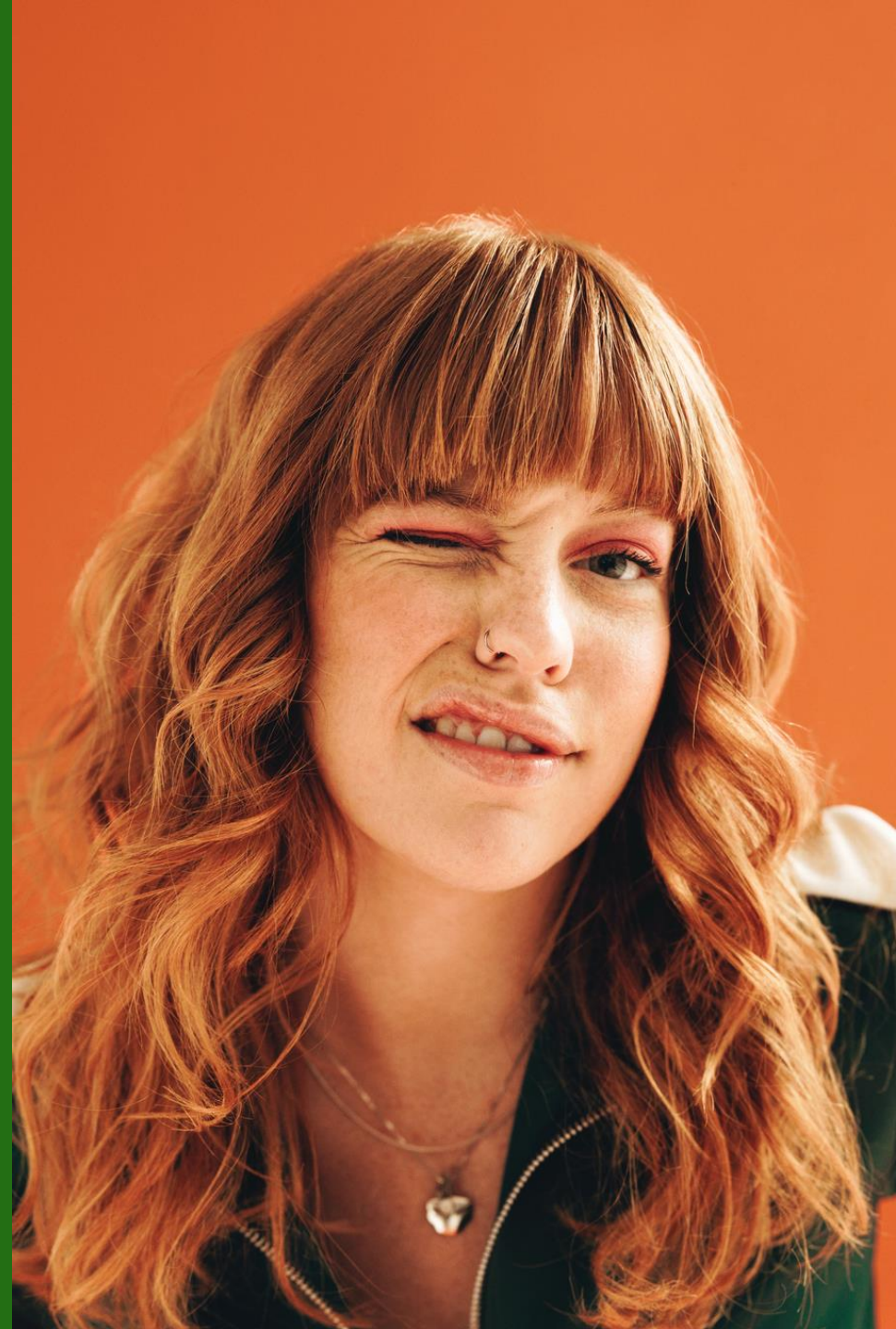
Day 2 Operations

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

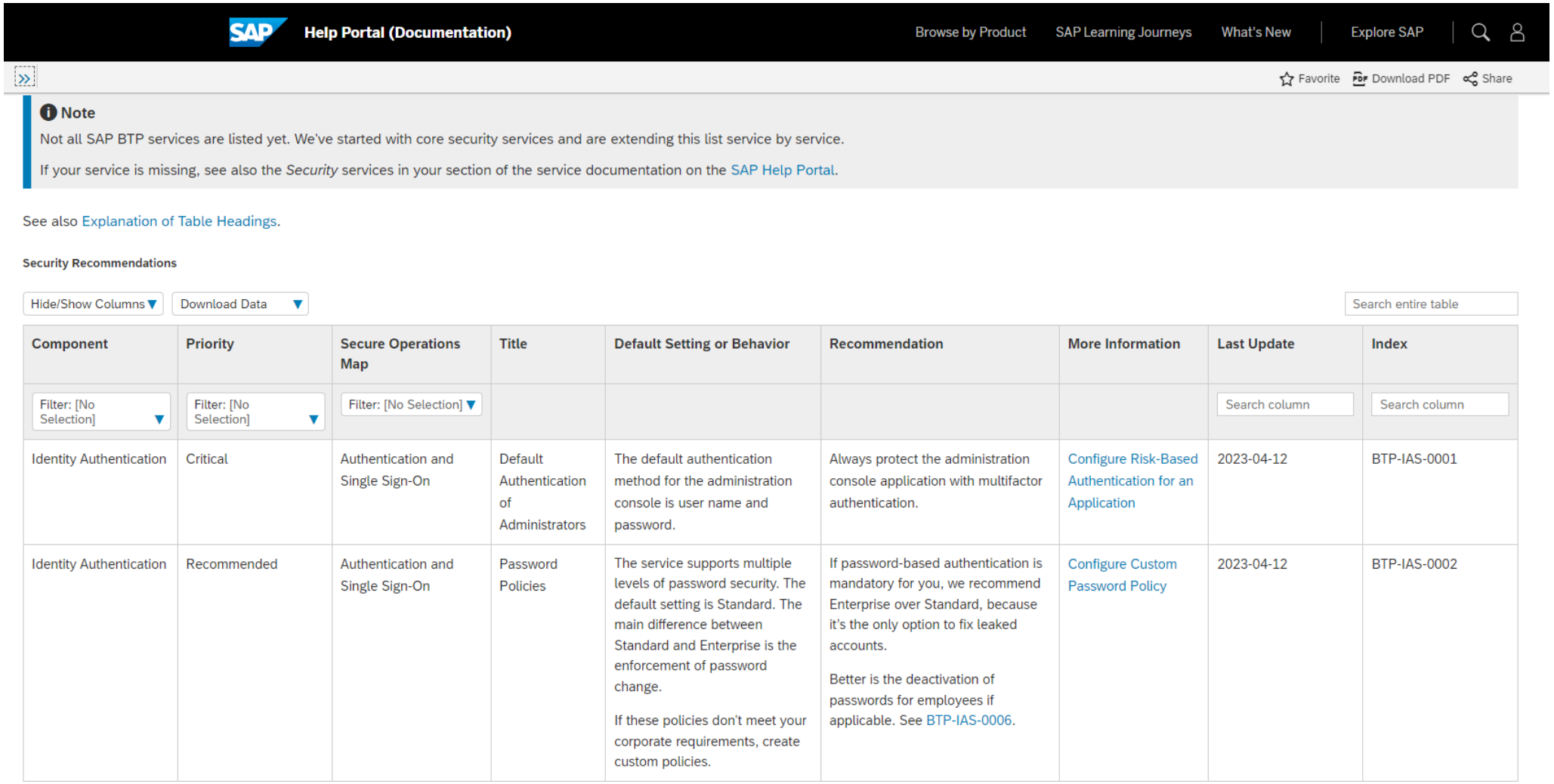
Monitoring Security Recommendations in SAP Cloud ALM

Recommendations for high-priority scenarios

Additional learning resources

Introduction to the SAP BTP Security Recommendations

SAP BTP Security Recommendations



SAP 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.

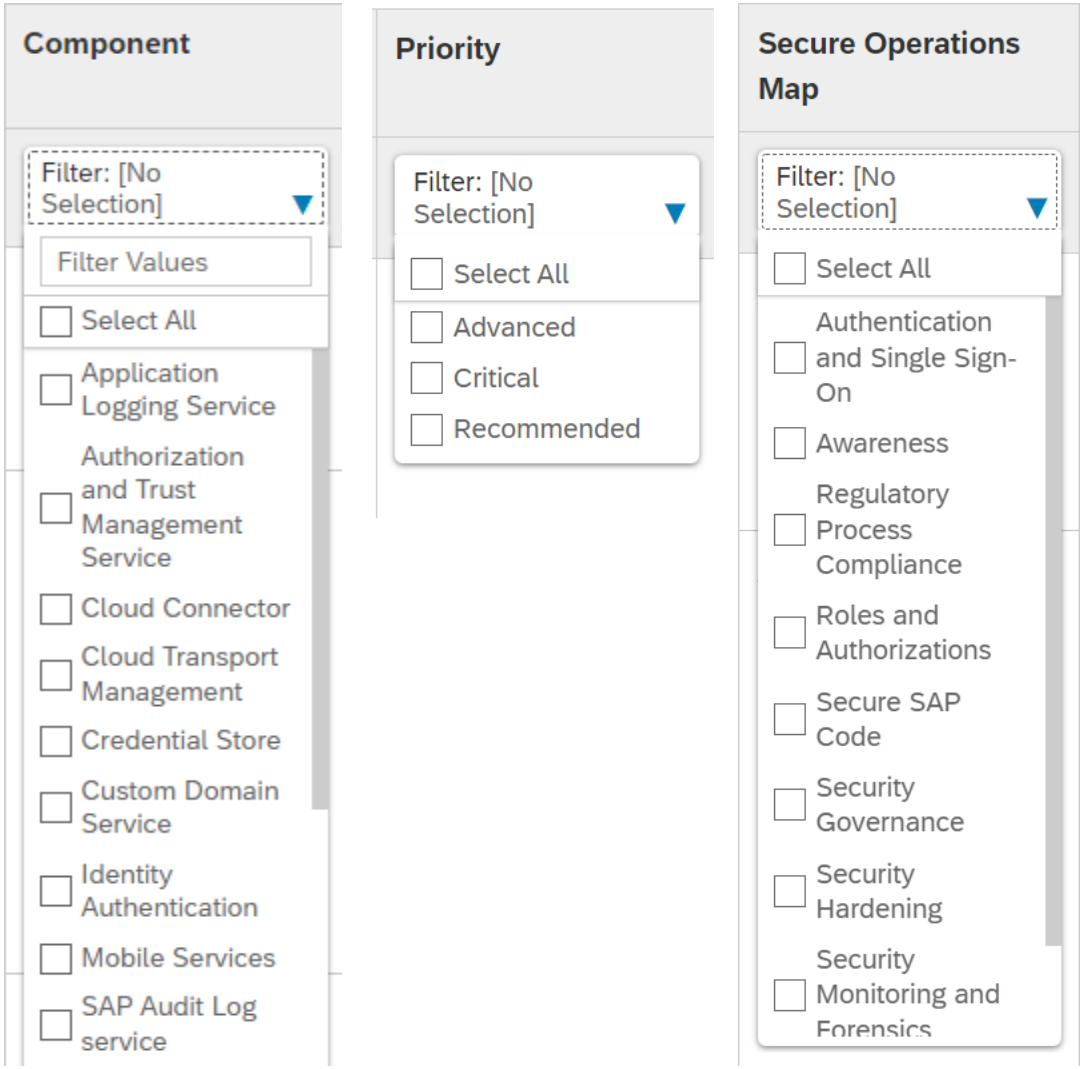
Security Recommendations

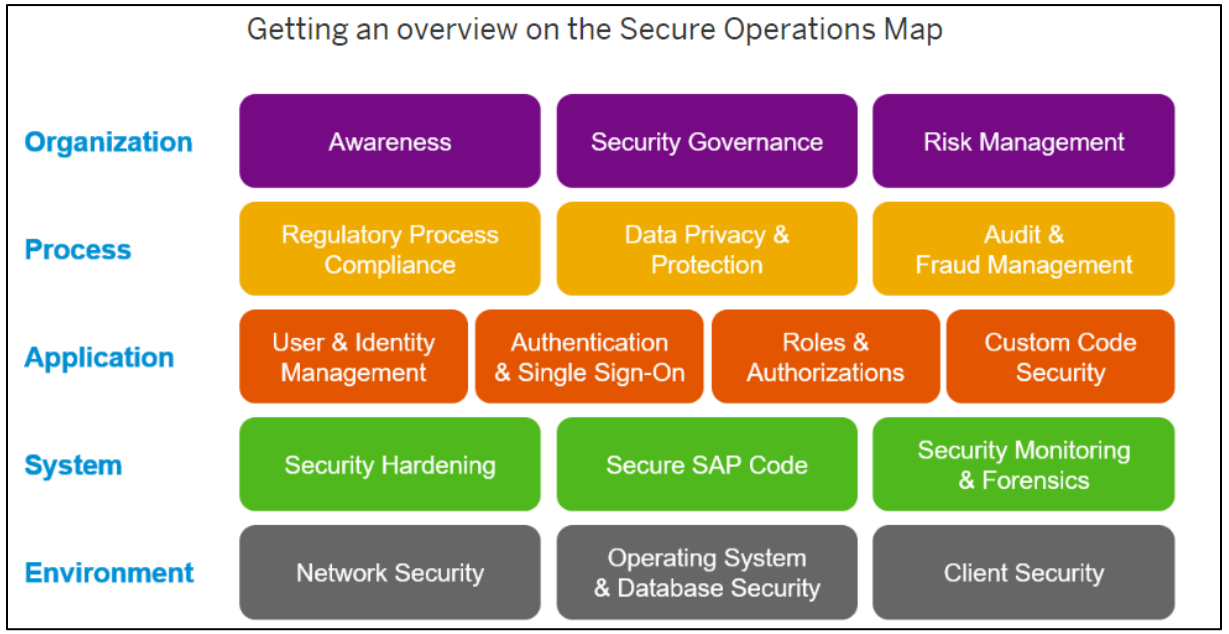
Hide/Show Columns ▼ | Download Data ▼ | Search entire table

Component	Priority	Secure Operations Map	Title	Default Setting or Behavior	Recommendation	More Information	Last Update	Index
Filter: [No Selection] ▼	Filter: [No Selection] ▼	Filter: [No Selection] ▼					Search column	Search column
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 | SAP Help Portal

