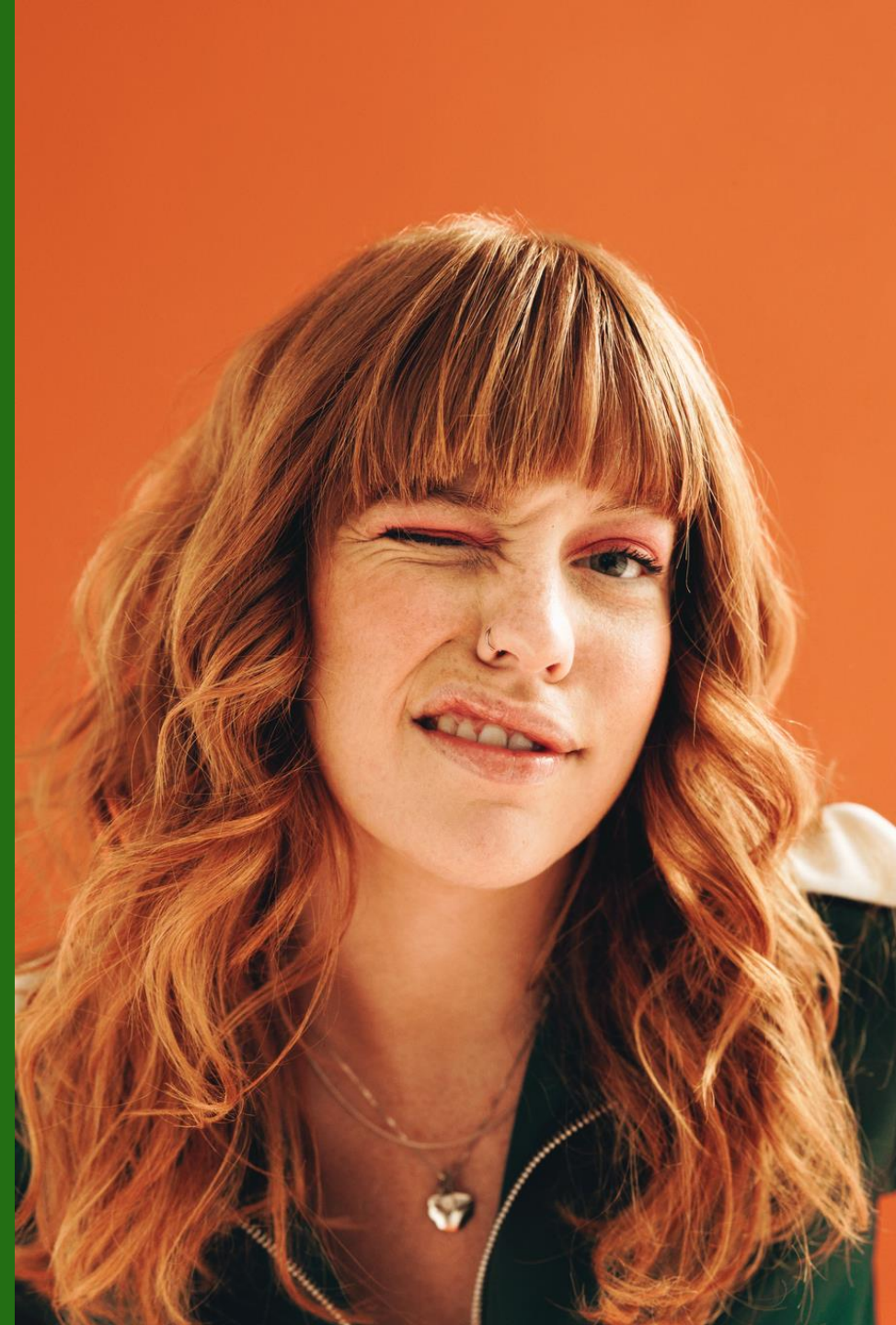


Day 2 Operations

Secure Configuration for your SAP BTP Services

Christian Cohrs, Jürgen Adolf, Hendrik Müller
SAP SE

LIVE SESSION



Agenda

Introduction to the SAP BTP Security Recommendations

Monitoring Security Recommendations in SAP Cloud ALM


Recommendations for high-priority scenarios



Additional learning resources


Introduction to the SAP BTP Security Recommendations




SAP BTP Security Recommendations

 **Help Portal (Documentation)**

[Browse by Product](#) | [SAP Learning Journeys](#) | [What's New](#) | [Explore SAP](#) |  

 [Favorite](#) [Download PDF](#) [Share](#)

 **Note**

Not all SAP BTP services are listed yet. We've started with core security services and are extending this list service by service.
If your service is missing, see also the *Security* services in your section of the service documentation on the [SAP Help Portal](#).

See also [Explanation of Table Headings](#).

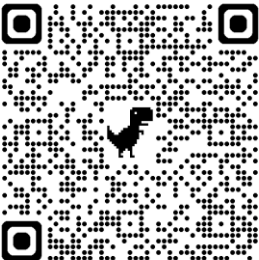
Security Recommendations

Hide/Show Columns ▼

Download Data ▼

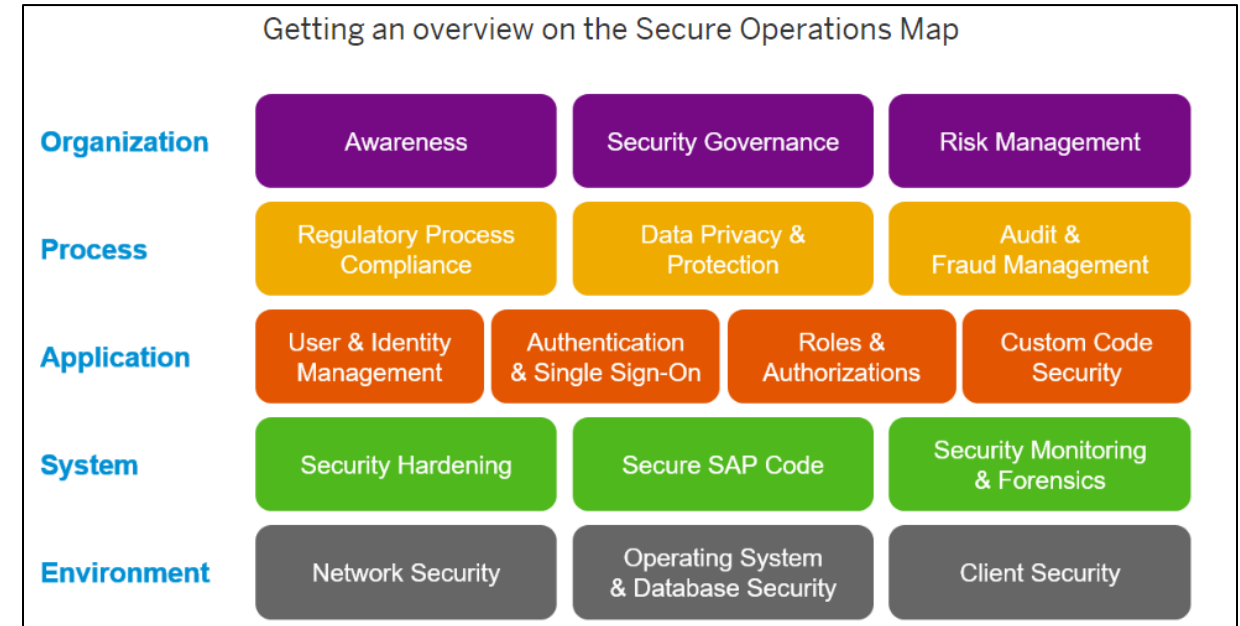
Search entire table

Component	Priority	Secure Operations Map	Title	Default Setting or Behavior	Recommendation	More Information	Last Update	Index
<div>Filter: [No Selection] ▼</div>	<div>Filter: [No Selection] ▼</div>	<div>Filter: [No Selection] ▼</div>					<div>Search column</div>	<div>Search column</div>
Identity Authentication	Critical	Authentication and Single Sign-On	Default Authentication of Administrators	The default authentication method for the administration console is user name and password.	Always protect the administration console application with multifactor authentication.	Configure Risk-Based Authentication for an Application	2023-04-12	BTP-IAS-0001
Identity Authentication	Recommended	Authentication and Single Sign-On	Password Policies	The service supports multiple levels of password security. The default setting is Standard. The main difference between Standard and Enterprise is the enforcement of password change. If these policies don't meet your corporate requirements, create custom policies.	If password-based authentication is mandatory for you, we recommend Enterprise over Standard, because it's the only option to fix leaked accounts. Better is the deactivation of passwords for employees if applicable. See BTP-IAS-0006 .	Configure Custom Password Policy	2023-04-12	BTP-IAS-0002

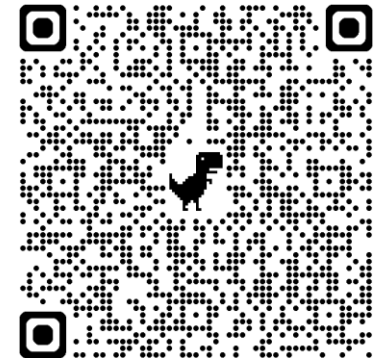


SAP BTP Security Recommendations - Structure

Component	Priority	Secure Operations Map
Filter: [No Selection] ▼	Filter: [No Selection] ▼	Filter: [No Selection] ▼
Filter Values		
<input type="checkbox"/> Select All	<input type="checkbox"/> Select All	<input type="checkbox"/> Select All
<input type="checkbox"/> Application Logging Service	<input type="checkbox"/> Advanced	<input type="checkbox"/> Authentication and Single Sign-On
<input type="checkbox"/> Authorization and Trust Management Service	<input type="checkbox"/> Critical	<input type="checkbox"/> Awareness
<input type="checkbox"/> Cloud Connector	<input type="checkbox"/> Recommended	<input type="checkbox"/> Regulatory Process Compliance
<input type="checkbox"/> Cloud Transport Management		<input type="checkbox"/> Roles and Authorizations
<input type="checkbox"/> Credential Store		<input type="checkbox"/> Secure SAP Code
<input type="checkbox"/> Custom Domain Service		<input type="checkbox"/> Security Governance
<input type="checkbox"/> Identity Authentication		<input type="checkbox"/> Security Hardening
<input type="checkbox"/> Mobile Services		<input type="checkbox"/> Security Monitoring and Forensics
<input type="checkbox"/> SAP Audit Log service		




[Secure Operations Map](#)





Monitoring Security Recommendations in SAP Cloud ALM




SAP BTP Security Recommendations - in SAP Cloud ALM

 **Help Portal**



Browse by Product | SAP Learning Journeys | What's New | Explore SAP |  



Home > SAP Business Technology Platform (SAP BTP) > SAP BTP Security Recommendations > Monitor Security Recommendations with SAP Cloud ALM

SAP BTP Security Recommendations English ▼

This document ▼ 

▼ Advanced Search

☆ Favorite  Download PDF  Share <<

Monitor Security Recommendations with SAP Cloud ALM


To support you with the application lifecycle management of SAP BTP components, SAP BTP pushes the configuration status of components to SAP Cloud ALM. In SAP Cloud ALM, you can monitor which of your components are configured in alignment with our recommendations.

Prerequisites

Your organization has subscribed to SAP Cloud ALM.

For more information, see [Required Setup for SAP Cloud ALM](#) in *Setup and Administration for SAP Cloud ALM*.

Context

 **Note**

Not all SAP BTP components are integrated yet. We've started with the core components and are extending this list component-by-component.

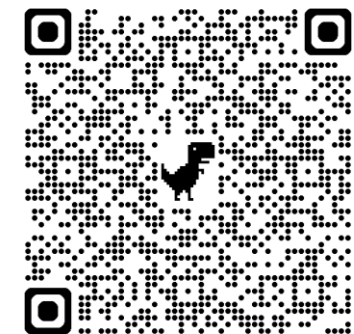
Not all recommendations of each component can be monitored. You must manually monitor those recommendations that can't be monitored automatically.

