



Secure Configuration Monitoring of SAP Cloud Services

Wihem Arsac, Product Security Expert, SAP
Michael Vogel, Product Security Expert, SAP
23. May 2024

Public



Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP's intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

Agenda

- Background & Motivation
- Accomplishments
- Outlook

Background & Motivation



Cloud Shared Responsibility Model

Responsibilities:

- Cloud providers:
 - Security of datacenters, physical hosts, network, underlying virtualization layer and the list of provided services and APIs
- SAP:
 - Security of cloud accounts configuration, securing the infrastructure (operating systems and/or container images, networking, etc.), securing applications logic/code, and the secure and reliable operation and monitoring of solutions within contractual Service Level Agreements (SLAs),
- Customers:
 - Securing their customer data via security settings in applications and underlying platform services.

Depending on specifics of the solution, some responsibilities can be shifted from one actor to another.

Customers shall therefore be aware of security-related settings they are responsible for.

Further Information: <https://support.sap.com/en/my-support/trust-center/tools-information.html?anchorId=cde4601b0afb44f79a790b599c2cd8b2>

Motivation

- Introducing transparency on security related settings
- Introducing comparability of the same security related setting in all systems
- Introducing capabilities to identify misconfigurations
- Increasing usability and reducing complexity of security features
- Adding transparency and harmonization of Security Recommendations
- Strengthening the shared-responsibility model

Security APIs and Central Security Dashboard

Security powered by transparency

- SAP is harmonizing security reporting capabilities
- With BTP as a frontrunner, key services will support a set of security APIs
- Deliver transparency across services using these APIs
- Partners and customers may use these APIs for custom development and integration into established security tools

1 Note

This guide does not cover security-relevant information for SAP HANA options and capabilities, such as SAP HANA dynamic tiering and SAP HANA smart data streaming. For more information about the security of options and capabilities, see the documentation of the relevant SAP HANA option on SAP Help Portal. Be aware that you need additional licenses for SAP HANA options and capabilities. For more information, see Important Disclaimer for Features in SAP HANA Platform, Options and Capabilities [page 303].

Why Is Security Necessary?

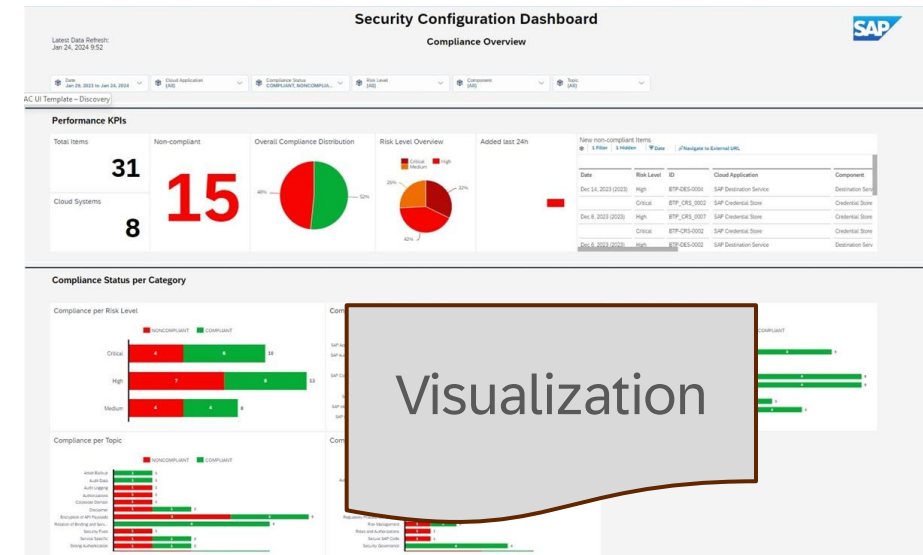
Protecting corporate information is one of the most important topics for you as an SAP HANA customer. You need to meet ever increasing cyber-security challenges, keep your systems secure, and stay on top of the compliance and regulatory requirements of today's digital world. SAP HANA allows you to securely run and operate SAP HANA in a variety of environments and to implement your specific compliance, security, and regulatory requirements.