SAP BTP Security Recommendations - Structure

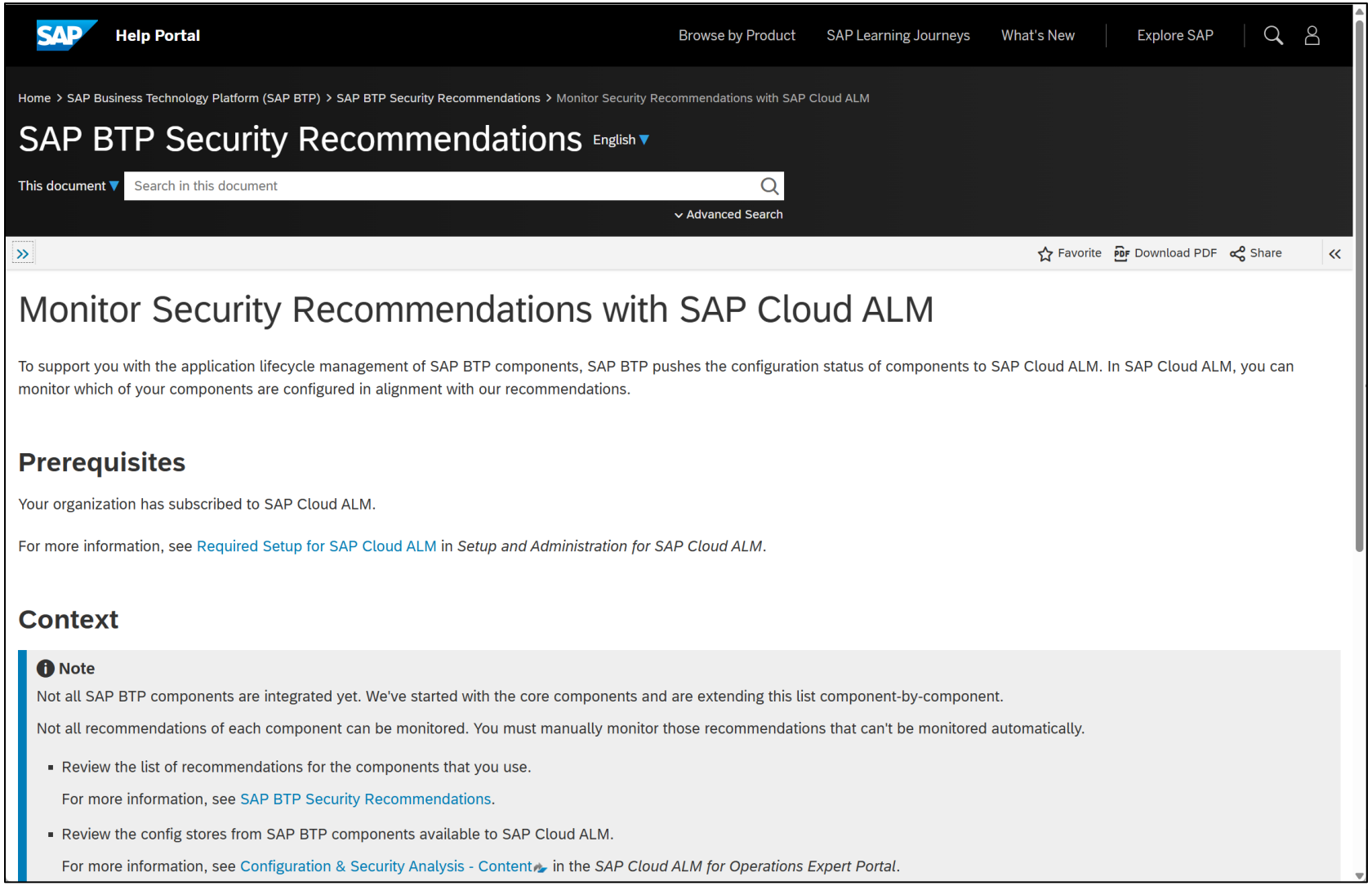




Secure Operations Map

Monitoring Security Recommendations in SAP Cloud ALM

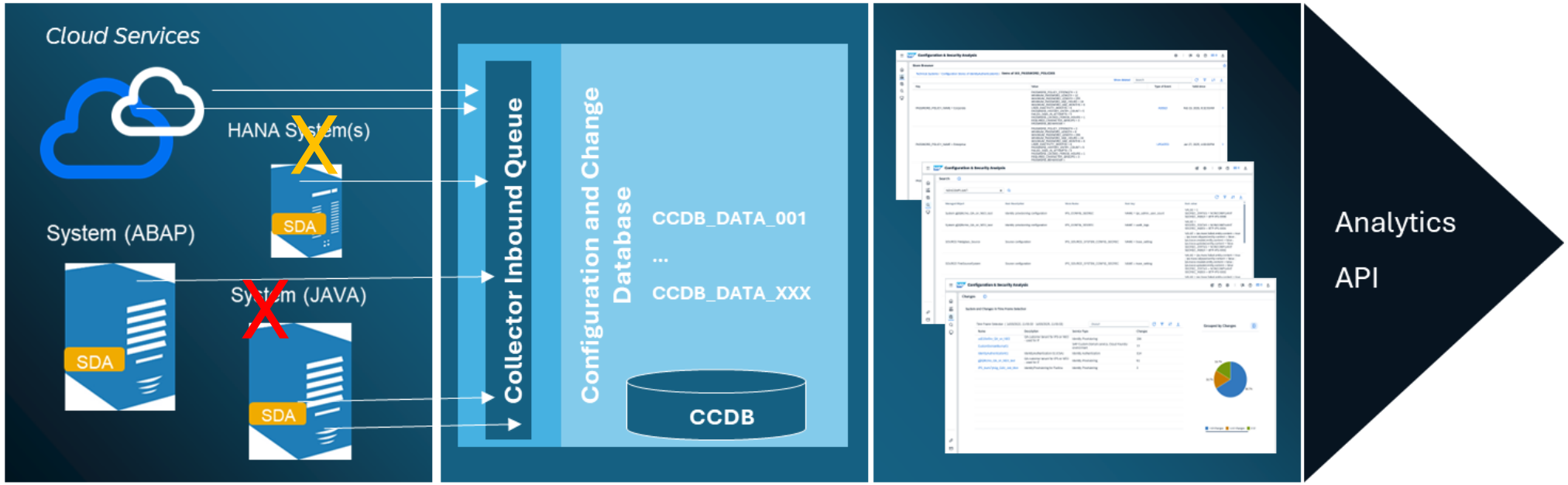
SAP BTP Security Recommendations - in SAP Cloud ALM



Monitor Security Recommendations with SAP Cloud ALM

SAP Cloud ALM – Configurations- & Security Analysis

From Data to Dashboards



Daily Snapshot

Configuration Stores & History

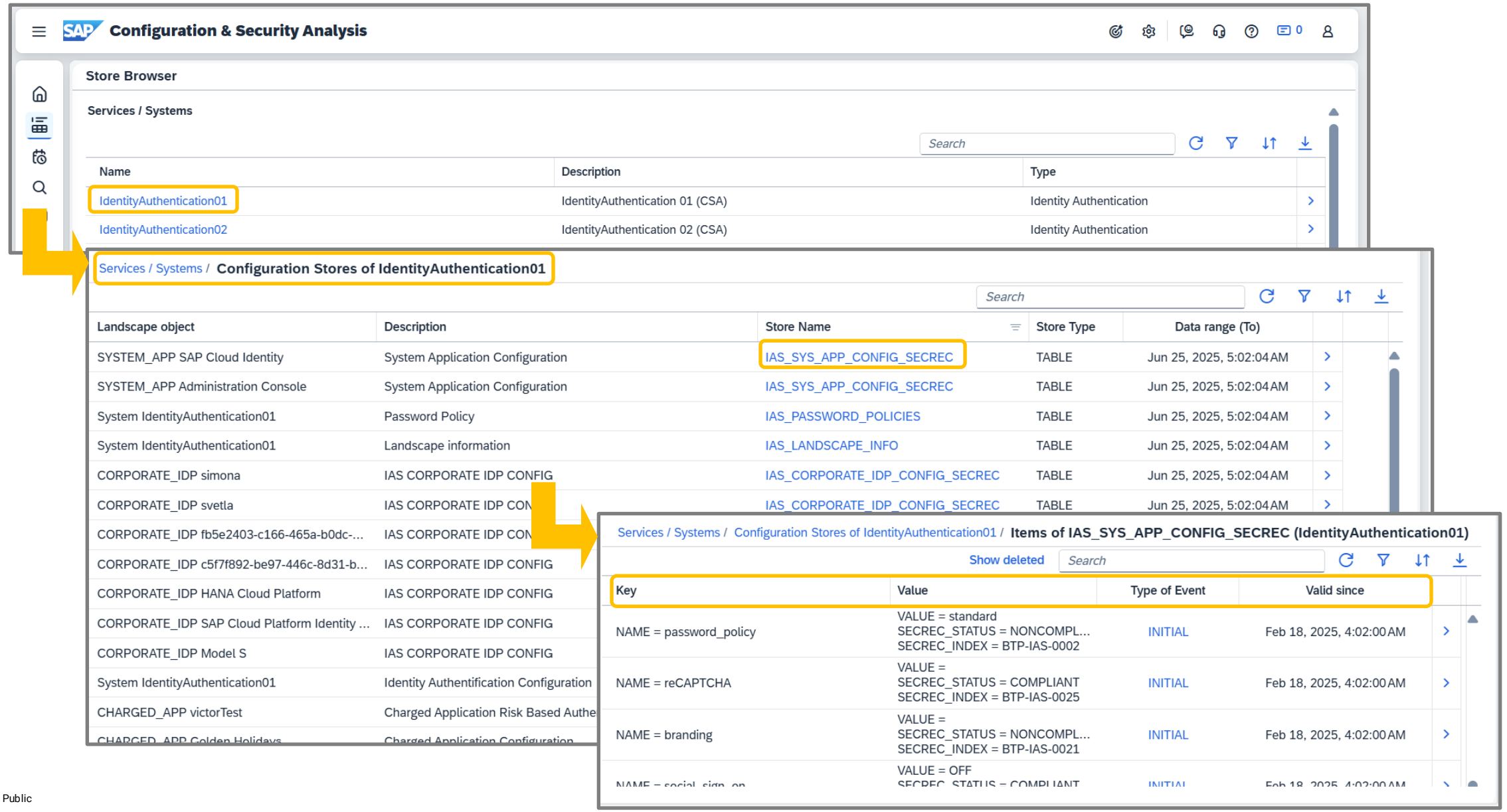
Browse
Search
Change Analysis
Home Screen with Cloud Service Status

Outbound API

SAP Cloud ALM Demo Tenant

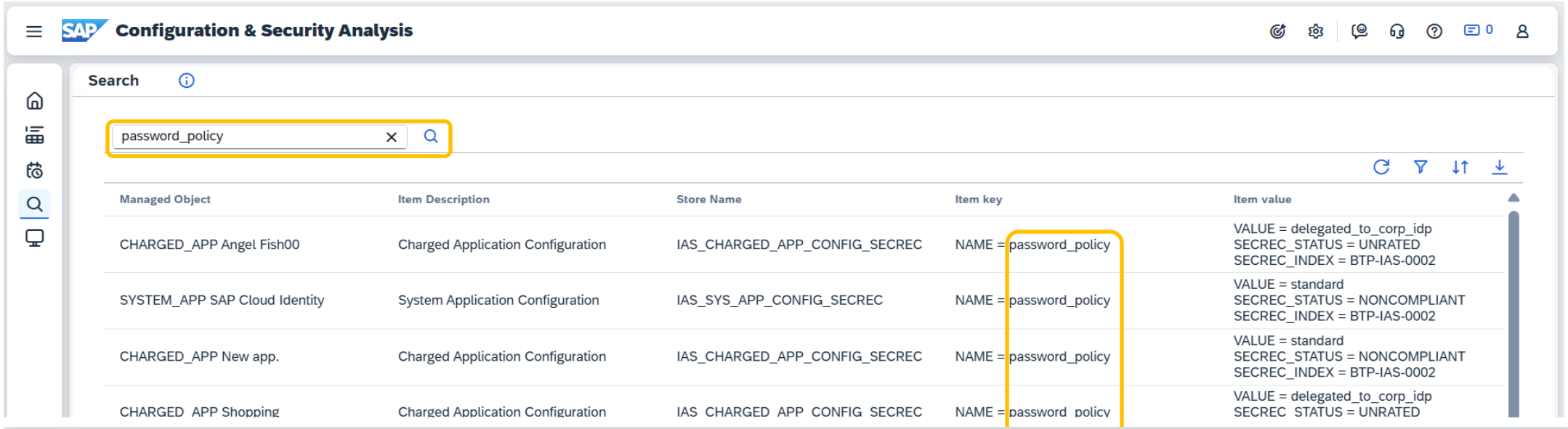
Public

Browse - Example



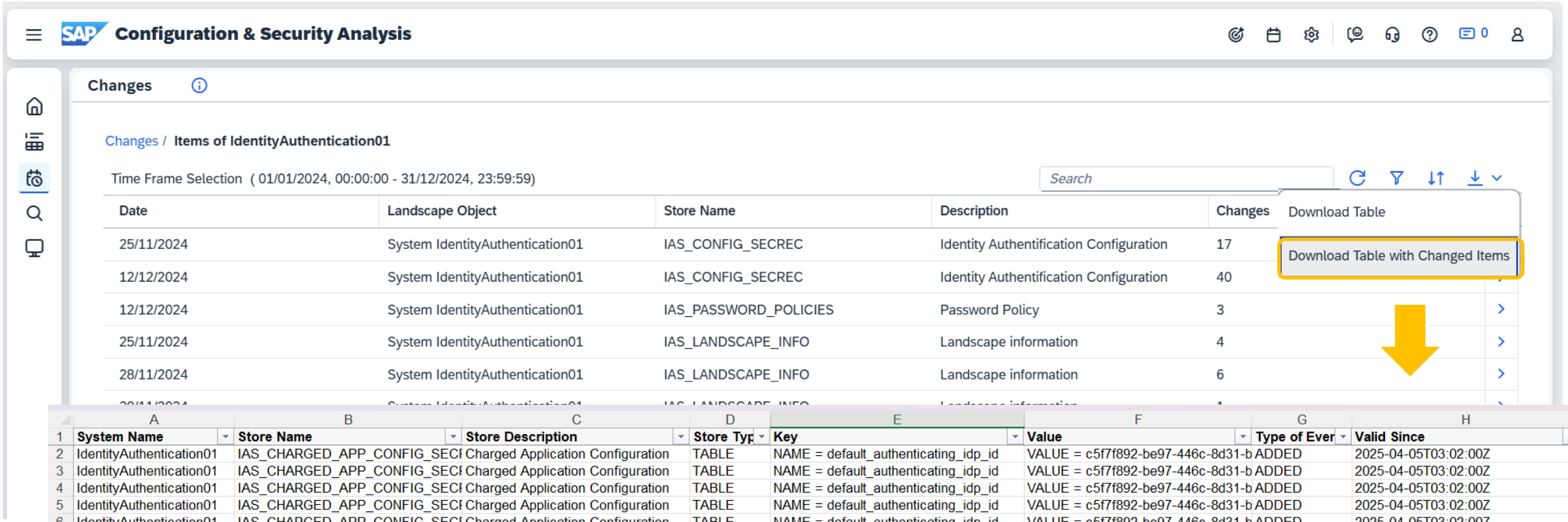
Search – Examples

Example 1.