- Review the list of recommendations for the components that you use.

For more information, see [SAP BTP Security Recommendations](#).

- Review the config stores from SAP BTP components available to SAP Cloud ALM.

For more information, see [Configuration & Security Analysis - Content](#) in the *SAP Cloud ALM for Operations Expert Portal*.



SAP Cloud ALM – Configurations- & Security Analysis

From Data to Dashboards



Daily Snapshot

Configuration Stores & History

Browse
Search
Change Analysis
Home Screen with Cloud Service Status

Outbound API



Browse - Example

SAP

Configuration & Security Analysis

Store Browser

Services / Systems

Search

Name	Description	Type	
IdentityAuthentication01	IdentityAuthentication 01 (CSA)	Identity Authentication	>
IdentityAuthentication02	IdentityAuthentication 02 (CSA)	Identity Authentication	>

Services / Systems / Configuration Stores of IdentityAuthentication01

Search

Landscape object	Description	Store Name	Store Type	Data range (To)	
SYSTEM_APP SAP Cloud Identity	System Application Configuration	IAS_SYS_APP_CONFIG_SECREC	TABLE	Jun 25, 2025, 5:02:04 AM	>
SYSTEM_APP Administration Console	System Application Configuration	IAS_SYS_APP_CONFIG_SECREC	TABLE	Jun 25, 2025, 5:02:04 AM	>
System IdentityAuthentication01	Password Policy	IAS_PASSWORD_POLICIES	TABLE	Jun 25, 2025, 5:02:04 AM	>
System IdentityAuthentication01	Landscape information	IAS_LANDSCAPE_INFO	TABLE	Jun 25, 2025, 5:02:04 AM	>
CORPORATE_IDP simona	IAS CORPORATE IDP CONFIG	IAS_CORPORATE_IDP_CONFIG_SECREC	TABLE	Jun 25, 2025, 5:02:04 AM	>
CORPORATE_IDP svetla	IAS CORPORATE IDP CONFIG	IAS_CORPORATE_IDP_CONFIG_SECREC	TABLE	Jun 25, 2025, 5:02:04 AM	>
CORPORATE_IDP fb5e2403-c166-465a-b0dc-...	IAS CORPORATE IDP CONFIG				
CORPORATE_IDP c5f7f892-be97-446c-8d31-b...	IAS CORPORATE IDP CONFIG				
CORPORATE_IDP HANA Cloud Platform	IAS CORPORATE IDP CONFIG				
CORPORATE_IDP SAP Cloud Platform Identity ...	IAS CORPORATE IDP CONFIG				
CORPORATE_IDP Model S	IAS CORPORATE IDP CONFIG				
System IdentityAuthentication01	Identity Authentication Configuration				
CHARGED_APP victorTest	Charged Application Risk Based Authen				
CHARGED_APP Golden Holidays	Charged Application Configuration				

Services / Systems / Configuration Stores of IdentityAuthentication01 / Items of IAS_SYS_APP_CONFIG_SECREC (IdentityAuthentication01)

Show deleted

Search

Key	Value	Type of Event	Valid since	
NAME = password_policy	VALUE = standard SECREC_STATUS = NONCOMPL... SECREC_INDEX = BTP-IAS-0002	INITIAL	Feb 18, 2025, 4:02:00 AM	>
NAME = reCAPTCHA	VALUE = SECREC_STATUS = COMPLIANT SECREC_INDEX = BTP-IAS-0025	INITIAL	Feb 18, 2025, 4:02:00 AM	>
NAME = branding	VALUE = SECREC_STATUS = NONCOMPL... SECREC_INDEX = BTP-IAS-0021	INITIAL	Feb 18, 2025, 4:02:00 AM	>
NAME = social_sign_on	VALUE = OFF SECREC_STATUS = COMPLIANT	INITIAL	Feb 18, 2025, 4:02:00 AM	>

Search – Examples

Example

1.

The screenshot shows the SAP Configuration & Security Analysis interface. The search bar at the top contains the text 'password_policy'. Below the search bar, a table displays the search results. The table has five columns: Managed Object, Item Description, Store Name, Item key, and Item value. The search results are filtered to show only items where the Item key is 'password_policy'.

Managed Object	Item Description	Store Name	Item key	Item value
CHARGED_APP Angel Fish00	Charged Application Configuration	IAS_CHARGED_APP_CONFIG_SECREC	NAME = password_policy	VALUE = delegated_to_corp_idp SECREC_STATUS = UNRATED SECREC_INDEX = BTP-IAS-0002
SYSTEM_APP SAP Cloud Identity	System Application Configuration	IAS_SYS_APP_CONFIG_SECREC	NAME = password_policy	VALUE = standard SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0002
CHARGED_APP New app.	Charged Application Configuration	IAS_CHARGED_APP_CONFIG_SECREC	NAME = password_policy	VALUE = standard SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0002
CHARGED_APP Shopping	Charged Application Configuration	IAS_CHARGED_APP_CONFIG_SECREC	NAME = password_policy	VALUE = delegated_to_corp_idp SECREC_STATUS = UNRATED

Example

2.

The screenshot shows the SAP Configuration & Security Analysis interface. The search bar at the top contains the text 'noncompliant'. Below the search bar, a table displays the search results. The table has five columns: Managed Object, Item Description, Store Name, Item key, and Item value. The search results are filtered to show only items where the Item value contains the word 'NONCOMPLIANT'.

Managed Object	Item Description	Store Name	Item key	Item value
System IdentityAuthentication02	Identity Authentication Configuration	IAS_CONFIG_SECREC	NAME = mail_server_configuration	VALUE = SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0020
System IdentityAuthentication02	Identity Authentication Configuration	IAS_CONFIG_SECREC	NAME = security_alerts	VALUE = email_change=OFF,login_name_change=OFF,password_change=OFF,tfa_change=ON SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0023
System IdentityAuthentication01	Identity Authentication Configuration	IAS_CONFIG_SECREC	NAME = audit_logs	VALUE = SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0011
System IdentityAuthentication01	Identity Authentication Configuration	IAS_CONFIG_SECREC	NAME = certificate_authentication	VALUE = SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0006

Change Analysis – Example

SAP

Configuration & Security Analysis

Changes

Changes / Items of IdentityAuthentication01

Time Frame Selection (01/01/2024, 00:00:00 - 31/12/2024, 23:59:59)

Search

Date	Landscape Object	Store Name	Description	Changes	Download Table
25/11/2024	System IdentityAuthentication01	IAS_CONFIG_SECREC	Identity Authentication Configuration	17	Download Table with Changed Items
12/12/2024	System IdentityAuthentication01	IAS_CONFIG_SECREC	Identity Authentication Configuration	40	
12/12/2024	System IdentityAuthentication01	IAS_PASSWORD_POLICIES	Password Policy	3	
25/11/2024	System IdentityAuthentication01	IAS_LANDSCAPE_INFO	Landscape information	4	
28/11/2024	System IdentityAuthentication01	IAS_LANDSCAPE_INFO	Landscape information	6	

A	B	C	D	E	F	G	H
System Name	Store Name	Store Description	Store Type	Key	Value	Type of Event	Valid Since
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_BUNDLED_APP_CONFIG_SEC	Bundled Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_BUNDLED_APP_CONFIG_SEC	Bundled Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_BUNDLED_APP_CONFIG_SEC	Bundled Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_SYS_APP_CONFIG_SEC	System Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = b638b739-2eac-46aa-a9b6-	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = SECREC_STATUS = SECR	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = SECREC_STATUS = SECR	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = SECREC_STATUS = SECR	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = SECREC_STATUS = SECR	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = SECREC_STATUS = SECR	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = SECREC_STATUS = SECR	ADDED	2025-04-05T03:02:00Z
IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SEC	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = SECREC_STATUS = SECR	ADDED	2025-04-05T03:02:00Z

Downloads

Configuration & Security Analysis_IdentityAuthentication01(2025-06-25T11_27_43.664Z).xlsx

Open file

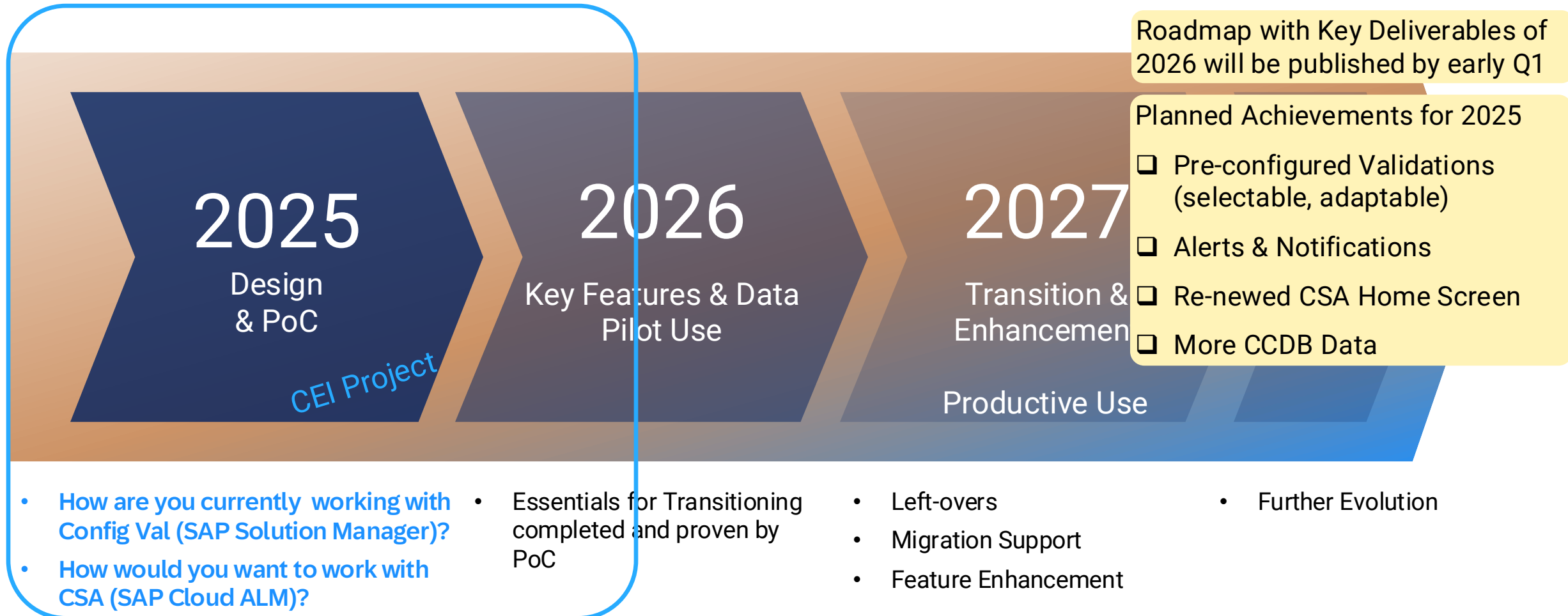
Public

11

Outlook – Customer Engagement Initiative will shape our Roadmap

SAP aims to deliver product readiness for your transition from SAP Solution Manager ConfigVal to SAP Cloud ALM Configuration and Security Analysis by End of 2026.

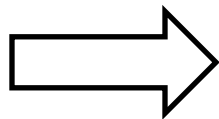
Planned duration of CEI



SAP Cloud ALM – Configuration & Security Analysis *new* HOME Screen

The screenshot shows the current interface of the SAP Cloud ALM Configuration & Security Analysis tool. The header includes the SAP logo and the title 'Configuration & Security Analysis'. Below the header, there are tabs for 'Overview' and 'Favorites'. The 'Overview' tab is active, showing a card for 'IdentityAuthentication01' with a status of 'READY' and a 'Number of Stores' of 60. The 'Favorites' tab shows a card for 'QKJ'.

Today



Planned

The screenshot shows the planned interface of the SAP Cloud ALM Configuration & Security Analysis tool. The header includes the SAP logo and the title 'Configuration & Security Analysis'. Below the header, there are tabs for 'Overview' and 'Favorites'. The 'Overview' tab is active, showing a card for 'IdentityAuthentication01' with a status of 'READY' and a 'Number of Stores' of 60. The 'Favorites' tab shows a card for 'QKJ'.