1.1 Important Critical Configurations

Security Recommendations

```
1 {
2   "Description": "Identity Authentication System",
3   "CustomerID": "390sds1kd2",
4   "SecurityScore": "78",
5   "CustomerContacts":
6   {
7     "admin": "person@place.com",
8     "support": "someone@place.com"
9   },
10  "Systems":
11  [
12    {
13      "Service-411": "IAS Gateway",
14      "Configuration Review":
15      {
16        "Logging events in Audit Log": "True",
17      },
18      "Risky Accounts":
19      {
20        "User-1234": "No MFA Enabled",
21      },
22    }
23  ]
24 }
25
26
27
28
29
30
31
32
33
34
35
36
37 }
```

API



1 Document Security Recommendations

2 Automation through APIs

3 Compliance Visualization

Accomplishments



Security APIs and Central Security Dashboard

Security powered by transparency

- SAP is harmonizing security reporting capabilities
- With BTP as a frontrunner, key services will support a set of security APIs
- Deliver transparency across services using these APIs
- Partners and customers may use these APIs for custom development and integration into established security tools

A central external-facing SAP Cloud ALM API providing data access to customers for all connected SAP services

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation
Identify Authentication	Critical	Filter (No Selector)	Filter (No Selector)	Filter (No Selector)	Filter (No Selector)
Identify Authentication	Critical	Filter (No Selector)	Filter (No Selector)	Filter (No Selector)	Filter (No Selector)

[Security Recommendations](#)

1

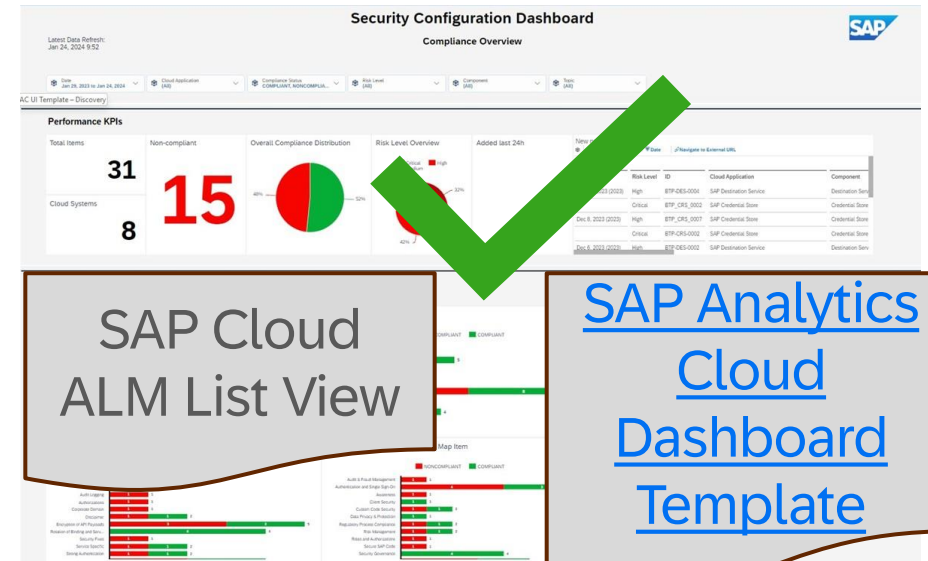
Document Security Recommendations

```
1 {
2   "Description": "Identity Authentication System",
3   "CustomerID": "390sds1kd2",
4   "SecurityScore": "78",
5   "CustomerContacts":
6   {
7     "admin": "person@place.com",
8     "support": "someone@place.com"
9   },
10  "systems":
11  [
12    {
13      "Service": "SAP AS Gateway",
14      "Configuration": "New",
15      "Logging enabled": "True",
16      "Logging event": "Log"
17    },
18  ],
19  "Risky Accounts":
20  {
21    "User-1234": "No MFA Enabled",
22    "User-4949": "Password expires in 10 days",
23    "SolutionLink": "https://help.sap.com/item123",
24  }
25  }
26  }
27  }
28  }
29  }
30  }
31  }
32  }
33  }
34  }
35  }
36  }
37  }
```

[SAP Cloud ALM API](#)

2

Automation through APIs



[SAP Cloud ALM List View](#)

[SAP Analytics Cloud Dashboard Template](#)