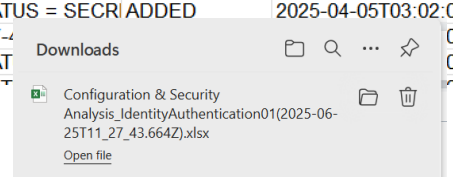


Example 2.

Change Analysis – Example



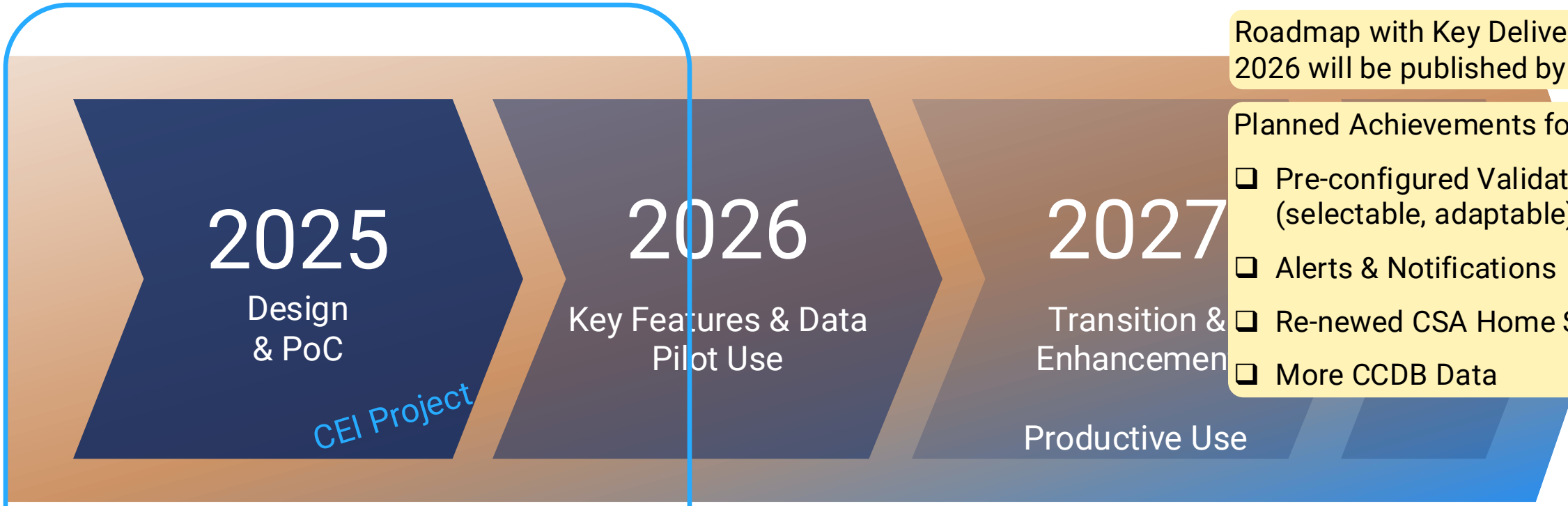
	A	B	C	D	E	F	G	H
1	System Name	Store Name	Store Description	Store Typ	Key	Value	Type of Ever	Valid Since
2	IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SECI	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
3	IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SECI	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
4	IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SECI	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
5	IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SECI	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
6	IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SECI	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
7	IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SECI	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
8	IdentityAuthentication01	IAS_BUNDLED_APP_CONFIG_SECF	Bundled Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
9	IdentityAuthentication01	IAS_BUNDLED_APP_CONFIG_SECF	Bundled Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
10	IdentityAuthentication01	IAS_BUNDLED_APP_CONFIG_SECF	Bundled Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
11	IdentityAuthentication01	IAS_SYS_APP_CONFIG_SECREC	System Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-446c-8d31-b	ADDED	2025-04-05T03:02:00Z
12	IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SECI	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = b638b739-2eac-46aa-a9b6-	ADDED	2025-04-05T03:02:00Z
13	IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SECI	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = SECREC_STATUS = SECR	ADDED	2025-04-05T03:02:00Z
14	IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SECI	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = SECREC_STATUS = SECR	ADDED	2025-04-05T03:02:00Z
15	IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SECI	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = SECREC_STATUS = SECR	ADDED	2025-04-05T03:02:00Z
16	IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SECI	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = SECREC_STATUS = SECR	ADDED	2025-04-05T03:02:00Z
17	IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SECI	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = c5f7f892-be97-		00Z
18	IdentityAuthentication01	IAS_CHARGED_APP_CONFIG_SECI	Charged Application Configuration	TABLE	NAME = default_authenticating_idp_id	VALUE = SECREC_STAT		00Z



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



- **How are you currently working with Config Val (SAP Solution Manager)?**
- **How would you want to work with CSA (SAP Cloud ALM)?**
- Essentials for Transitioning completed and proven by PoC
- Left-overs
- Migration Support
- Feature Enhancement
- Further Evolution

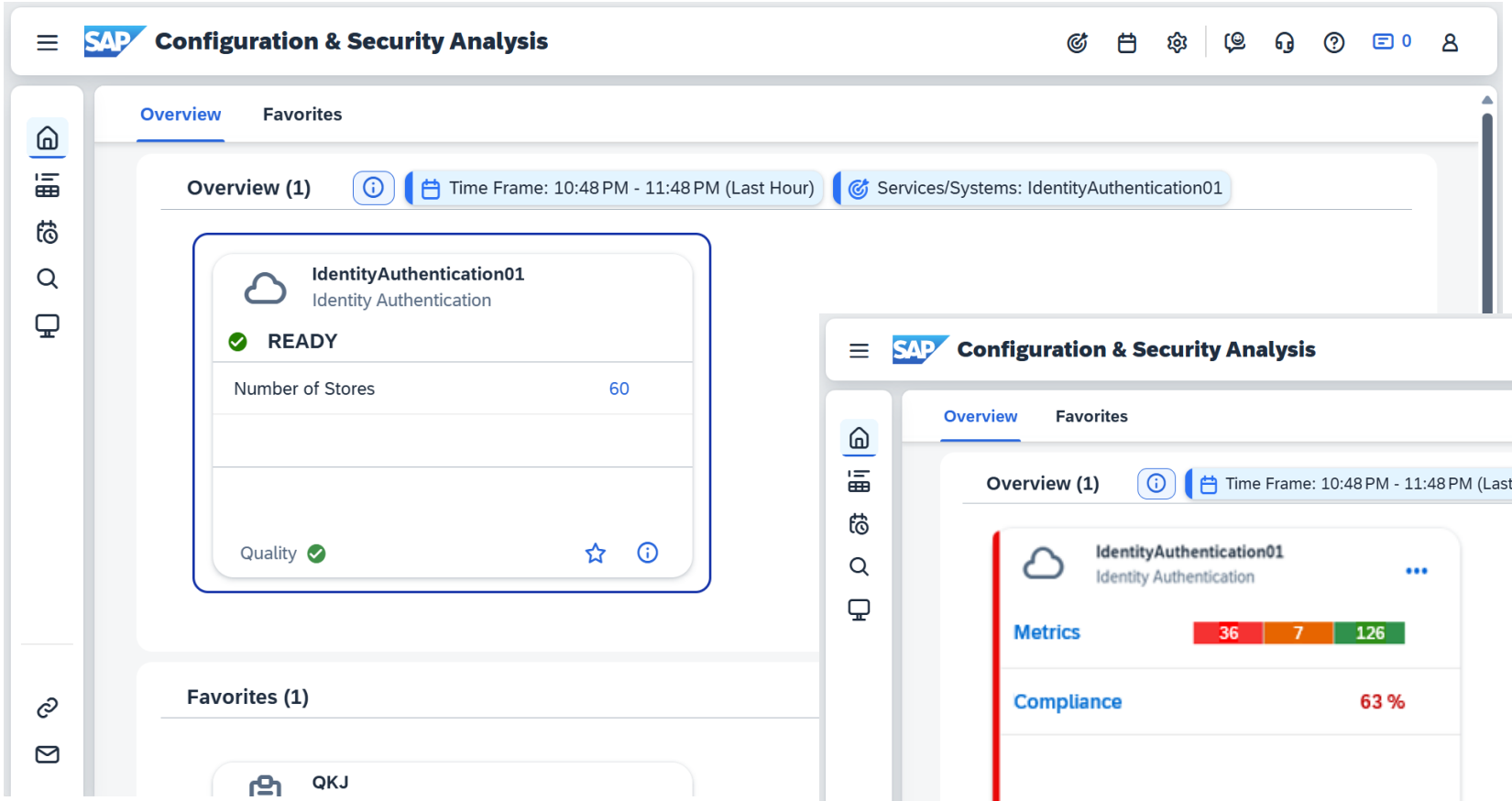
Coming next:
Roadmap with Key Deliverables of 2025 will be published in Q2

Roadmap with Key Deliverables of 2026 will be published by early Q1

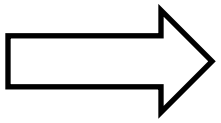
Planned Achievements for 2025

- ❑ Pre-configured Validations (selectable, adaptable)
- ❑ Alerts & Notifications
- ❑ Re-newed CSA Home Screen
- ❑ More CCDB Data

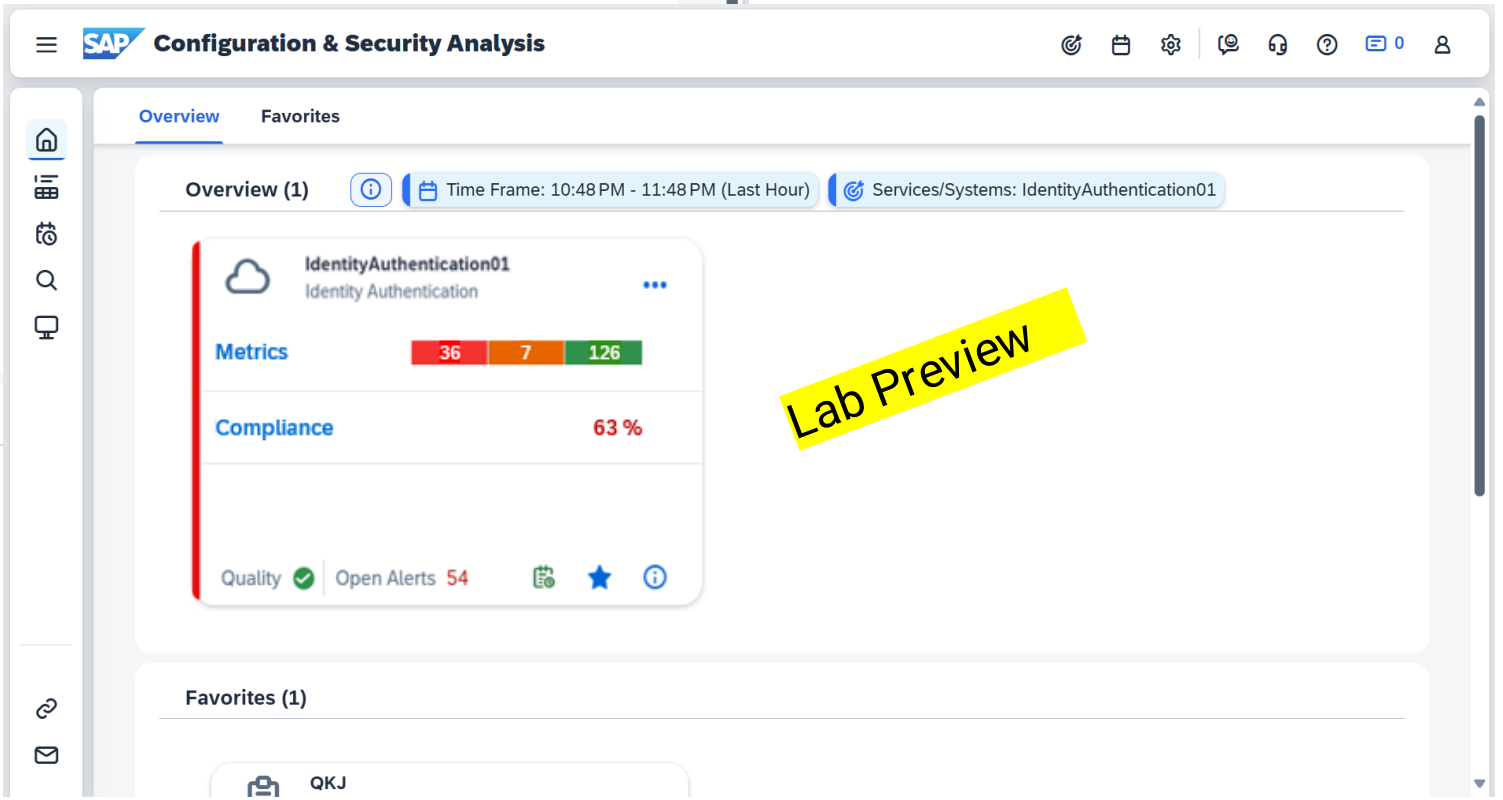
SAP Cloud ALM – Configuration & Security Analysis *new* HOME Screen