Metrics

36	7	126
----	---	-----

Compliance

63 %

Quality Open Alerts 54

Lab Preview

High-Priority Scenarios

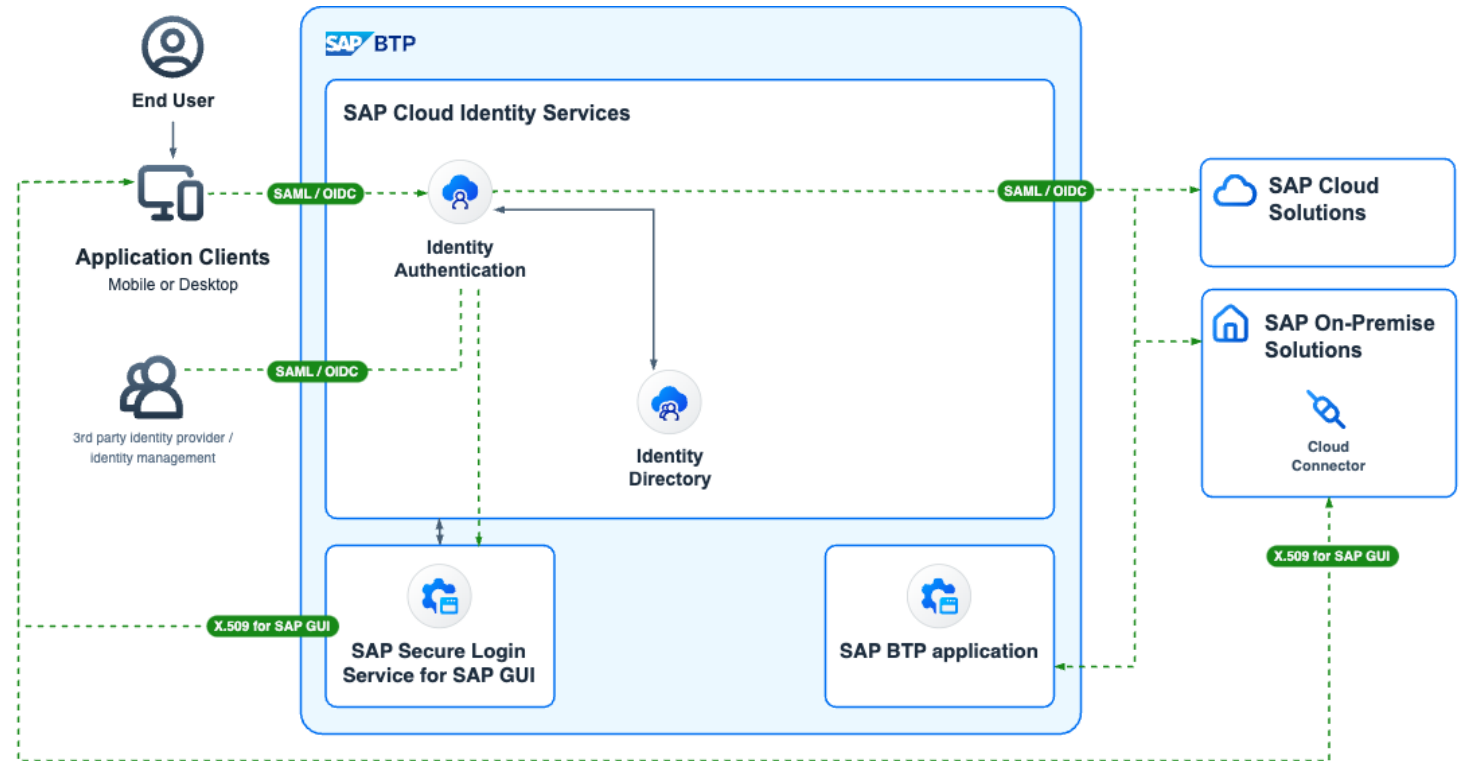
SAP Cloud Identity Services



SAP Cloud Identity Services – Identity Authentication

Identity Authentication

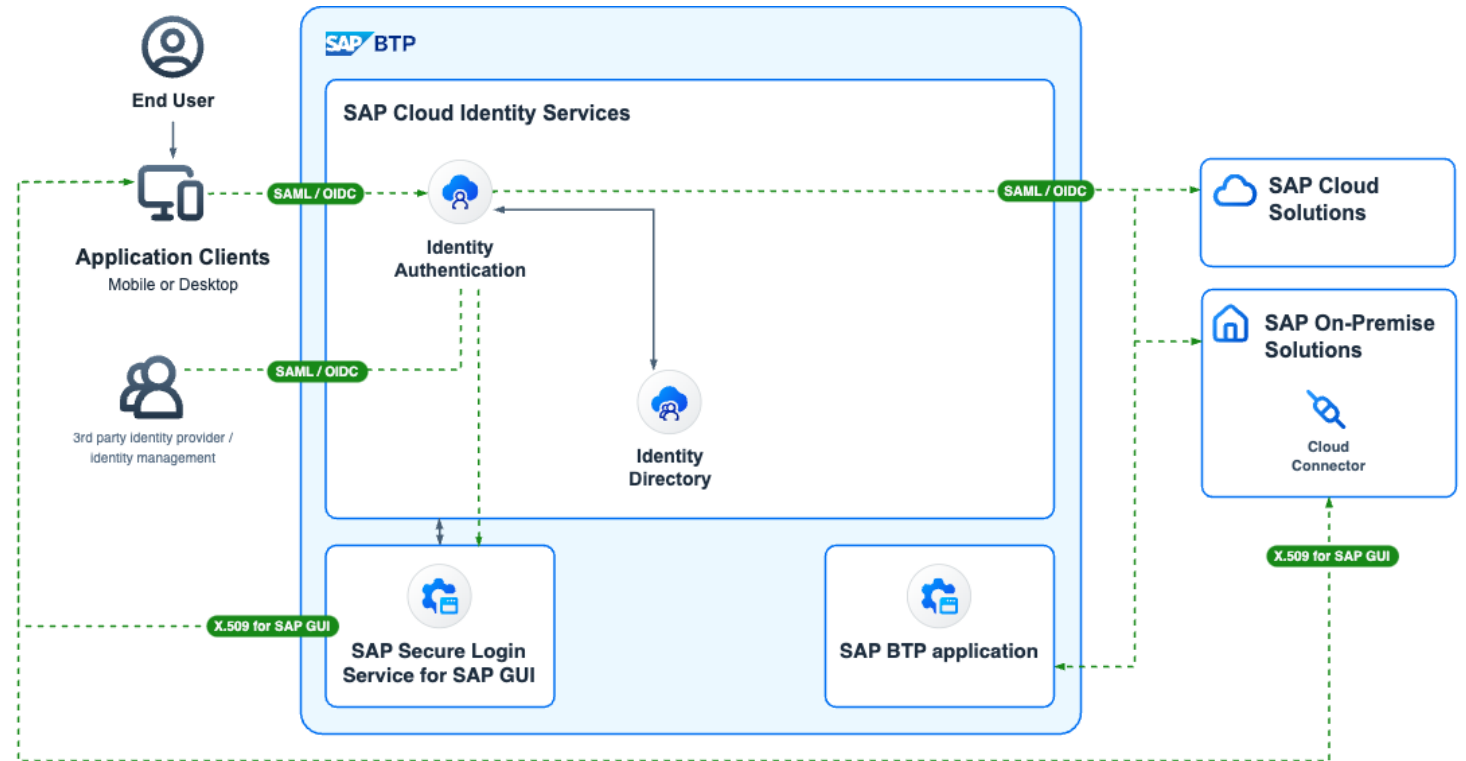
- Identity provider supporting **SAML** or **OpenID Connect**
- SAP's strategic solution for authentication
- **Pre-configured trust** for many SAP cloud applications
- Option to act as **proxy** for a 3rd party Identity Provider



SAP Cloud Identity Services – Identity Authentication

Secure Access Starts Here

- Enforce MFA for admin console access
- Use [passwordless](#) authentication where possible (certificate, FIDO)
- Keep self-registration and social sign-on disabled
- Integrate with an existing corporate identity provider
- Manage trust settings with 3rd-party identity providers



Security Configurations and Recommendations – How is it in SAP Cloud ALM?

SAP Configuration & Security Analysis

Store Browser

Services / Systems / Configuration Stores of IdentityAuthentication01 / Items of IAS_SYS_APP_CONFIG_SECREC (IdentityAuthentication01)

Show deleted Search

Key	Value	Type of Event	Valid since
NAME = default_authenticating_idp_name	VALUE = validation.accounts400.ondema SECREC_STATUS = SECREC_INDEX =		
NAME = disable_password_authentication	VALUE = SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0006		
NAME = default_authenticating_idp_type	VALUE = SAP_ID_SERVICE SECREC_STATUS = SECREC_INDEX =		
NAME = password_policy	VALUE = enterprise SECREC_STATUS = COMPLIANT SECREC_INDEX = BTP-IAS-0002		
NAME = reCAPTCHA	VALUE = SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0025	INITIAL	Feb 18, 2025, 4:02:00 AM
NAME = branding	VALUE = SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0021	INITIAL	Feb 18, 2025, 4:02:00 AM
NAME = social_sign_on	VALUE = OFF SECREC_STATUS = COMPLIANT SECREC_INDEX = BTP-IAS-0005		
NAME = user_application_access	VALUE = public SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0003		
NAME = admin_console_mfa	VALUE = misconfigured SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0001		

Expected IDP is configured as default

Only passwordless authentication is allowed

IAS running in proxy mode or as default IDP ?

Expected Password Policy is configured

No Authentication with Google, Facebook, etc.

No self-registration of users

Admin Console Access only via Multi Factor Authentication(enforced)

BTP-IAS-0006

BTP-IAS-0002

BTP-IAS-0005

BTP-IAS-0003

BTP-IAS-0001

Password Policy – Representation in SAP Cloud ALM

[illegible]

SAP Cloud Identity Services – Identity Authentication

Custom Platform IdP in the SAP Business Technology Platform

- Identity Authentication Service is the Identity Provider for SAP BTP-based applications, stand-alone or in proxy mode
- IAS can also be used to authenticate platform users (BTP admins) on subaccount and global account level
- With IAS as a proxy, platform users can be authenticated by the corporate IdP

The screenshot shows the SAP BTP Cockpit interface for the 'Global Account: 7ada904ctrial - Trust Configuration'. The left sidebar contains navigation options: Account Explorer, Resource Providers, Boosters, System Landscape, Entitlements, Security (expanded), Users, Role Collections, Trust Configuration (selected), and Usage. The main content area displays a table of identity providers. A blue banner at the top right says 'Establish Trust'. A blue information box states: 'Add identity providers for platform users to enable users to log on to platform tools such as SAP BTP cockpit, SAP BTP CLI, and environments. Manage identity providers for business applications in your subaccounts.'

Name	Description	Origin Key (Cloud Foundry)	SAP BTP Cockpit	SAP BTP CLI	Actions
Default					
Default identity provider	Default identity provider		Open		Open
Custom Identity Provider for Platform Users					
aznauyuf.trial-accounts.ondemand.com (platform users)	Identity Authentication tenant aznauyuf.trial-accounts.ondemand.com used for platform users	aznauyuf-platform	Open	aznauyuf.trial-accounts.ondemand.com	Open

Learn more about how to [configure trust to platform identity providers](#).