3

Compliance Visualization

Publication of Security Recommendations on 'SAP Trust Center'

SAP Global Security

Recommended Security Configuration for SAP Cloud Services

THE BEST RUN 

[UPDATED] March 20, 2023


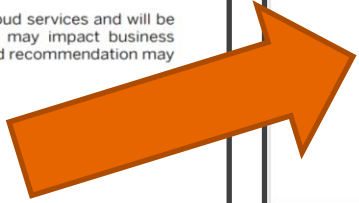
Summary

SAP is committed to delivering trustworthy products and cloud services. Secure configuration is essential to ensuring secure operations and data integrity. We have therefore documented security recommendations that are consolidated in this one place to help you configure the best in security for your SAP portfolio.


This document enlists security recommendation guides for SAP products and cloud services and will be enhanced with further products subsequently. Security configuration changes may impact business continuity and must be carefully planned. Suggestions to improve any documented recommendation may be sent via a ticket on the concerned product.

SAP Security Recommendations

- SAP Business Technology Platform ([Link](#))
- SAP S/4HANA Cloud ([Link](#))
- SAP SuccessFactors ([Link](#))
- SAP Ariba ([Link](#))
- SAP Concur ([Link](#))
- SAP Fieldglass ([Link](#))
- SAP Commissions ([Link](#))
- SAP Analytics Cloud ([Link](#))
- SAP Integrated Business Plan
- SAP Cloud for Customer ([Link](#))

SAP Help Portal (Documentation) Browse by Product SAP Learning Journeys Dashboards Help