Today



Planned



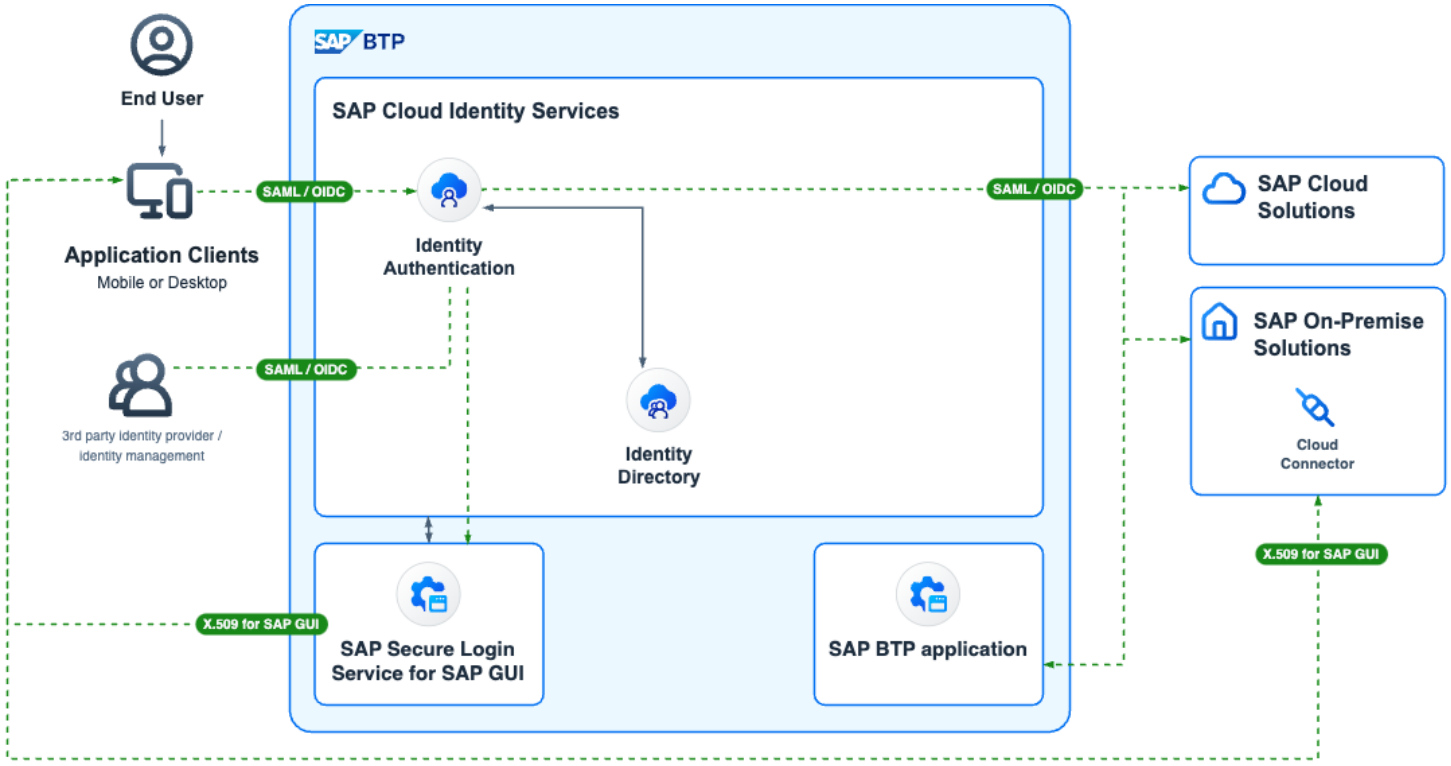
Lab Preview

High-Priority Scenarios
SAP Cloud Identity Services

SAP Cloud Identity Services – Identity Authentication

Identity Authentication

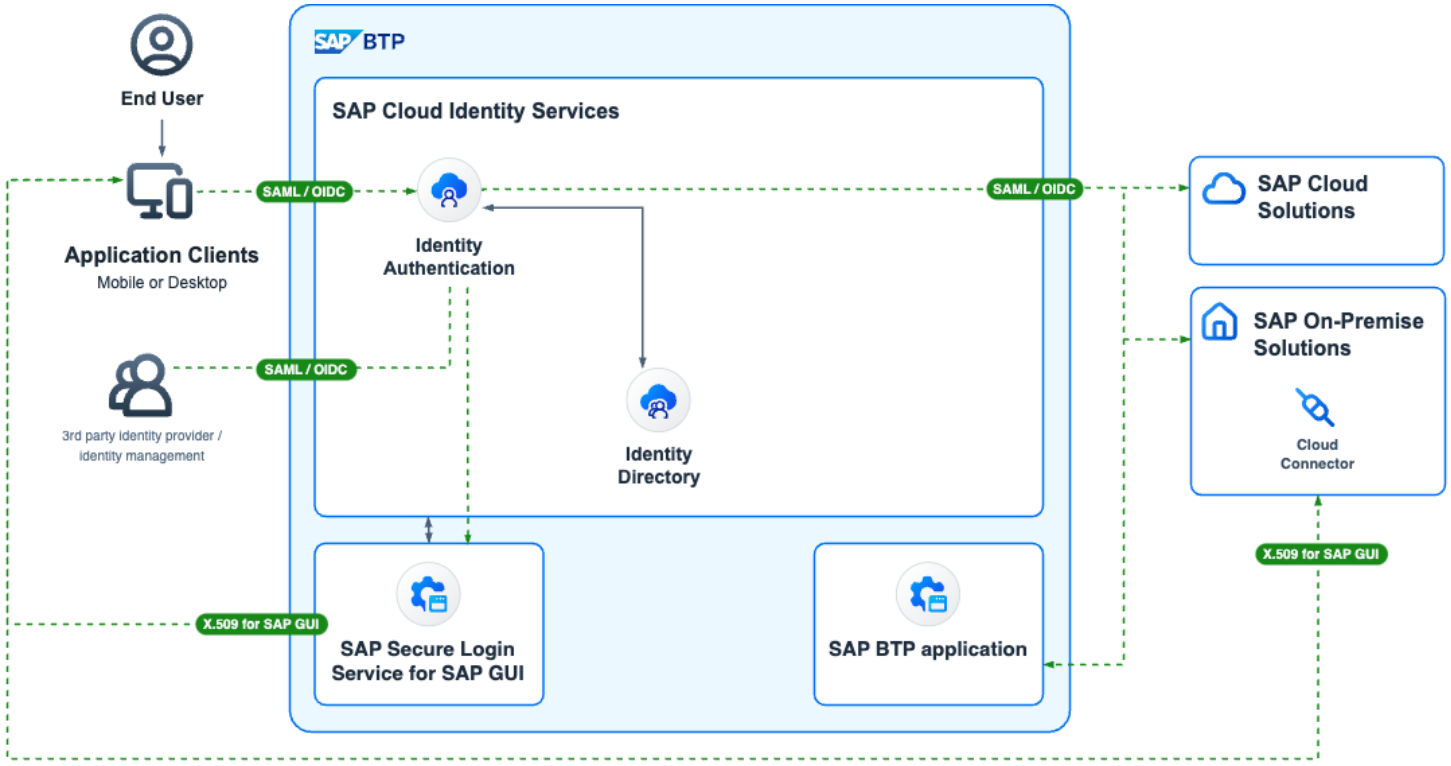
- Identity provider supporting **SAML** or **OpenID Connect**
- SAP's strategic solution for authentication
- **Pre-configured trust** for many SAP cloud applications
- Option to act as **proxy** for a 3rd party Identity Provider



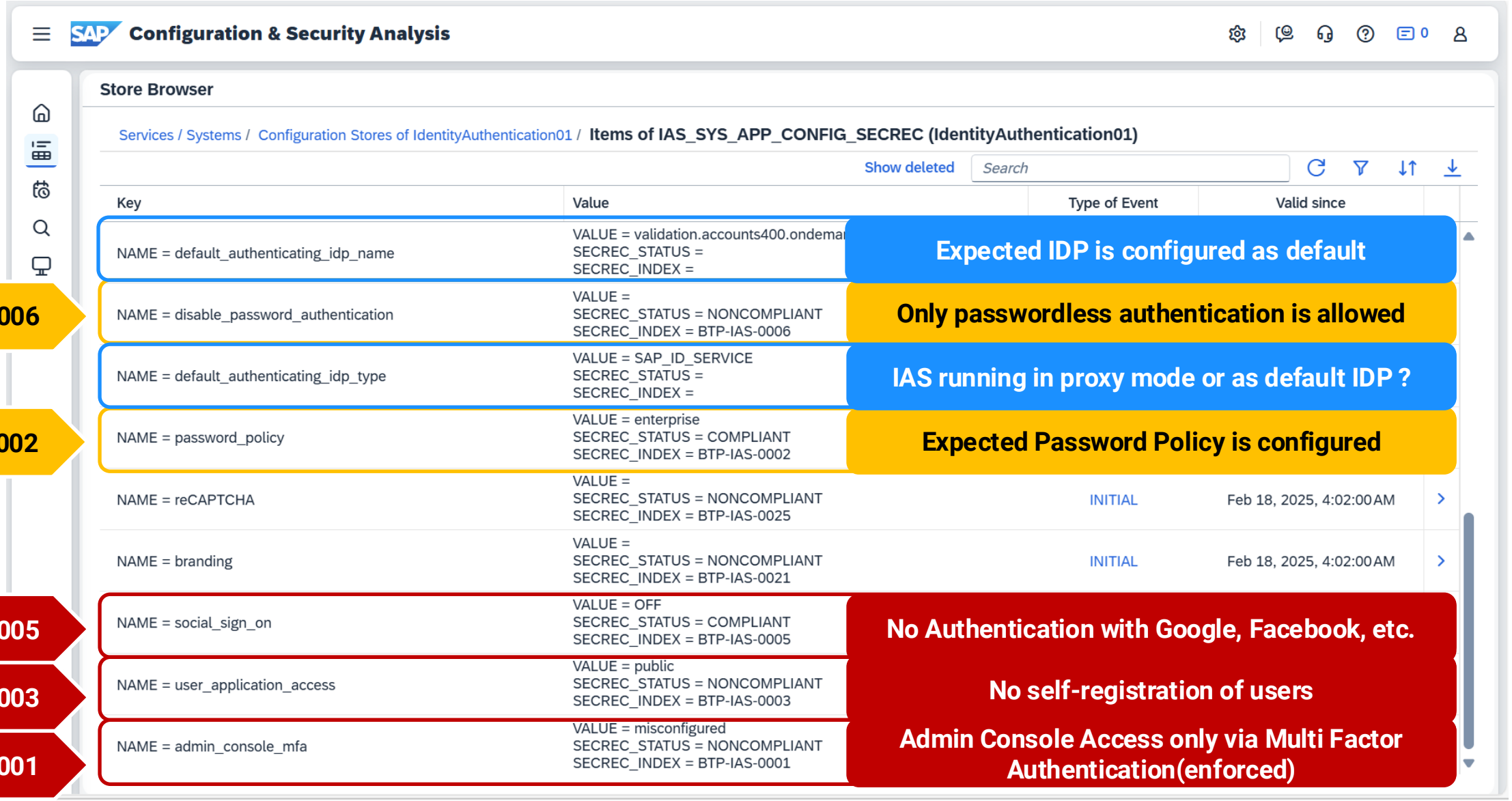
SAP Cloud Identity Services – Identity Authentication

Secure Access Starts Here

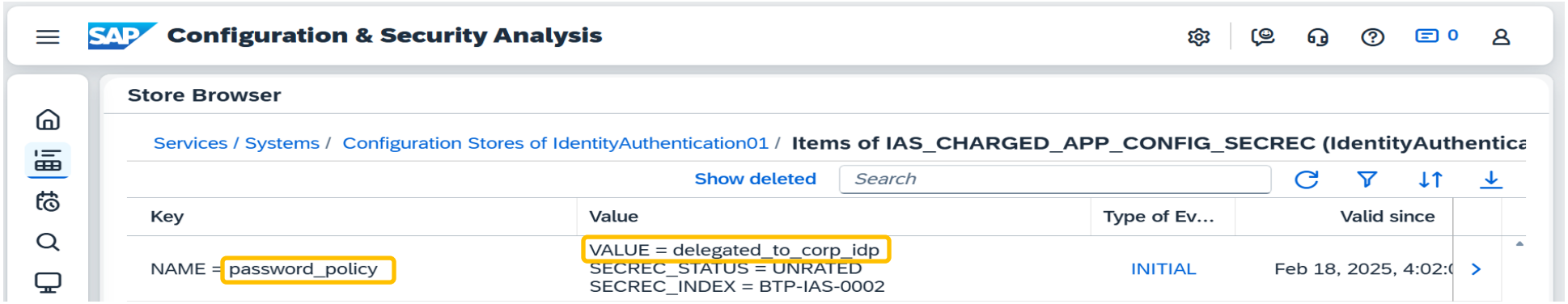
- Enforce MFA for admin console access
- Use passwordless authentication where possible (certificate, FIDO)
- Keep self-registration and social sign-on disabled
- Integrate with an existing corporate identity provider
- Manage trust settings with 3rd-party identity providers

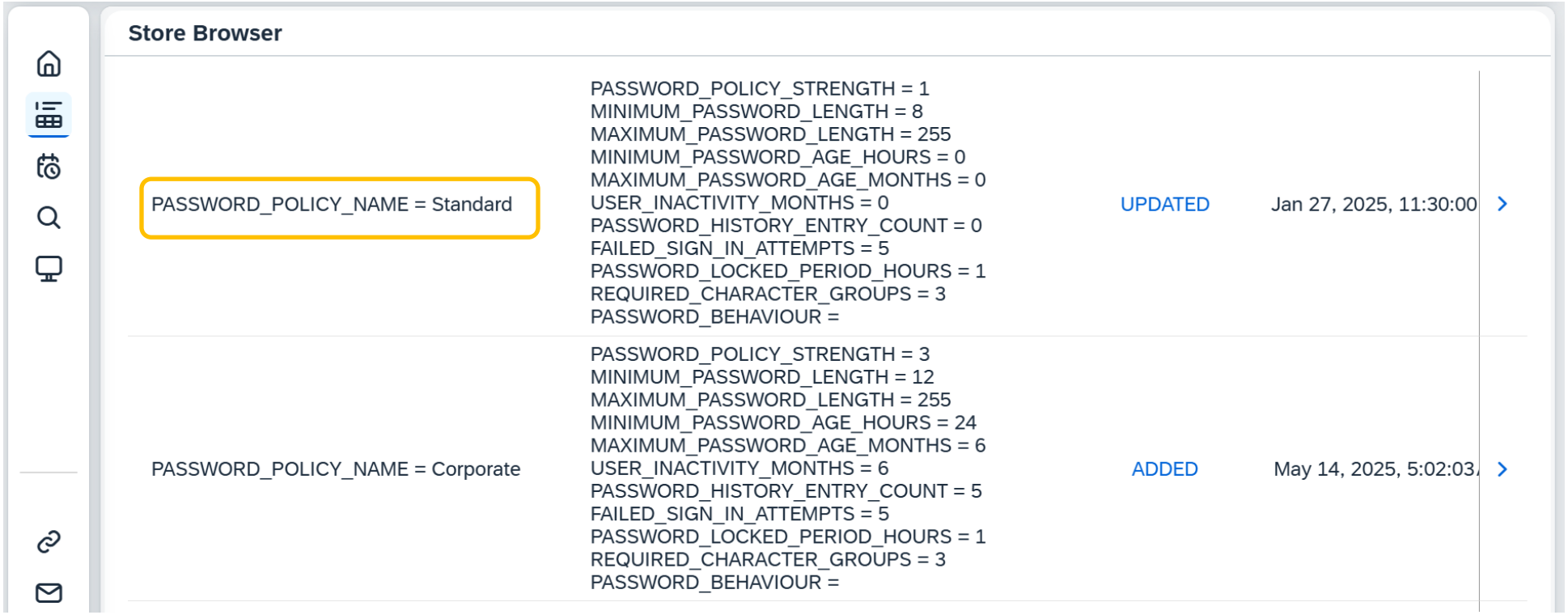


Security Configurations and Recommendations – How is it in SAP Cloud ALM?