Default IDP of each and every Service or App connected to IAS

SAP

Configuration & Security Analysis

0

Store Browser

Services / Systems / Configuration Stores of IdentityAuthentication01 / Items of IAS_SYS_APP_CONFIG_SECREC (IdentityAuthentication01)

Show deletedSearch

Key	Value	Type of Event	Valid since	
NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-be565431e6eb SECREC_STATUS = SECREC_INDEX =	ADDED	Apr 5, 2025, 5:02:00 AM	>
NAME = default_authenticating_idp_display_name	VALUE = SECREC_STATUS = SECREC_INDEX =	INITIAL	Feb 18, 2025, 4:02:00 AM	>
NAME = default_authenticating_idp_name	VALUE = validation.accounts400.ondemand.com SECREC_STATUS = SECREC_INDEX =	INITIAL	Feb 18, 2025, 4:02:00 AM	>
NAME = disable_password_authentication	VALUE = SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0006	INITIAL	Feb 18, 2025, 4:02:00 AM	>
NAME = default_authenticating_idp_type	VALUE = SAP_ID_SERVICE SECREC_STATUS = SECREC_INDEX =	INITIAL	Feb 18, 2025, 4:02:00 AM	>

Configurations of each and every connected IDP

Is configuration with regard to my Corporate IDP as expected?

Services / Systems / Configuration Stores of IdentityAuthentication01 / Items of IAS_CORPORATE_IDP_CONFIG_SECREC (IdentityAuthentication01)

Show details

Key	Value	Type of Event	Valid since	
NAME = allow_identity_auth_users_only	VALUE = OFF SECREC_STATUS = SECREC_INDEX =	INITIAL	Apr 5, 2025, 5:02:00AM	>
NAME = apply_app_auth_configs	VALUE = OFF SECREC_STATUS = SECREC_INDEX =	INITIAL	Apr 5, 2025, 5:02:00AM	>
NAME = default_signing_algorithm	VALUE = SHA1 SECREC_STATUS = SECREC_INDEX =	INITIAL	Apr 5, 2025, 5:02:00AM	>
NAME = forward_all_sso_requests	VALUE = OFF SECREC_STATUS = SECREC_INDEX =	INITIAL	Apr 5, 2025, 5:02:00AM	>
NAME = identity_provider_display_name	VALUE = svetla SECREC_STATUS = SECREC_INDEX =	INITIAL	Apr 5, 2025, 5:02:00AM	>
NAME = identity_provider_id	VALUE = b638b739-2eac-46aa-a9b6-5bb1e4424c79 SECREC_STATUS = SECREC_INDEX =	INITIAL	Apr 5, 2025, 5:02:00AM	>
NAME = identity_provider_name	VALUE = svetla.accounts400.ondemand.com SECREC_STATUS = SECREC_INDEX =	INITIAL	Apr 5, 2025, 5:02:00AM	>
NAME = identity_provider_type	VALUE = SAML_2.0 SECREC_STATUS = SECREC_INDEX =	INITIAL	Apr 5, 2025, 5:02:00AM	>
NAME = logout_redirect_url	VALUE = SECREC_STATUS = SECREC_INDEX =	INITIAL	Apr 5, 2025, 5:02:00AM	>
NAME = sign_authentication_requests	VALUE = ALWAYS SECREC_STATUS = SECREC_INDEX =	INITIAL	Apr 5, 2025, 5:02:00AM	>
NAME = sign_logout_messages	VALUE = ALWAYS SECREC_STATUS = SECREC_INDEX =	INITIAL	Apr 5, 2025, 5:02:00AM	>

Is there a new (unexpected) IDP in my landscape ?

Services / Systems / Configuration Stores of IdentityAuthentication01 / Items of IAS_LANDSCAPE_INFO (IdentityAuthentication01)

Key	Value	Type of Event	Valid since	
ID = b71e44eb-5d2f-4499-85b4-6d008ff838ff	ID_REF = TYPE = CHARGED_APP NAME = AMS Test Application DESCR =	ADDED	May 13, 2025, 5:02:02AM	>
ID = b96a0ca0-ac36-452e-bfdd-9d8c50cf4342	ID_REF = TYPE = CHARGED_APP NAME = Cook Book DESCR =	ADDED	May 13, 2025, 5:02:02AM	>
ID = bbc686c9-b6b5-4428-bc05-e2c85662164a	ID_REF = TYPE = CHARGED_APP NAME = Security Tools DESCR =	ADDED	May 13, 2025, 5:02:02AM	>
ID = bf86b640-3496-4701-bf00-42cd52f797a7	ID_REF = TYPE = CHARGED_APP NAME = Global Management DESCR =	ADDED	May 13, 2025, 5:02:02AM	>
ID = c5f7f892-be97-446c-8d31-be565431e6eb	ID_REF = TYPE = CORPORATE_IDP NAME = DESCR =	ADDED	May 13, 2025, 5:02:02AM	>
ID = c606a0b7-9a48-468a-9815-3bcf38c20e6c	ID_REF = TYPE = CORPORATE_IDP NAME = simona DESCR =	ADDED	May 13, 2025, 5:02:02AM	>
ID = ceb1effe-fce8-4e0b-9631-82af7fa20ab2	ID_REF = TYPE = BUNDLED_APP NAME = Test DESCR =	ADDED	May 13, 2025, 5:02:02AM	>
ID = d14db9f5-dbec-43d0-85c3-f83270b63a56	ID_REF = TYPE = CHARGED_APP NAME = Hello DESCR =	ADDED	May 13, 2025, 5:02:02AM	>
ID = d7e8d480-89a0-46f7-9fd7-e586d54ca254	ID_REF = TYPE = CHARGED_APP NAME = Conditional Auth Test DESCR =	ADDED	May 13, 2025, 5:02:02AM	>

Authorizations for Cloud Identity – representation in SAP Cloud ALM

Priority	Secure Operations Map	Title	Default Setting or Behavior	Recommendation	More Information	Last Update	Index
Recommended	User & Identity Management	Critical Administrator Authorizations	Identity Authentication plays a critical role in the access to SAP cloud applications. Because the central role of the service, it's required to reduce the number of administrators with full access. Identity Authentication permissions are based on the internal user store and its permission concept.	<p>The assignment of the following authorizations is critical. Manage them ideally as part of your identity lifecycle process.</p> <ul style="list-style-type: none"> • Manage Corporate Identity Providers • Manage Tenant Configuration • Manage Users 	List Administrators	2023-04-12	BTP-IAS-0017

Services / Systems / Configuration Stores of IdentityAuthentication01 / Items of IAS_CONFIG_SECREC (IdentityAuthentication01)

[Show >](#)

Key	Value	Type of Event	Valid since	
NAME = manage_applications_admin_count	VALUE = systems=2;users=29 SECREC_STATUS = SECREC_INDEX =	UPDATED	May 14, 2025, 5:02:03AM	>
NAME = manage_corp_idp_admin_count	VALUE = systems=2;users=29 SECREC_STATUS = SECREC_INDEX =	UPDATED	May 14, 2025, 5:02:03AM	>
NAME = manage_groups_admin_count	VALUE = systems=1;users=10 SECREC_STATUS = SECREC_INDEX =	UPDATED	May 14, 2025, 5:02:03AM	>
NAME = manage_identity_provisioning_admin...	VALUE = systems=0;users=1 SECREC_STATUS = SECREC_INDEX =	UPDATED	May 14, 2025, 5:02:03AM	>
NAME = manage_tenant_configuration_admin...	VALUE = systems=2;users=29 SECREC_STATUS = SECREC_INDEX =	UPDATED	May 14, 2025, 5:02:03AM	>
NAME = manage_users_admin_count	VALUE = systems=2;users=29 SECREC_STATUS = SECREC_INDEX =	UPDATED	May 14, 2025, 5:02:03AM	>

BTP-IAS-0017
Grant of Critical Authorizations should stay under control !

SAP Cloud Identity Services – Policy-based cockpit authorizations (new)

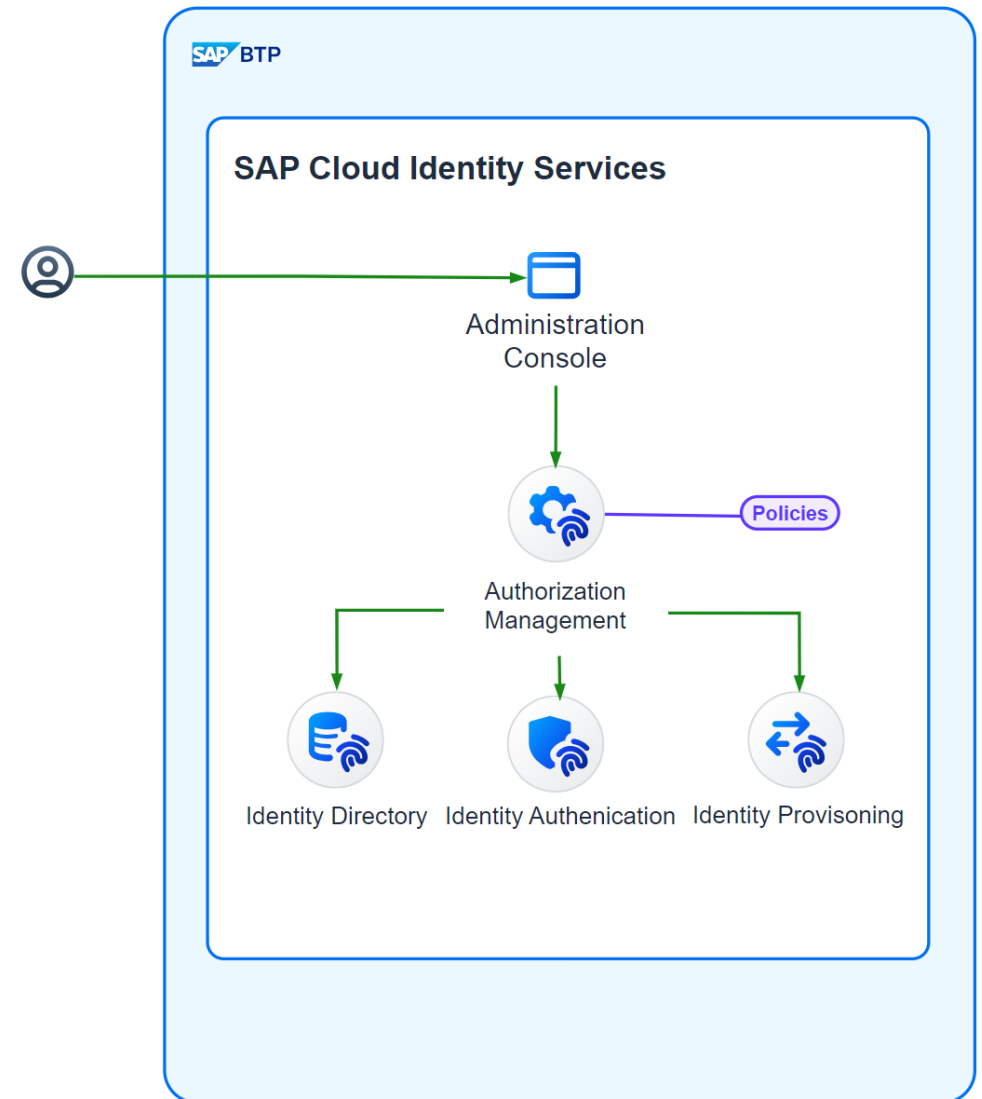
Adjust administrative access to the SAP Cloud Identity console with flexible, policy-based authorizations

Alternative to the existing, coarse granular authorization configuration

Access to user records can be granted on attribute level

Filters can be applied to give access to e.g. specific set of users

Administrative access can be managed via the standard identity lifecycle management processes



SAP Cloud Identity Services – Identity lifecycle with SAP SuccessFactors Recommended Approach

SAP SuccessFactors acts as **source** for **employee** data.

SAP Fieldglass acts as **source** for **contingent worker** data.