Password Policy – Representation in SAP Cloud ALM

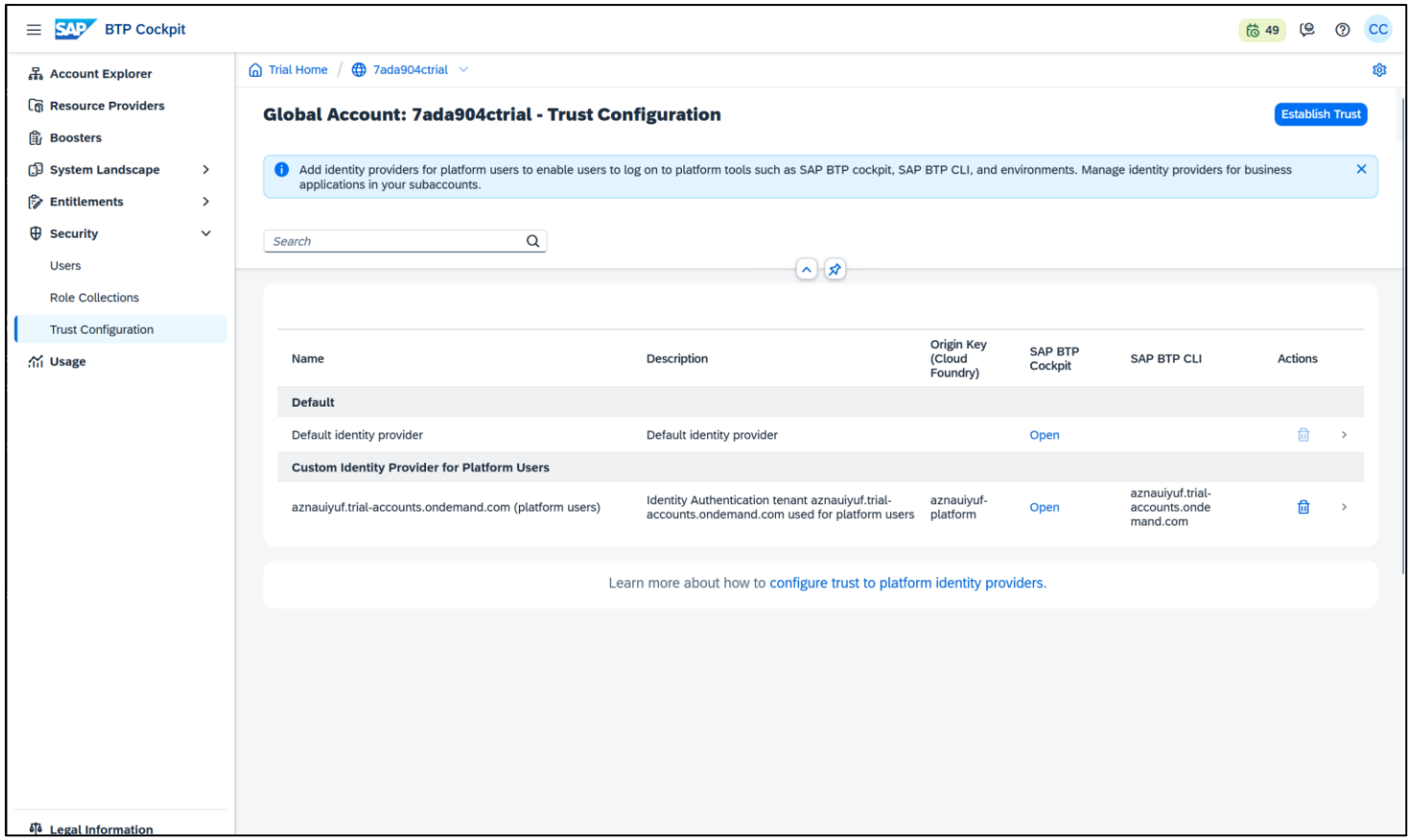




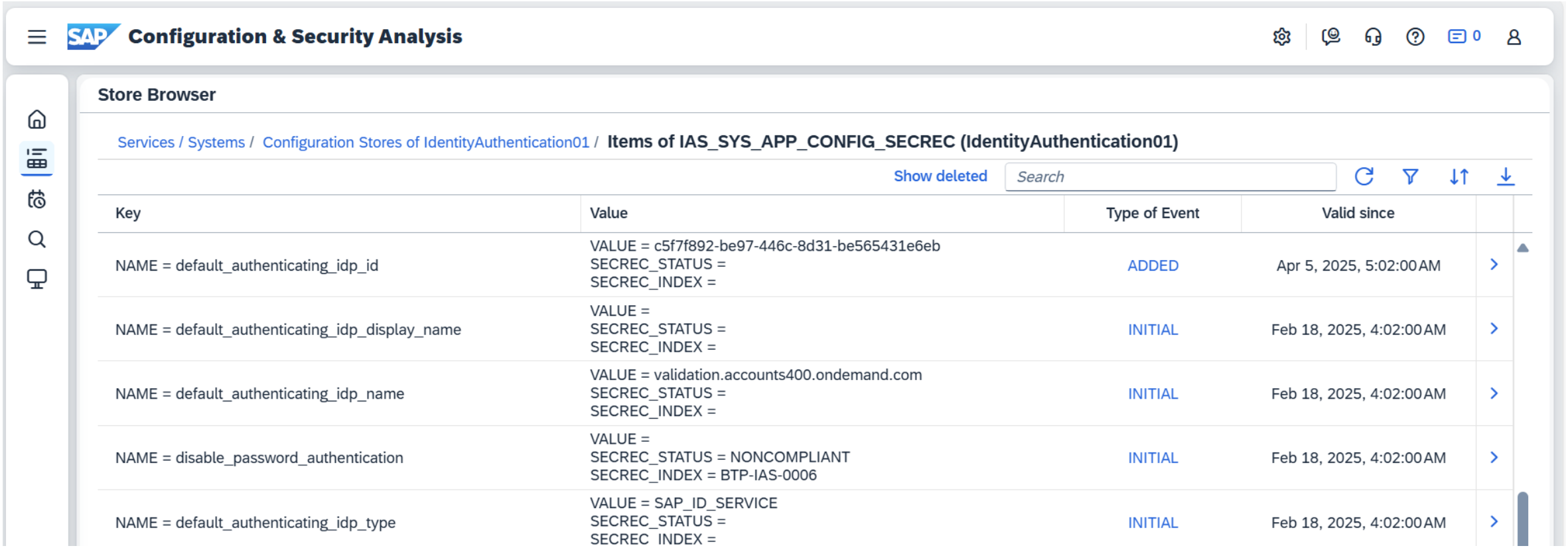
SAP Cloud Identity Services – Identity Authentication

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



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



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 de

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

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

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.	The assignment of the following authorizations is critical. Manage them ideally as part of your identity lifecycle process. • 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, 5:02:03 AM	>
NAME = manage_corp_idp_admin_count	VALUE = systems=2;users=29 SECREC_STATUS = SECREC_INDEX =	UPDATED	May 14, 2025, 5:02:03 AM	>
NAME = manage_groups_admin_count	VALUE = systems=1;users=10 SECREC_STATUS = SECREC_INDEX =	UPDATED	May 14, 2025, 5:02:03 AM	>
NAME = manage_identity_provisioning_admin...	VALUE = systems=0;users=1 SECREC_STATUS = SECREC_INDEX =	UPDATED	May 14, 2025, 5:02:03 AM	>
NAME = manage_tenant_configuration_admin...	VALUE = systems=2;users=29 SECREC_STATUS = SECREC_INDEX =	UPDATED	May 14, 2025, 5:02:03 AM	>
NAME = manage_users_admin_count	VALUE = systems=2;users=29 SECREC_STATUS = SECREC_INDEX =	UPDATED	May 14, 2025, 5:02:03 AM	>

BTP-IAS-0017

*Grant of **Critical Authorizations** should stay under control !*

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

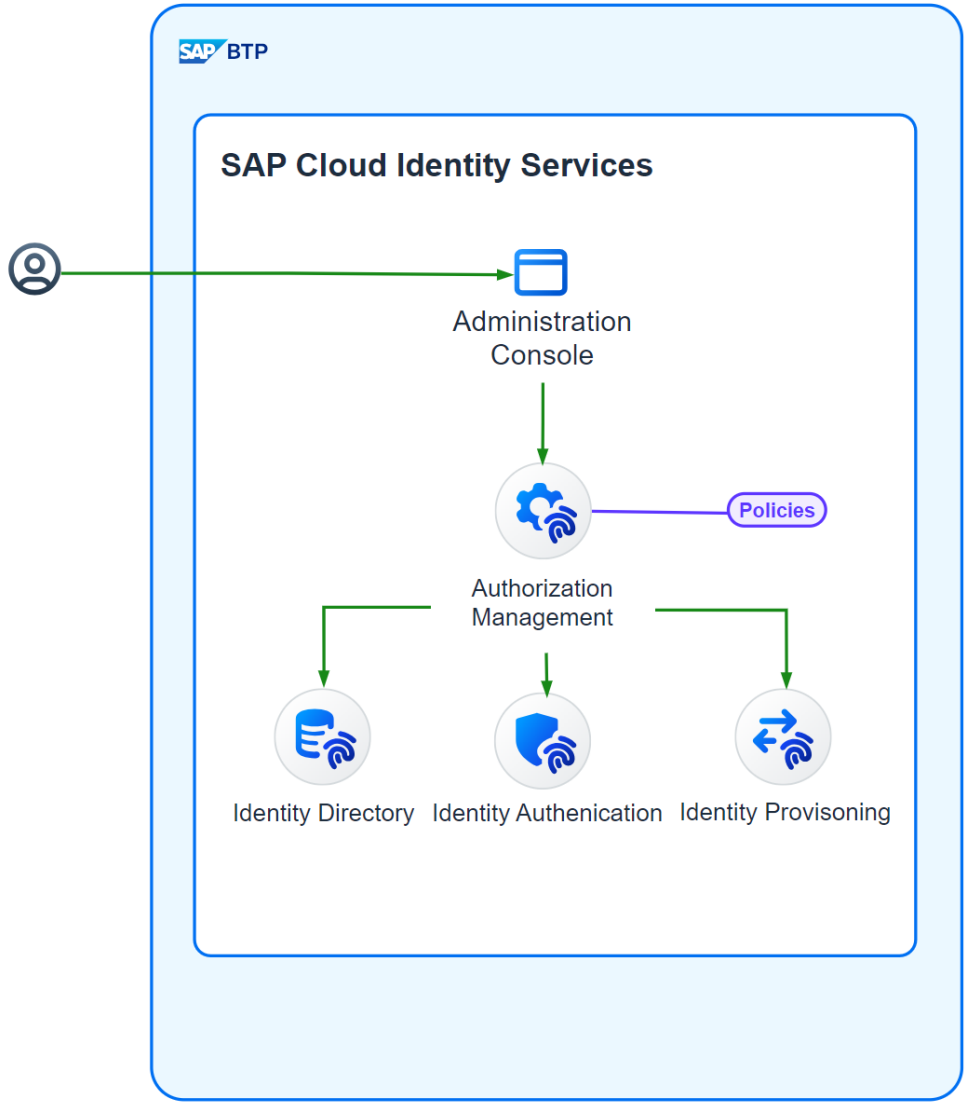
Adjust administrative access to the SAP Cloud Identity console with flexible, policy-based authorizations

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.

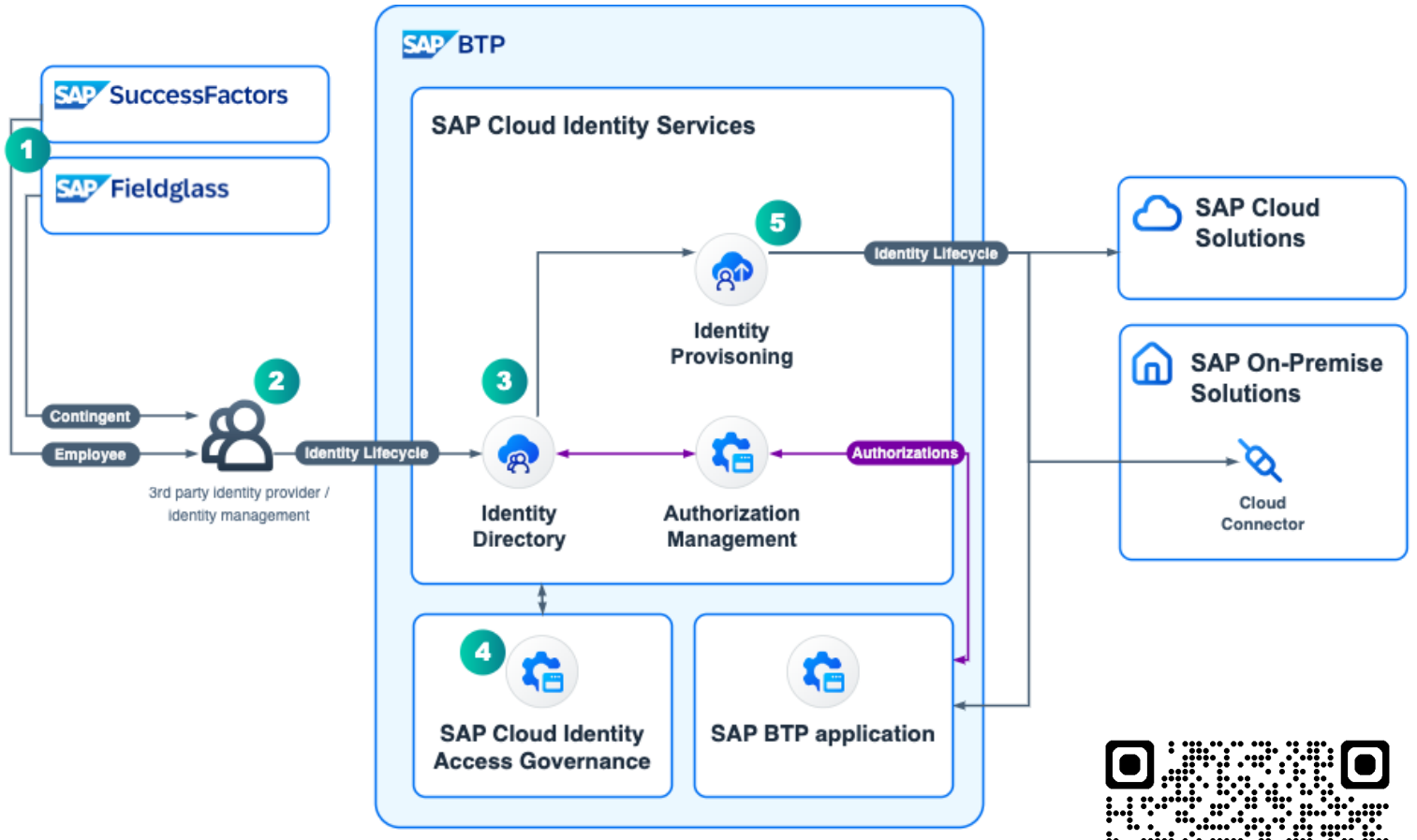
Identity Management solution derives **identity from workforce**.

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.

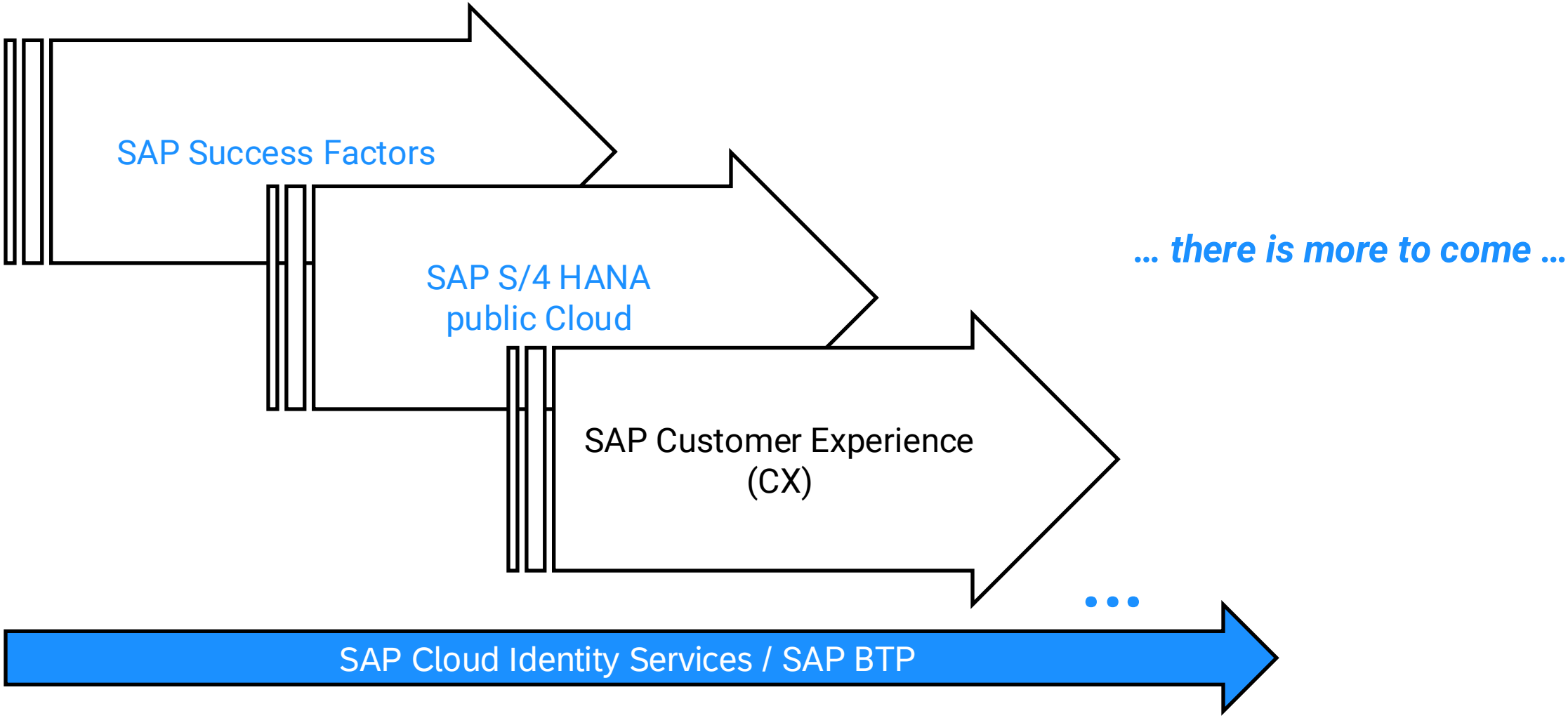
SAP Authorization Management Service manages **policies** for **new BTP apps**.

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



SAP Discovery Center Architecture - Cloud leading Identity Lifecycle

Security Configurations of SAP Cloud Solutions @ SAP Cloud ALM

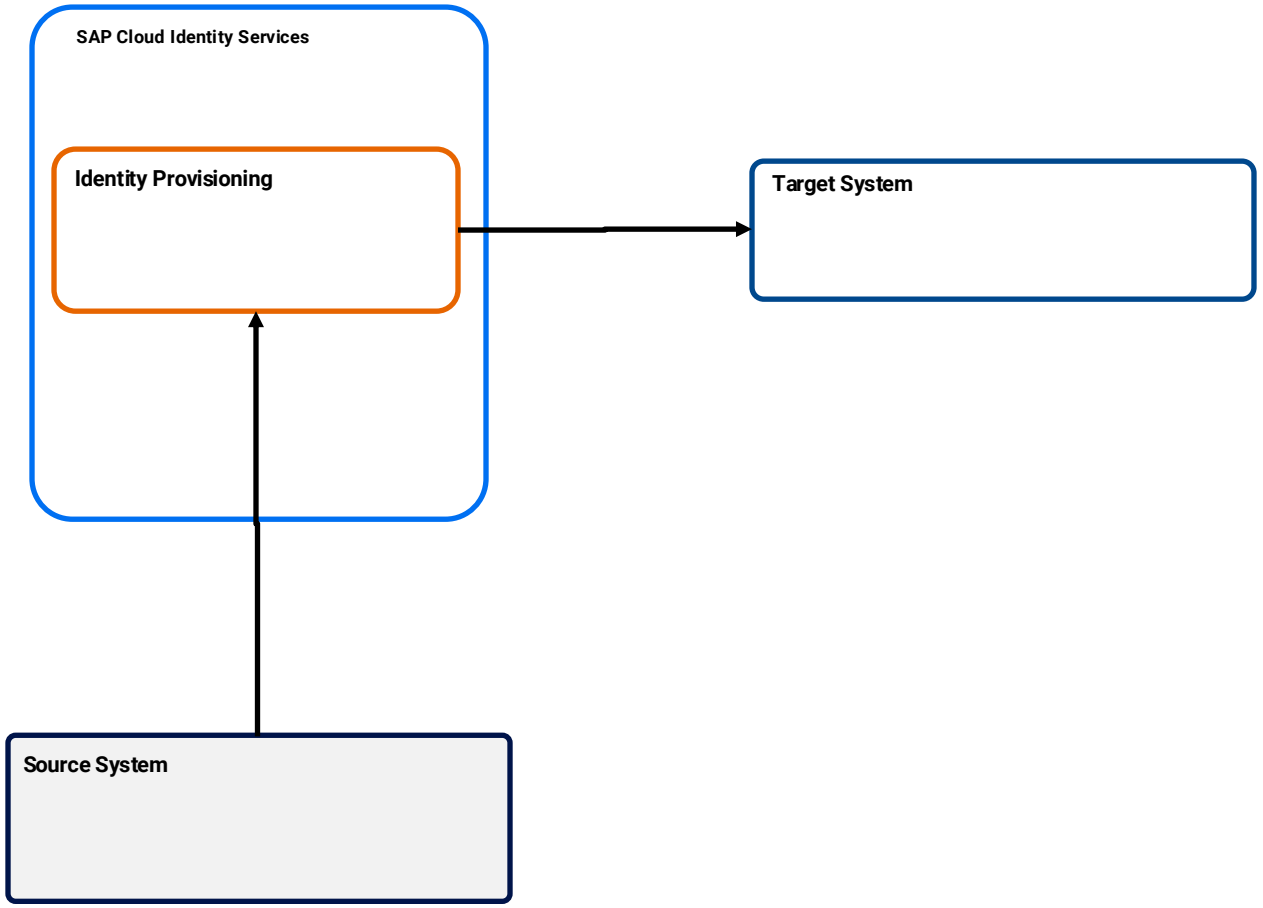


... there is more to come ...

SAP Cloud Identity Services - Identity Provisioning

Lifecycle Automation With Security

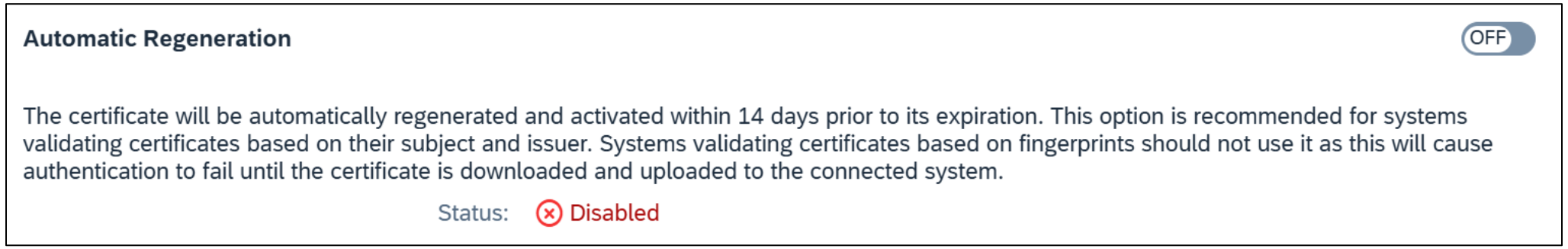
- Use certificate-based authentication
- Enable automatic certificate renewal whenever possible (see next slide)
- Avoid TrustAll in production
- Use secure protocols
- Use credential properties to hold sensitive information
- Assign multiple administrators



SAP Cloud Identity Services - Identity Provisioning
Lifecycle Automation With Security

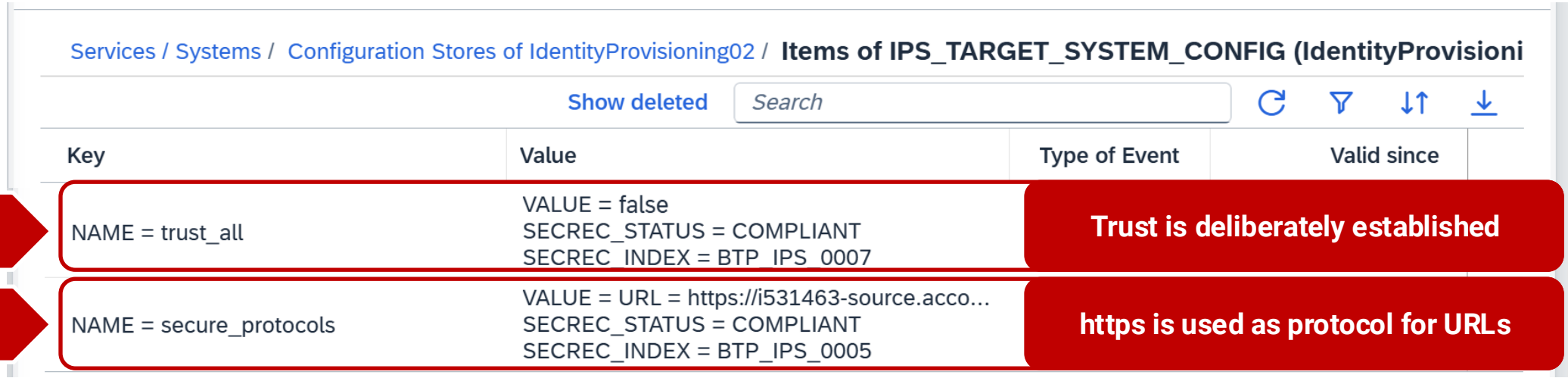
Automated certificate renewal in Identity Provisioning Service