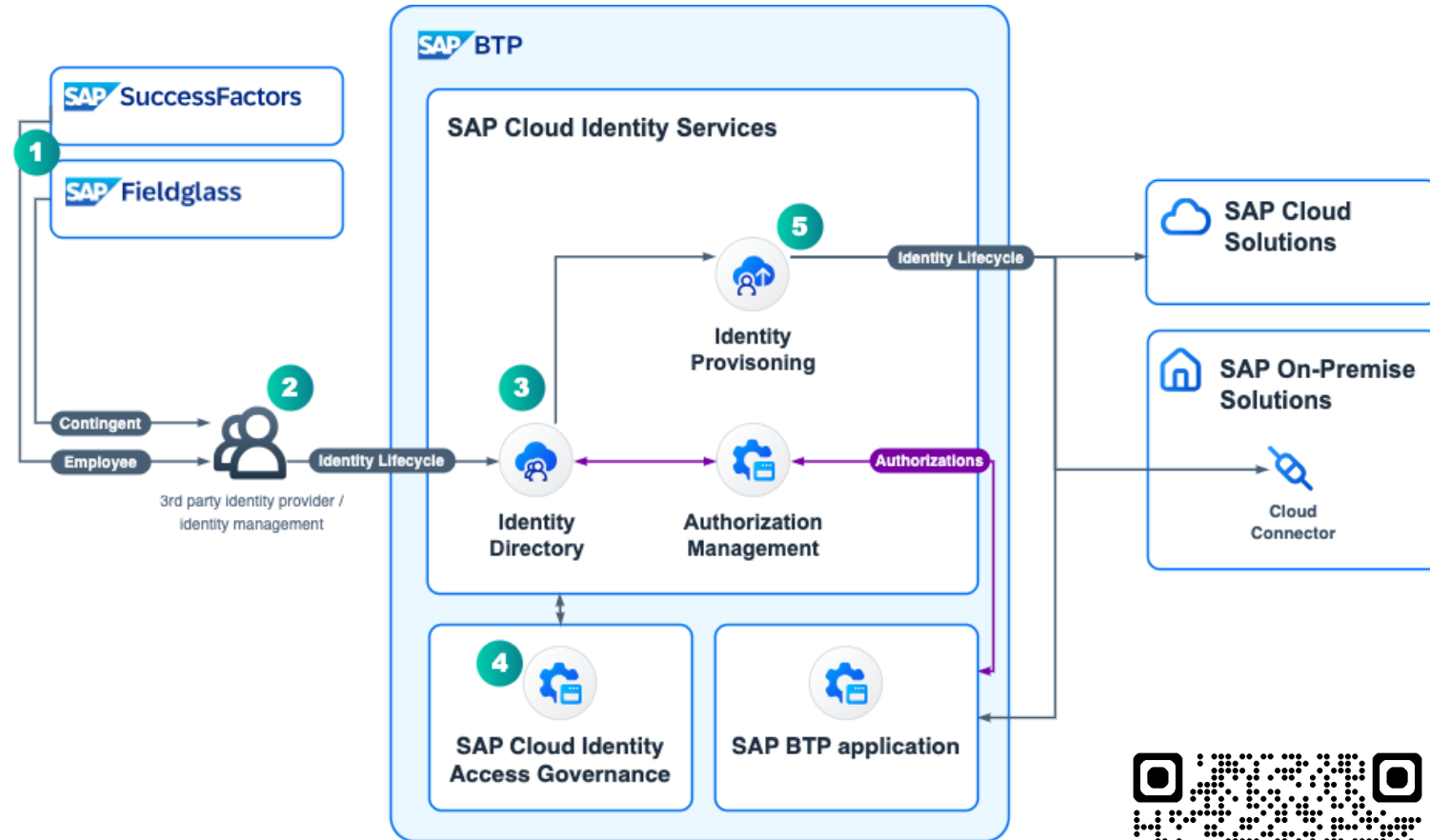
Identity Management solution derives **identity** from **workforce**.

SAP Cloud Identity Services **receive** the (customer specific) derived **identity** and act as a **single integration point** for **identity access management**.

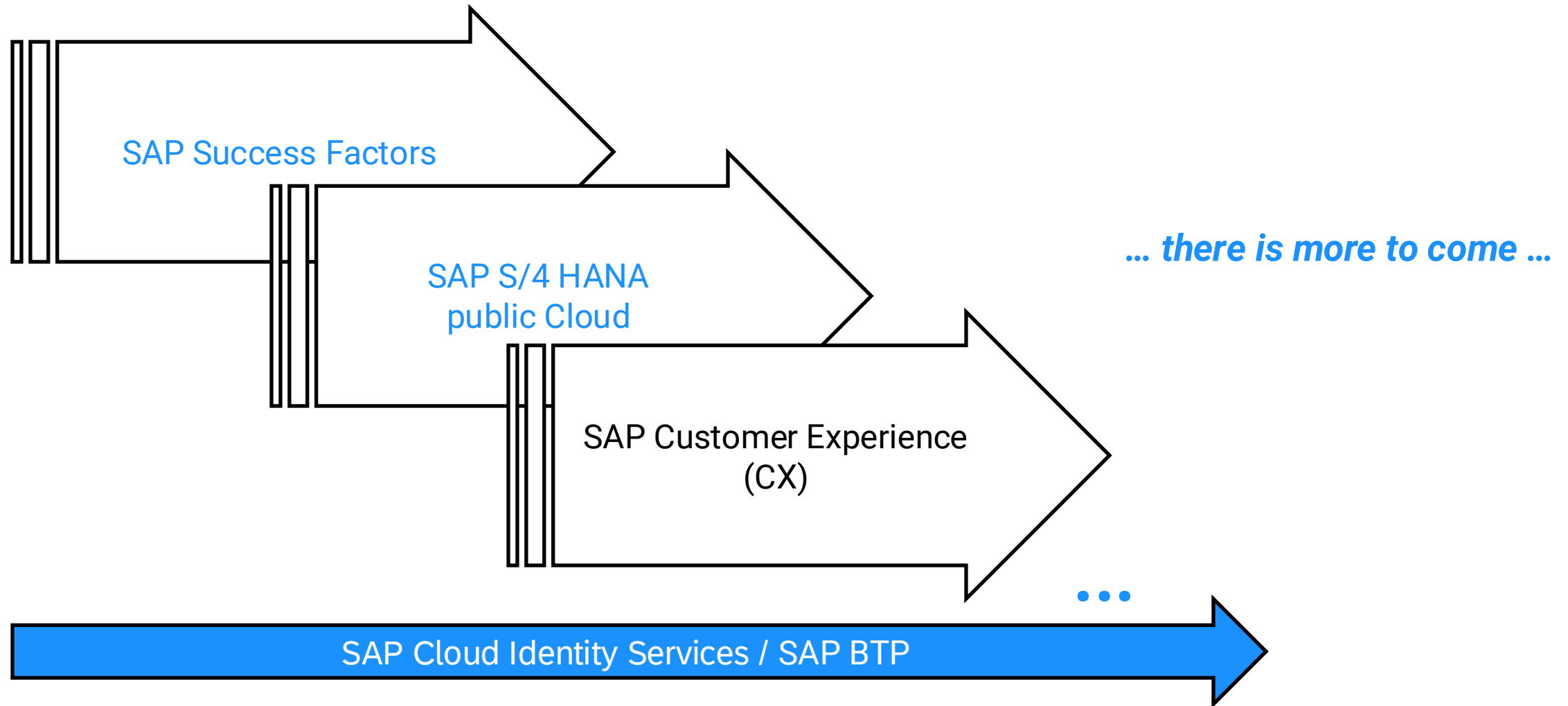
SAP Cloud Identity Services – **Identity Directory** and **Identity Provisioning** act as store and replication tool.

SAP Authorization Management Service manages **policies** for **new BTP apps**.

SAP Cloud Identity Access Governance offers additional risk & access governance features.

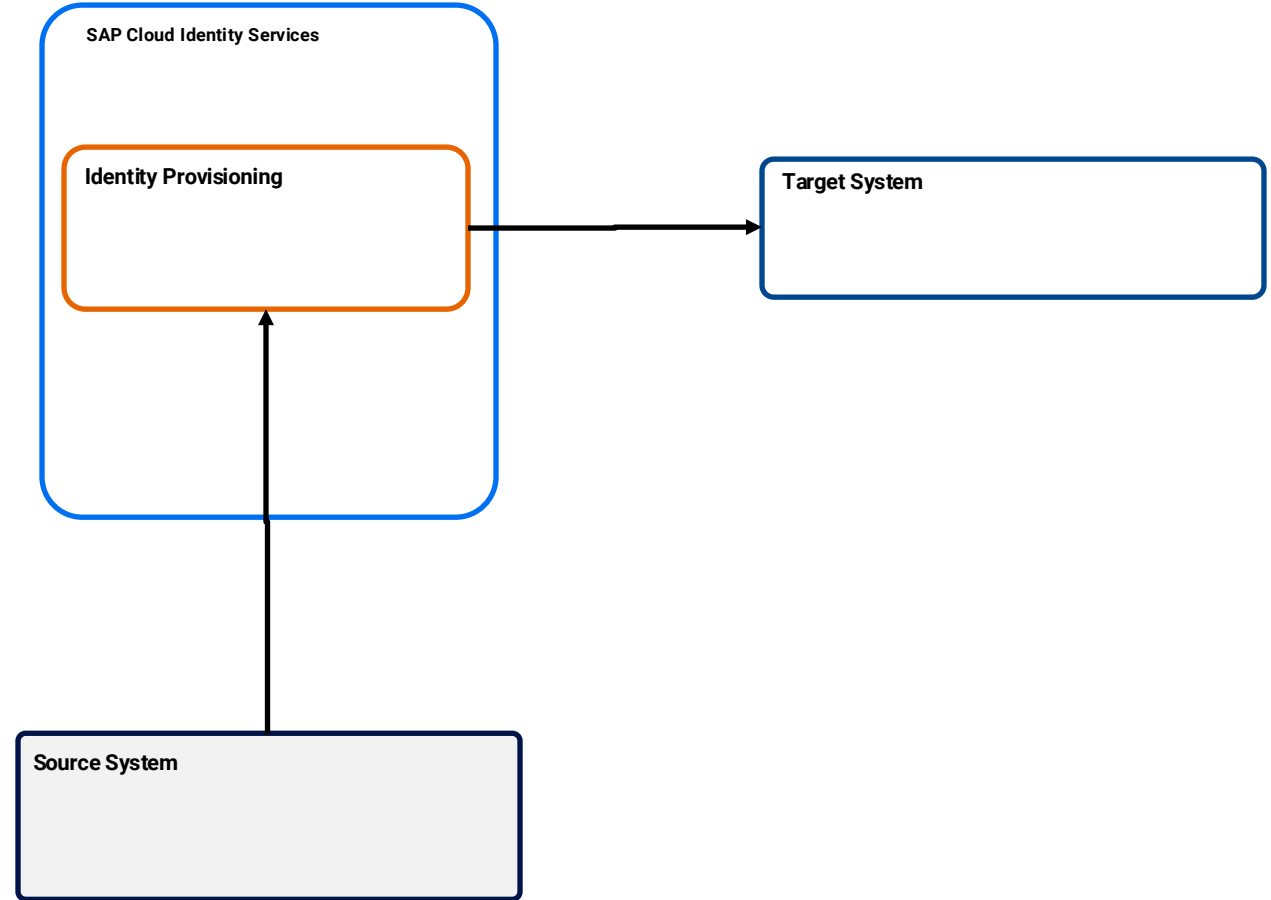


Security Configurations of SAP Cloud Solutions @ SAP Cloud ALM



SAP Cloud Identity Services - Identity Provisioning Lifecycle Automation With Security

- Use certificate-based authentication
- Enable automatic certificate renewal whenever possible (see next slide)
- Avoid [TrustAll](#) in production
- Use secure protocols
- Use credential properties to hold sensitive information
- Assign multiple administrators



SAP Cloud Identity Services - Identity Provisioning

Lifecycle Automation With Security

Automated certificate renewal in Identity Provisioning Service

- IPS supports automatic renewal of certificates that are used to access a target system
- However, there is a disclaimer:

Automatic RegenerationOFF

The certificate will be automatically regenerated and activated within 14 days prior to its expiration. This option is recommended for systems validating certificates based on their subject and issuer. Systems validating certificates based on fingerprints should not use it as this will cause authentication to fail until the certificate is downloaded and uploaded to the connected system.

Status: ⊗ Disabled

- If a target system pins the certificate, then manual renewal may be required
- Beware of systems that ask you to upload a client certificate. They might be pinning.