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



- 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



BTP-IPS-0007 — **Trust is deliberately established**

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

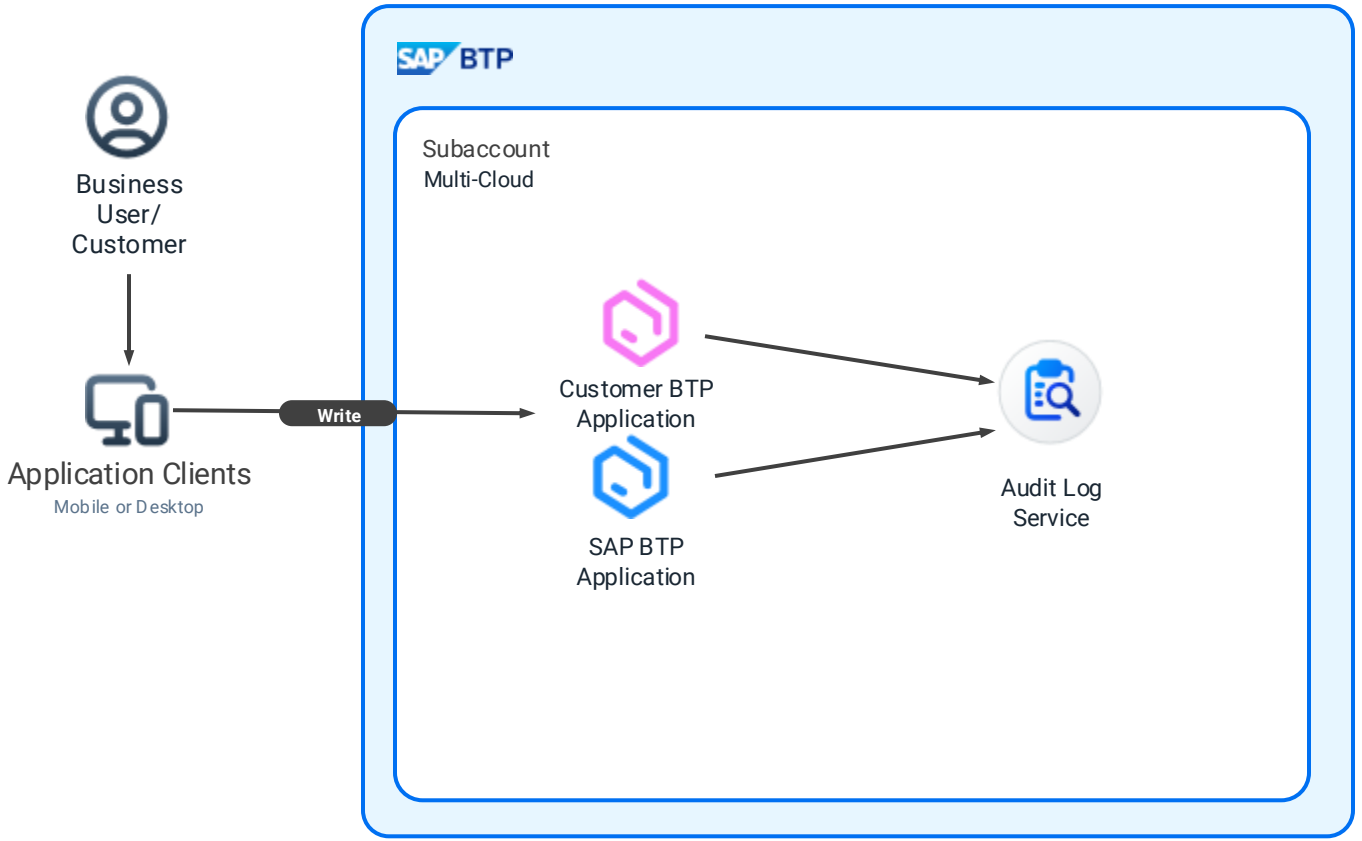
SAP Audit Log service

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

- Timestamp
- Terminal ID
- Audit log event

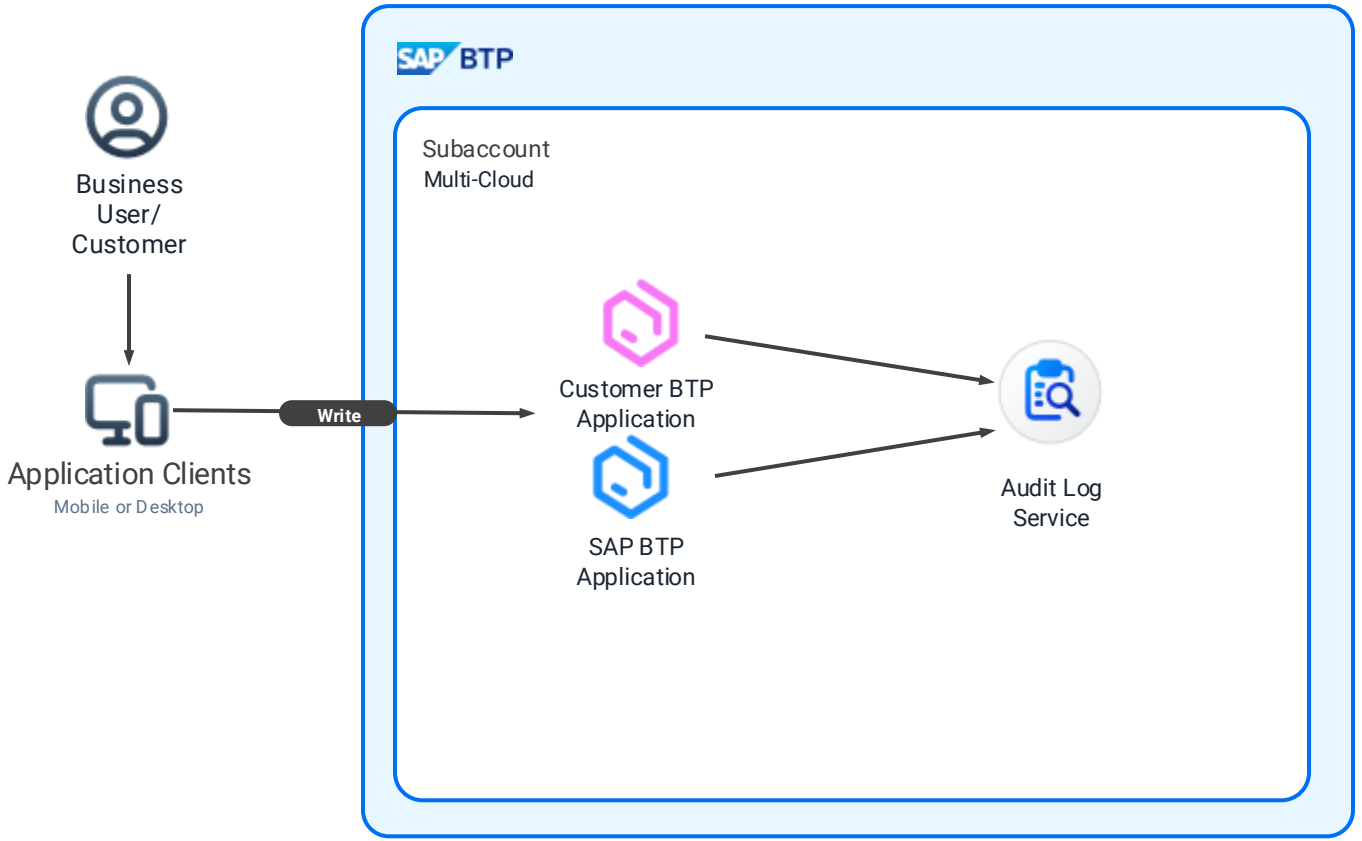
Security-relevant activities include

- 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

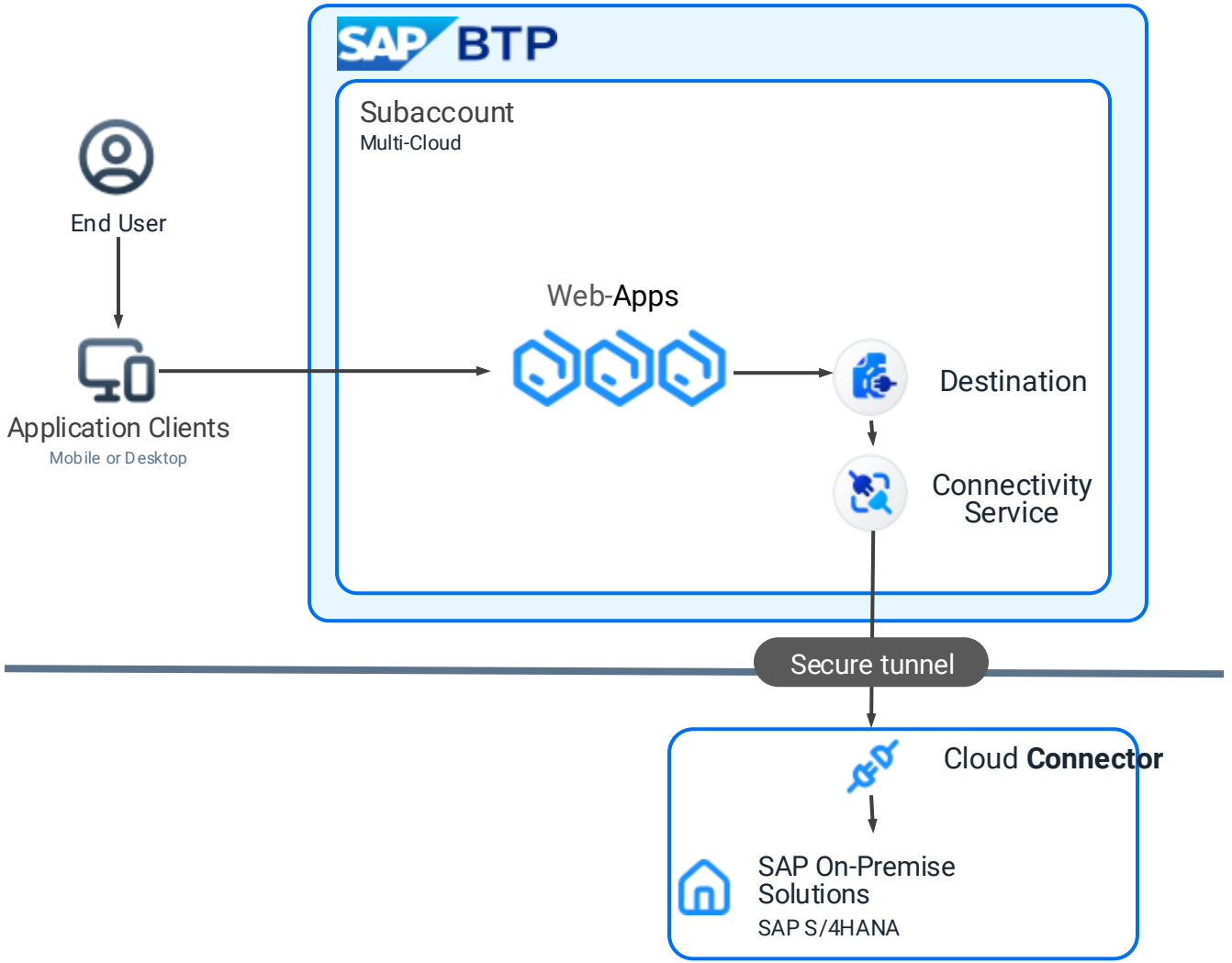


SAP BTP connectivity

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

Features:

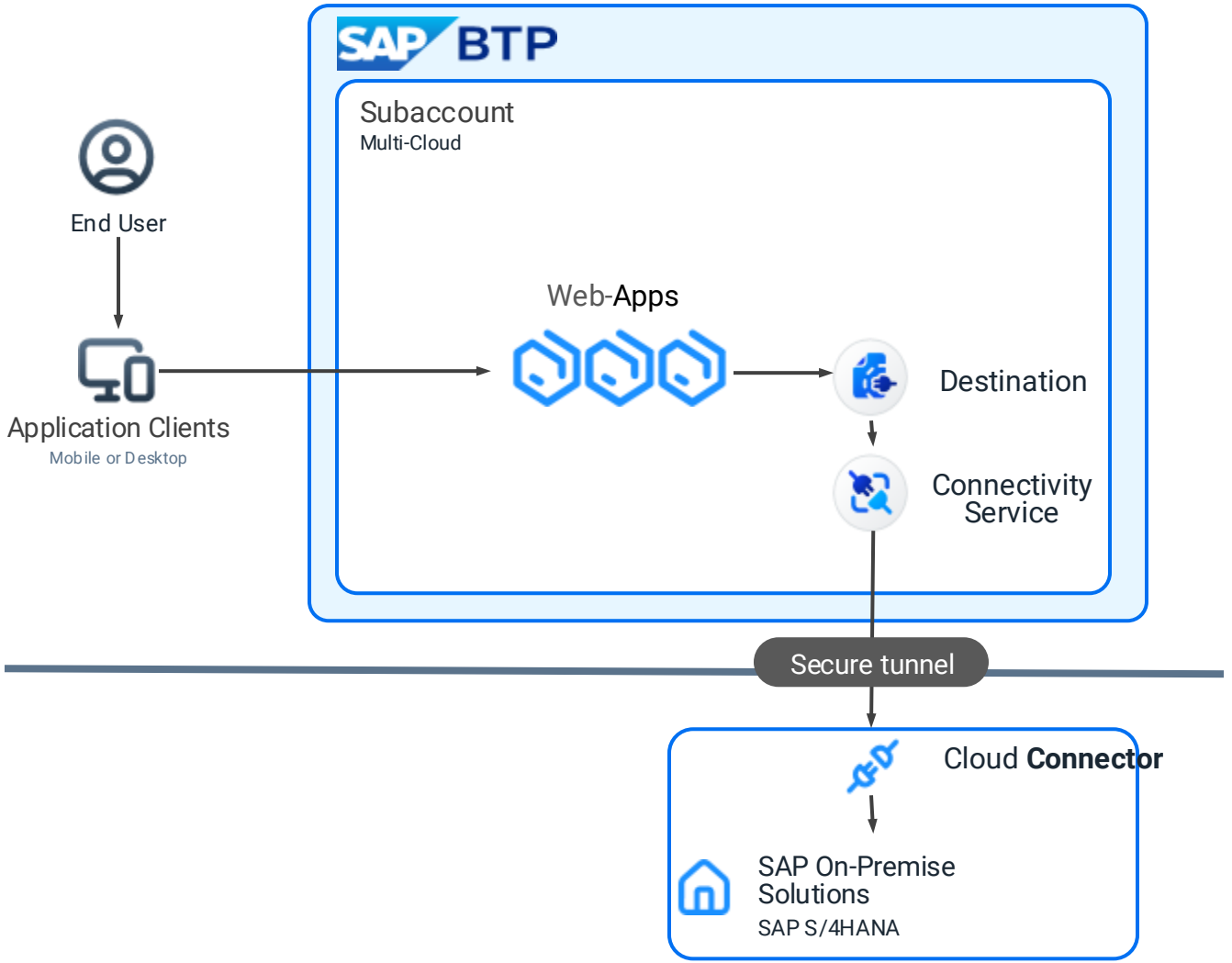
- Access on-premise systems
- Secure tunnel
- Multiple supported protocols
- Access cloud databases via JDBC/ODBC
- Propagate cloud user identity