Trust, Protocols, Certificates – representation in SAP Cloud ALM

Services / Systems / Configuration Stores of IdentityProvisioning02 / Items of IPS_TARGET_SYSTEM_CONFIG (IdentityProvisioni				
Show deleted		Search	↺	↻
Key	Value	Type of Event	Valid since	
BTP-IPS-0007	NAME = trust_all VALUE = false SECREC_STATUS = COMPLIANT SECREC_INDEX = BTP_IPS_0007			Trust is deliberately established
BTP-IPS-0005	NAME = secure_protocols VALUE = URL = https://i531463-source.acco... SECREC_STATUS = COMPLIANT SECREC_INDEX = BTP_IPS_0005			https is used as protocol for URLs

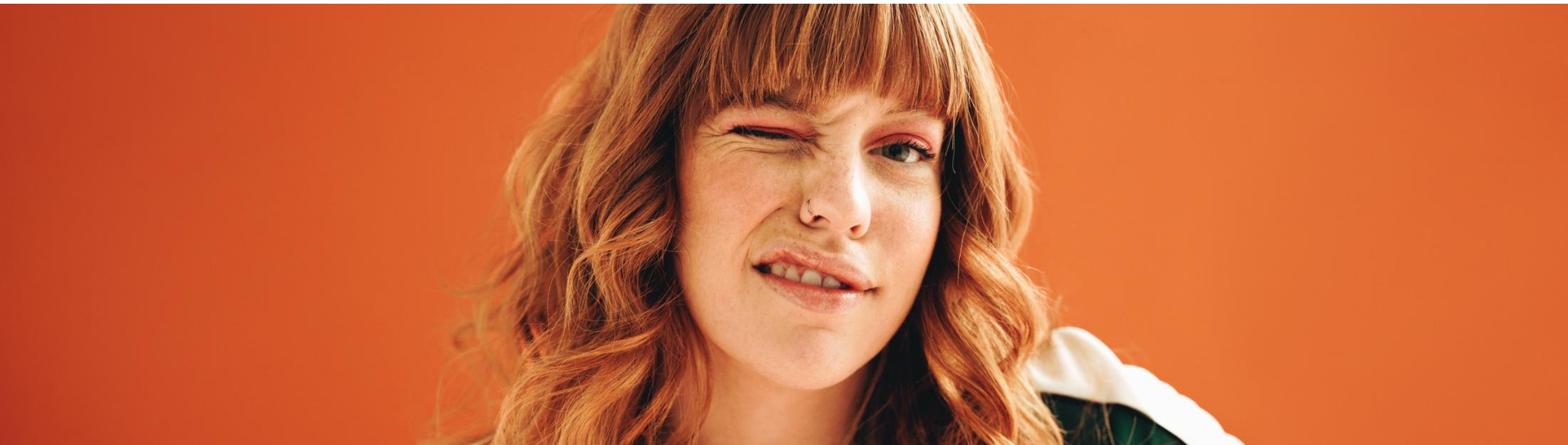
Certificates

... from IAS, IPS: not yet available

High-Priority Scenarios

SAP Business Technology Platform

Services



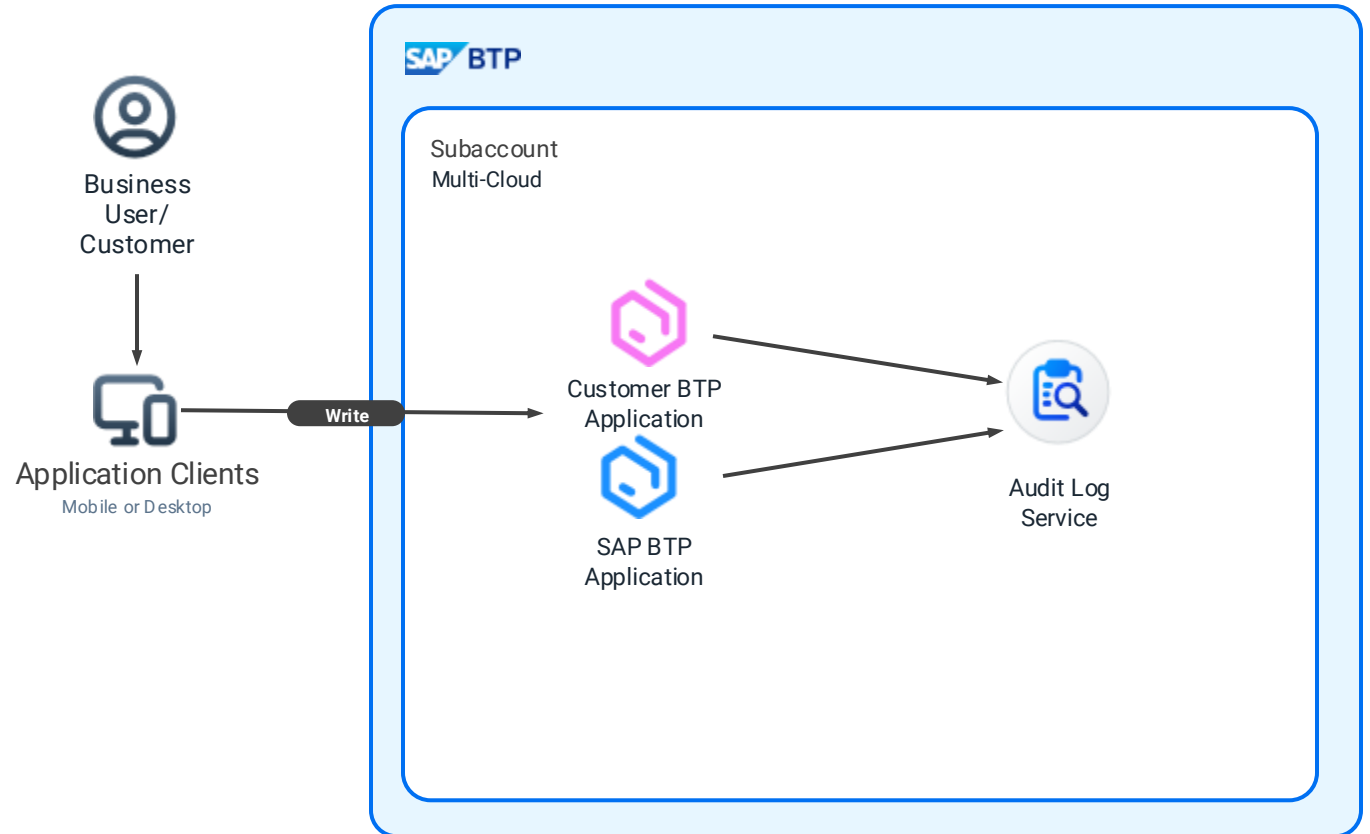
SAP Audit Log service

Customer can review security-relevant activities in the audit log with

- Timestamp
- Terminal ID
- Audit log event

Security-relevant activities include

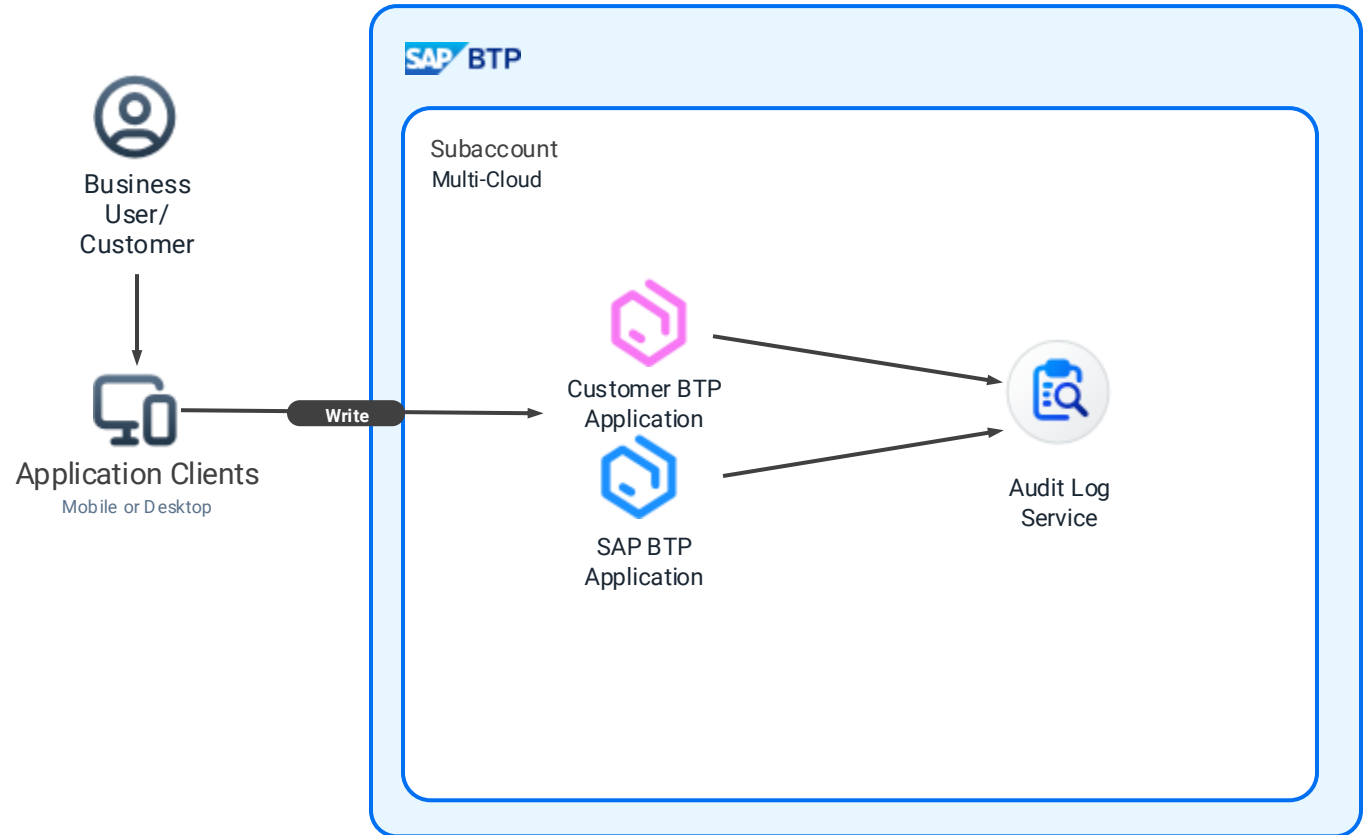
- User logins
- Permission assignments or removals
- Change of trust setups
- Subscription updates
- Change of monitoring checks



Audit Log Service

Evidence for Compliance

- Download and archive logs regularly
- Integrate with central audit log systems
- Use Audit Log APIs for automation
- Monitor retention settings

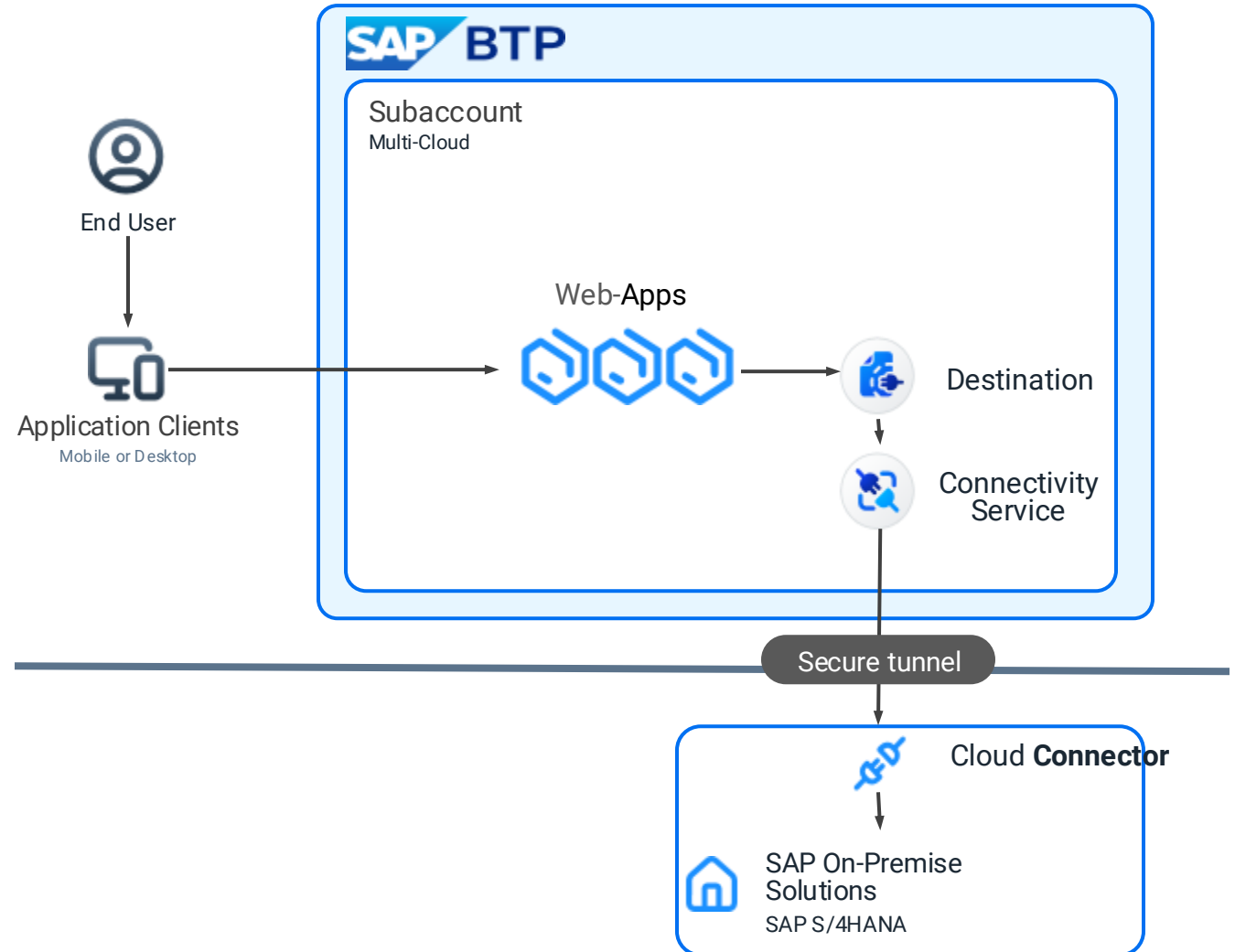


SAP BTP connectivity

SAP Connectivity service lets you establish connectivity between your cloud applications and on-premise systems running in isolated networks.

Features:

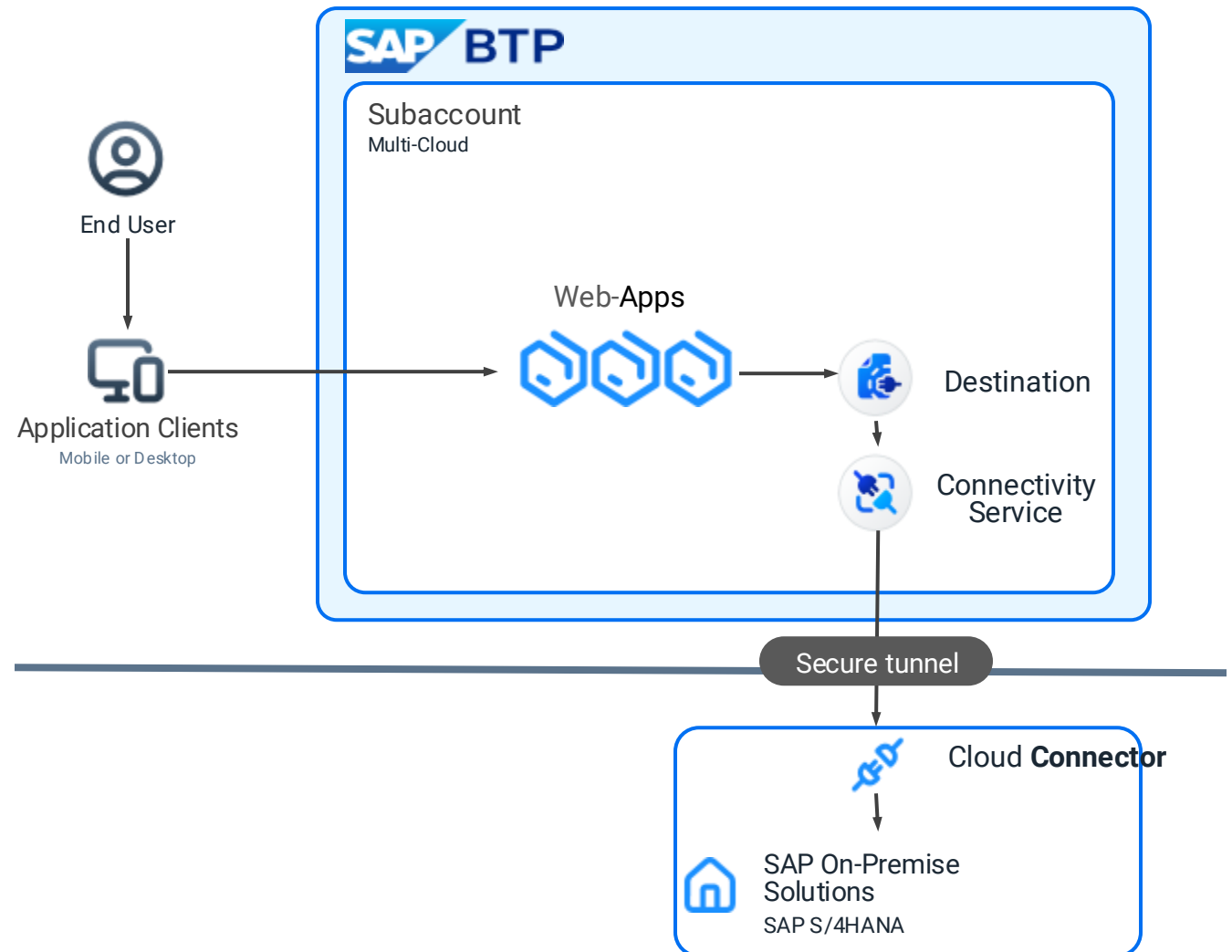
- Access on-premise systems
- Secure tunnel
- Multiple supported protocols
- Access cloud databases via JDBC/ODBC
- Propagate cloud user identity



SAP BTP Connectivity – Destination Service

Secure Your Connections

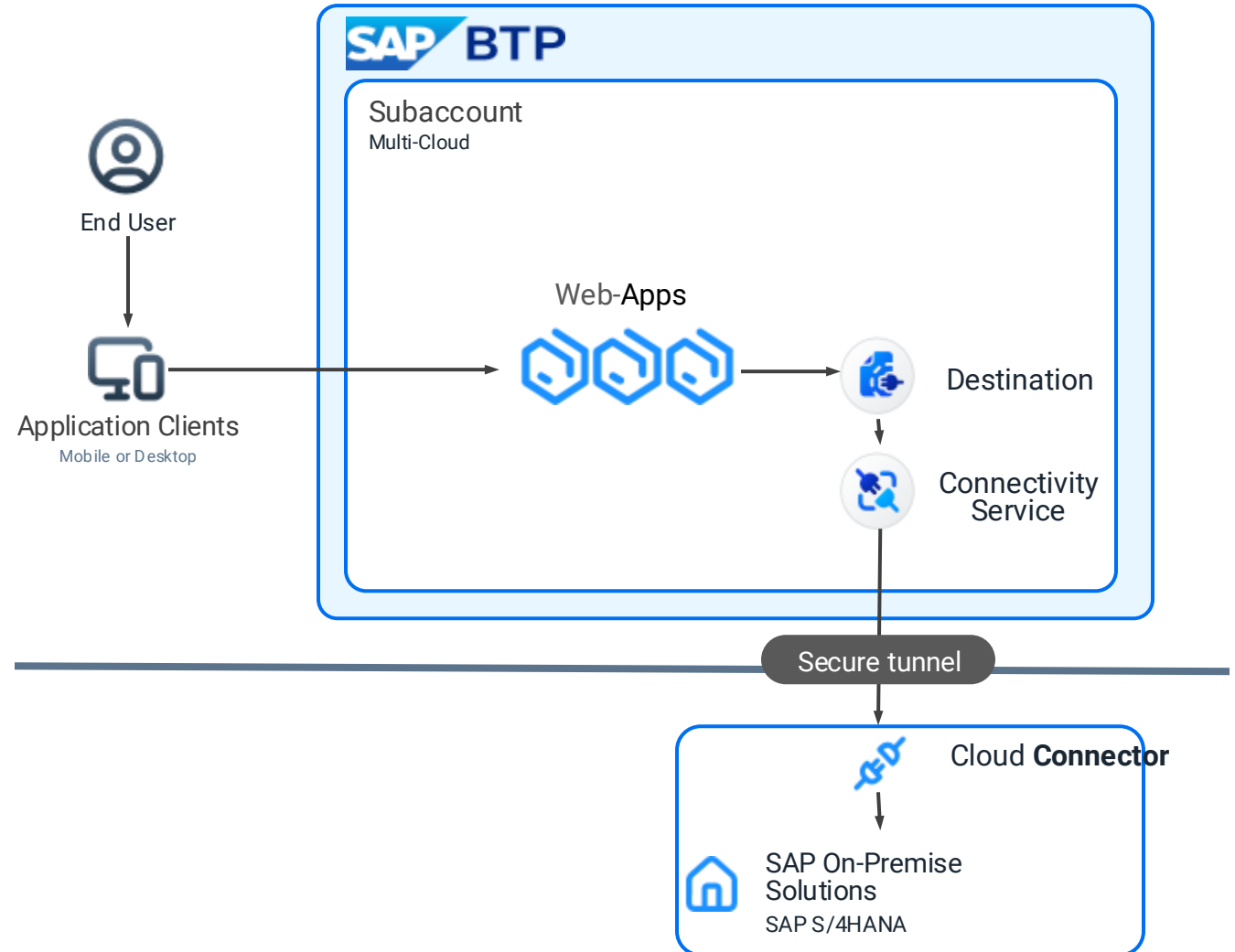
- Use TLS 1.2+ and enable auto-renewal for certs
- Prefer OAuth or SAML over password-based auth
- Avoid deprecated SAP Assertion SSO
- Use mutual TLS in production
- Enable SSO with Principal Propagation
- Validate server certificates