SAP BTP Connectivity – Destination Service

Secure Your Connections

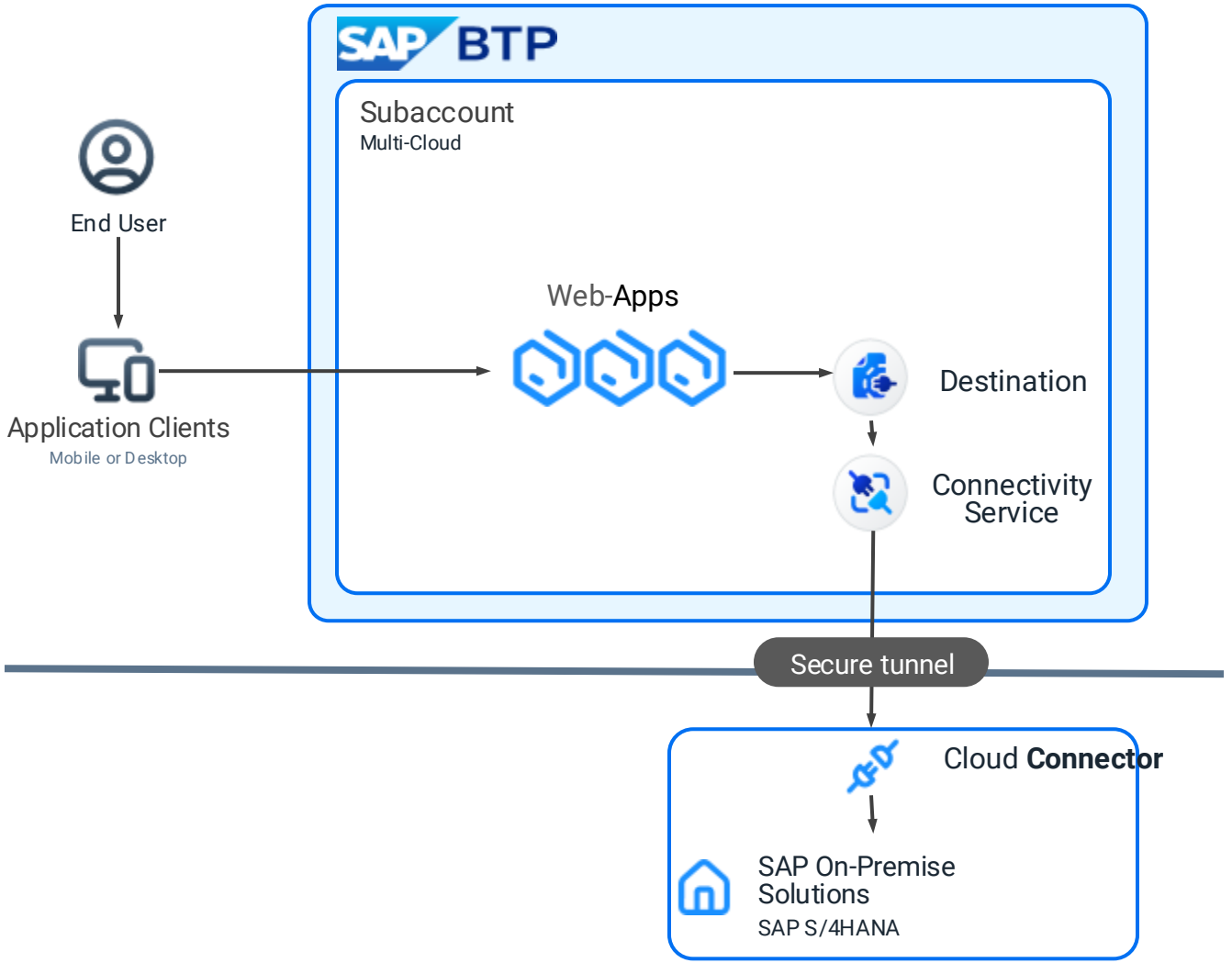
- Use TLS 1.2+ and enable auto-renewal for certs
- Prefer OAuth or SAML over password-based auth
- Avoid deprecated SAP Assertion SSO
- Use mutual TLS in production
- Enable SSO with Principal Propagation
- Validate server certificates



SAP BTP Connectivity – Cloud Connector

Secure The Hybrid Bridge

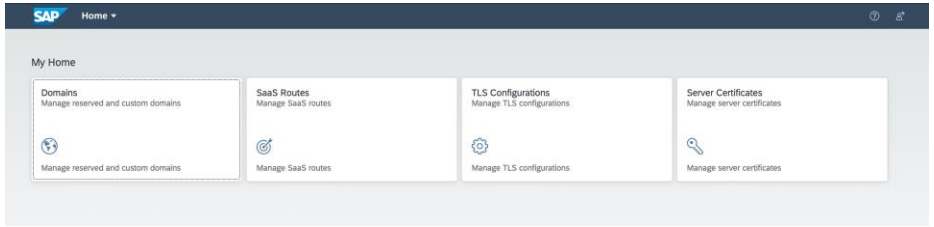
- Enforce HTTPS and monitor exceptions
- Avoid broad sub-paths in URLs
- Use LDAPS and SNC in production
- Limit trusted root CAs and cipher suites
- Replace default admin with LDAP users
- Enable audit logging and trace control

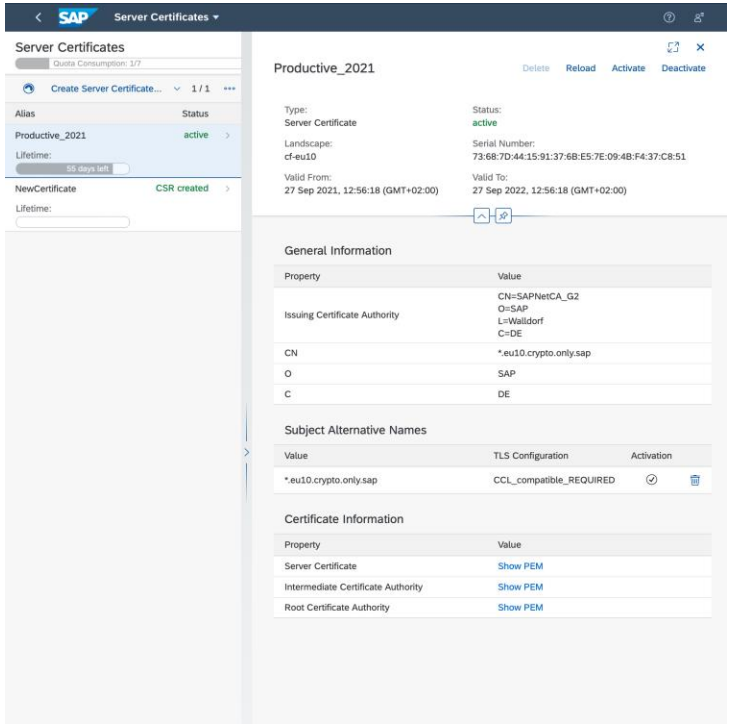


SAP Custom Domain Service

Secure Your Custom Domains

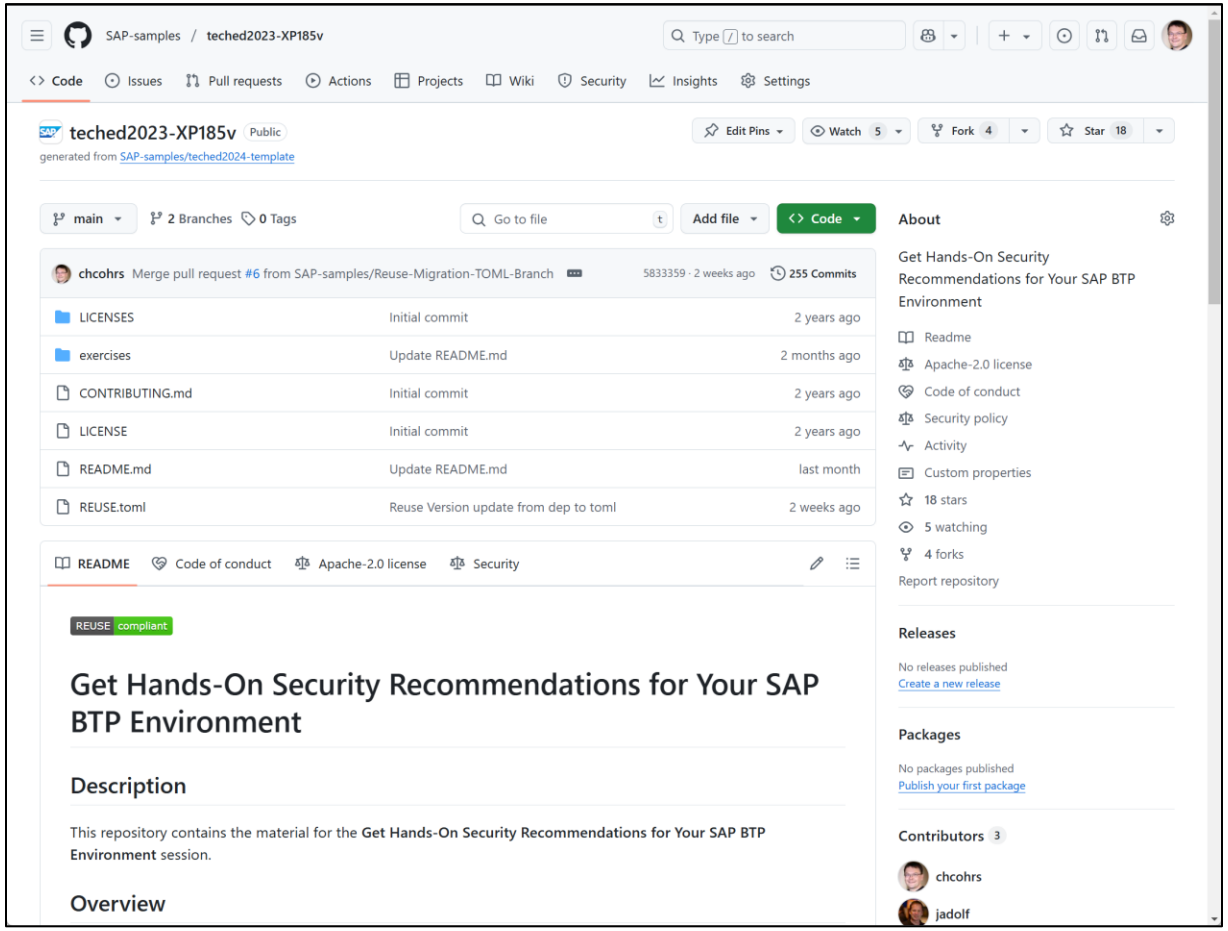
- Assign the Custom Domain Administrator role collection and Space Developer role only to administrators who manage custom domains
- Use the default TLS configurations offered by the Custom Domain Manager. Actively manage use cases that require a different configuration.
- Custom Domain Manager displays 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

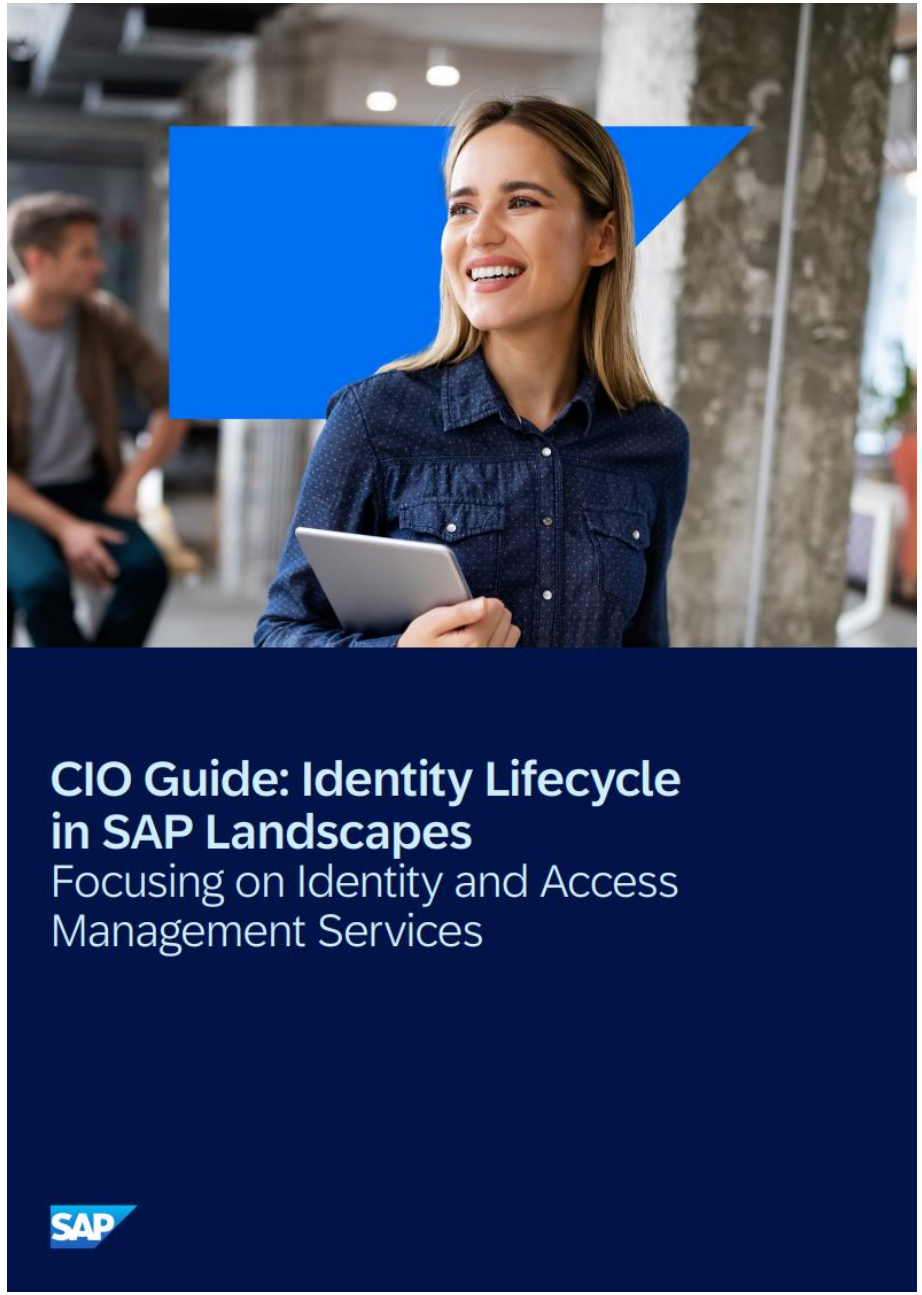
SAP BTP Security Recommendations Hands-On



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



Link

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

Public

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

Public

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

© 2025 SAP SE or an SAP affiliate company. All rights reserved. See Legal Notice on www.sap.com/legal-notice for use terms, disclaimers, disclosures, or restrictions related to this material.