SAP BTP Connectivity – Cloud Connector

Secure The Hybrid Bridge

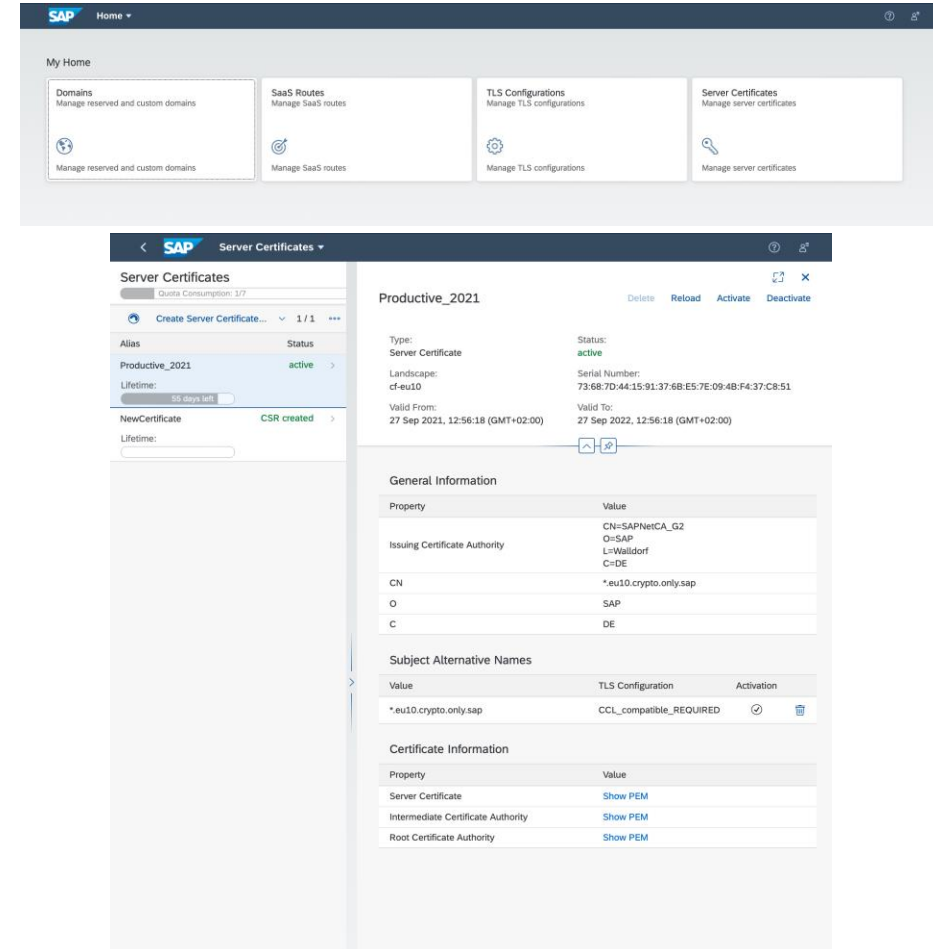
- Enforce HTTPS and monitor exceptions
- Avoid broad sub-paths in URLs
- Use LDAPS and SNC in production
- Limit trusted root CAs and cipher suites
- Replace default admin with LDAP users
- Enable audit logging and trace control



SAP Custom Domain Service

Secure Your Custom Domains

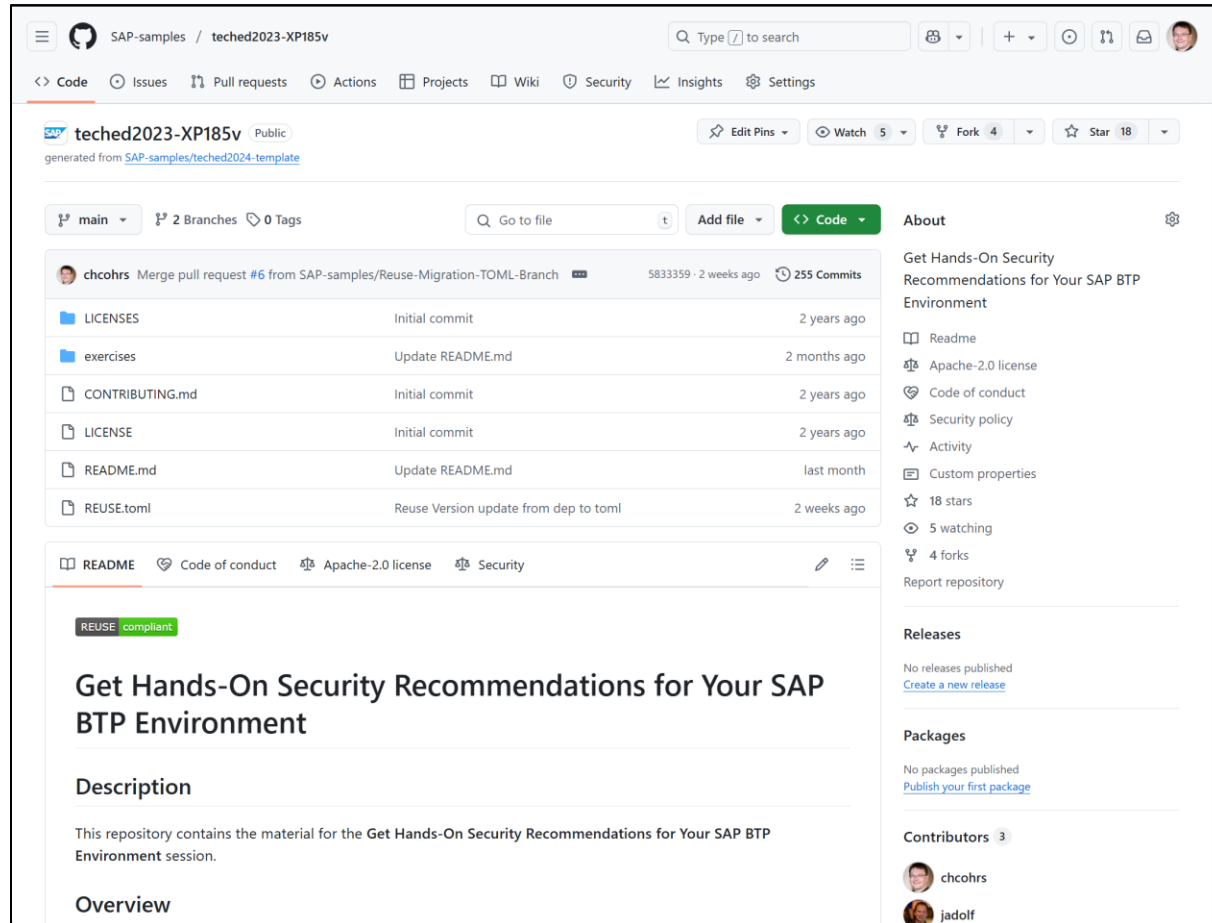
- Assign the Custom Domain Administrator role collection and Space Developer role only to administrators who manage custom domains
- Use the default TLS configurations offered by the Custom Domain Manager. Actively manage use cases that require a different configuration.
- Custom Domain Manager displays certificate expiration warnings long before the expiration date. In addition, certificates are reported to SAP Cloud ALM. Regularly check whether certificates need to be renewed.
- Configure only those Certificate Authority (CA) certificates as trusted for client authentication that are really needed. Do not add all the well-known CAs just to avoid configuration maintenance efforts.



Learning opportunities



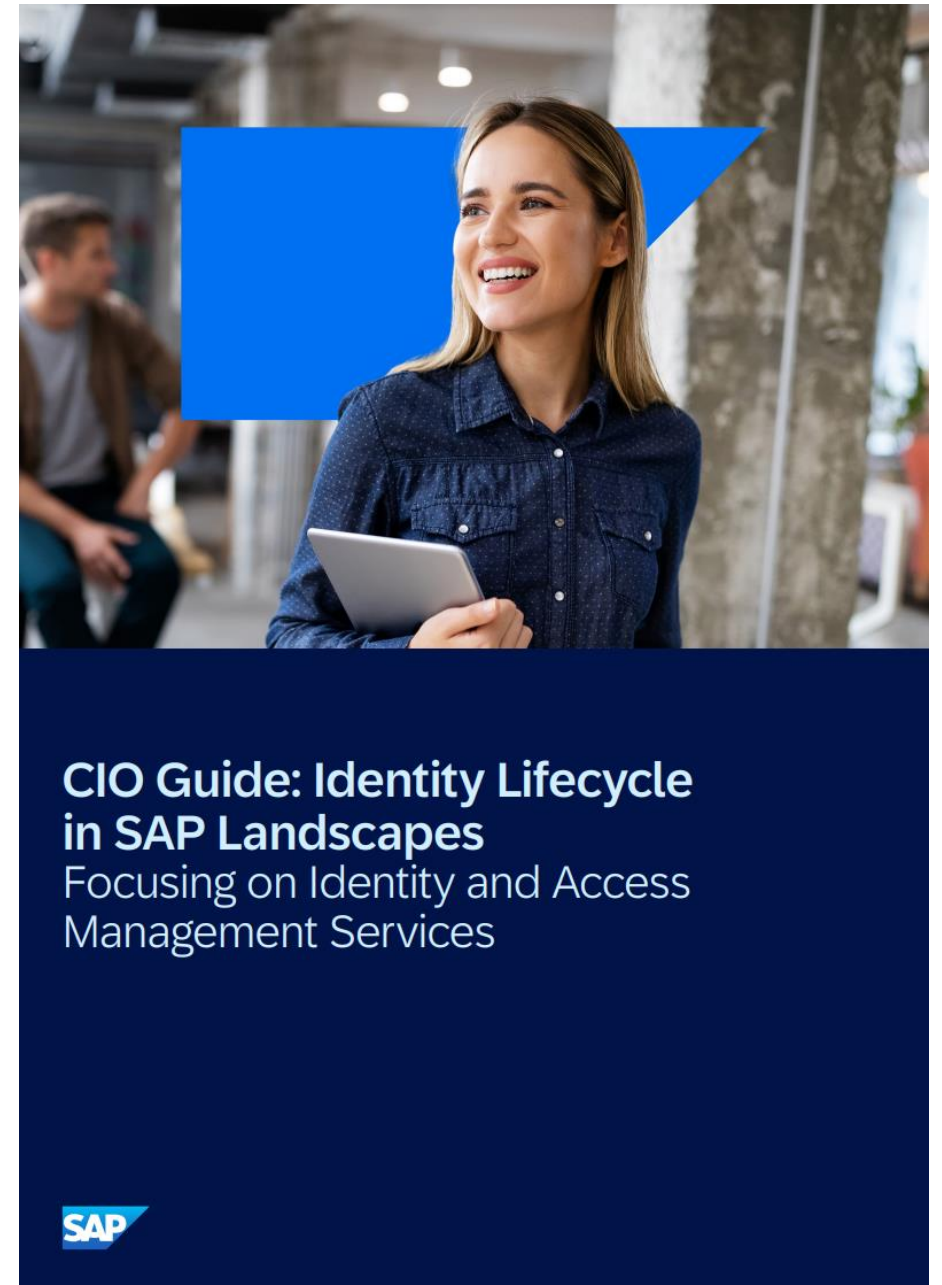
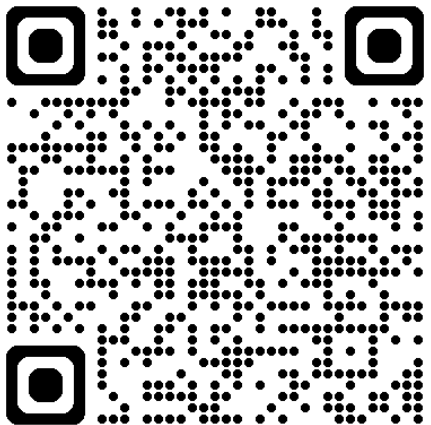
SAP BTP Security Recommendations Hands-On



<https://github.com/SAP-samples/teched2023-XP185v/tree/main>

SAP Strategy: The CIO Guide

See the updated “**CIO Guide: Identity Lifecycle in SAP Landscapes**” that covers IAM scenarios, IAM software from SAP, and the reference architectures



Further information

SAP Cloud Identity Services

- [Services Documentation](#)
- [Best Practices for SAP BTP: Onboard to SAP Cloud Identity Services](#)
- [Community](#)
- [Roadmap](#)
- [Submitting Improvement Requests](#)

IAM Strategy

- [SAP Discovery Center – Reference Architecture](#)
- [CIO Guide: Identity Lifecycle in SAP Landscapes](#)

[Subscribe to our monthly security newsletter](#)



Further information

SAP Help Portal

[SAP BTP documentation including security](#)

SAP Community

[SAP Business Technology Platform Security](#)

Secure software development

[The Secure Software Development Lifecycle at SAP](#)

Shared responsibility

[Shared Responsibility Model Between You and SAP](#)

SAP Trust Center

[SAP Compliance Offerings – Explore Certificates, Reports, and Attestations](#)

SAP Road Map Explorer

[SAP BTP Security Road Map](#)

Security related customer content

[Cloud Services: Reference Guide](#)

[Guide to Customer Content](#)



Thank you.

Contact information:

Christian Cohrs

christian.cohrs@sap.com

<https://www.linkedin.com/in/christian-cohrs>

Jürgen Adolf

juergen.adolf@sap.com

Hendrik Müller

hendrik.mueller@sap.com