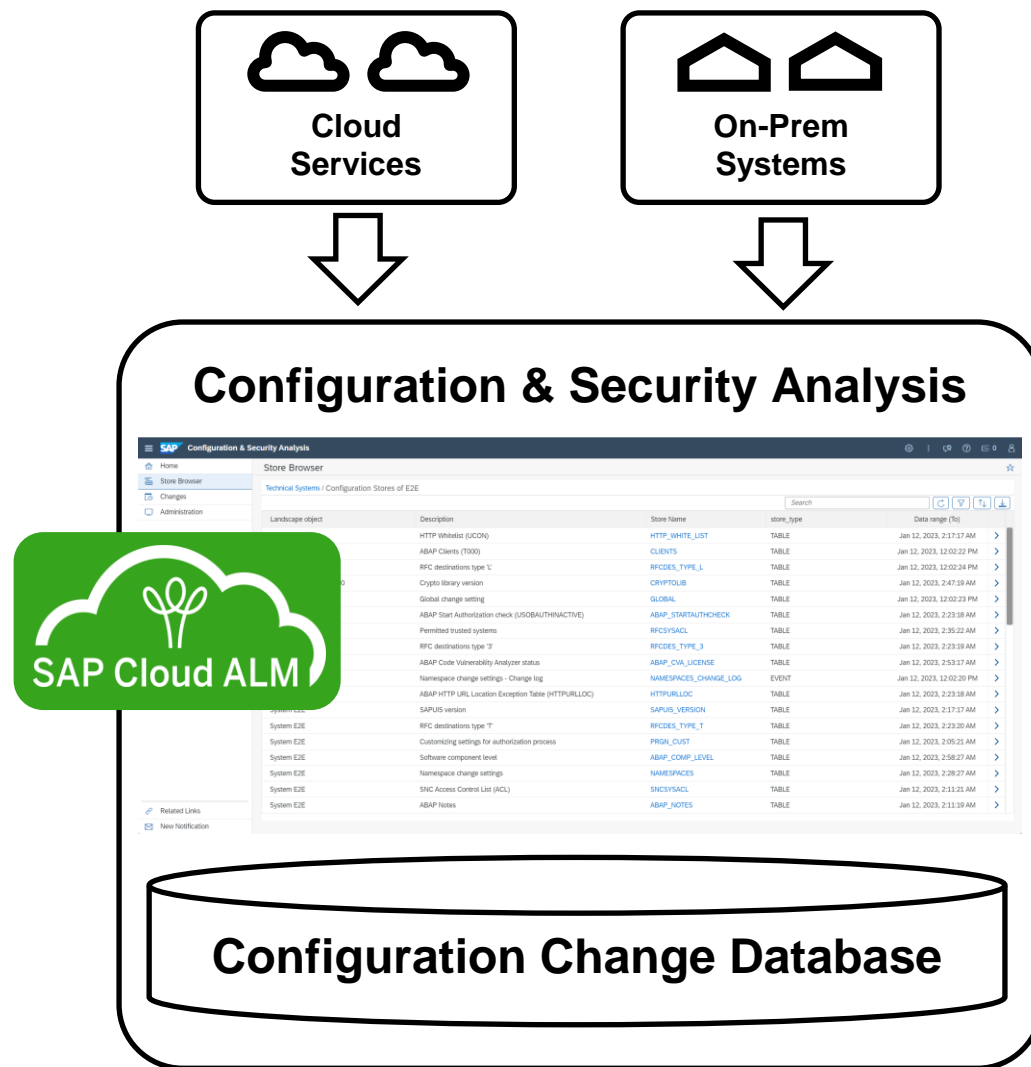
☆ Favorite  Do

Service	Priority	Secure Operations Map	Topic	Default Setting or Behavior	Recommendation	More Information
Filter: [No Selection] ▼	Filter: [No Selection] ▼	Filter: [No Selection] ▼	Filter: Strong Authentication ▼			
Identity Authentication	Critical	Authentication and Single Sign-On	Strong Authentication	Default authentication method for the administration console is user name and password.	Protect the administration console application with two-factor authentication.	Configure Risk Based Authentication on an Application
Identity Authentication	Advanced	Authentication and Single Sign-On	Strong Authentication	End users must authenticate against the service to achieve single sign-on across services. The default authentication method is to enter a user name and password.	Use passwordless authentication methods. Disable password authentication for end users.	<ul style="list-style-type: none"> ▪ Configure Kerberos Authentication ▪ Enable User to Generate and Authenticate with Certificate ▪ Enable or Disable FIDO Biometric Authentication for an Application
SAP Destination service	Recommended	Authentication and Single Sign-On	Strong Authentication	HTTP Destinations: The service offers a number of authentication types for HTTP destinations, which you can configure based on your technical or security requirements.	Use the following authentication types: <ul style="list-style-type: none"> ▪ For on-premise connections, use Principal Propagation SSO Authentication for interactive HTTP sessions. ▪ For Internet connections, use OAuth SAML Bearer Assertion Authentication or SAML Assertion Authentication. 	HTTP Destina

SAP Cloud ALM – Configuration & Security Analysis

Existing functionality:

- ✓ **Regular collection** of configuration items and software levels into the configuration stores of the **Configuration Change Database**
- ✓ **Store browser** as user interface to **visualize content of configuration stores**
- ✓ **Change analysis** for selected scope and timeframe
- ✓ **Search capability** for pattern-based browsing into configuration items of selected scope
- ✓ **Analytics API** for aggregated and item-level data



SAP Identity Authentication Service – API Payload

Priority	Title	Default Setting or Behavior	Recommendation	Index	API Payload
Critical	Self-Registration of End Users	For business-to-consumer (public) scenarios, self-registration may be required. By default, self-registration is disabled (value = internal) and can be configured per application. Corporate identity lifecycle processes make self-registration undesirable in most business-to-employee (B2E) and business-to-business (B2B) scenarios.	Keep self-registration disabled (value = internal). Actively manage use cases that require the function.	BTP-IAS-0003	NAME= user_application_access VALUE= public SECREC_INDEX= BTP-IAS-0003 SECREC_STATUS= NONCOMPLIANT
Critical	Social Sign-On of End Users	For business-to-consumer (public) scenarios, social sign-on may be required. By default, social sign-on is disabled (value = internal) and can be configured per application. Corporate identity lifecycle processes make social sign-on undesirable in most business-to-employee (B2E) and business-to-business (B2B) scenarios.	Keep social sign-on disabled (value = off). Actively manage use cases that require the function.	BTP-IAS-0005	NAME= social_sign_on VALUE= OFF SECREC_INDEX= BTP-IAS-0005 SECREC_STATUS= COMPLIANT

SAP Identity Authentication Service – Payload Representation in SAP Cloud ALM

SAP Configuration & Security Analysis

Store Browser

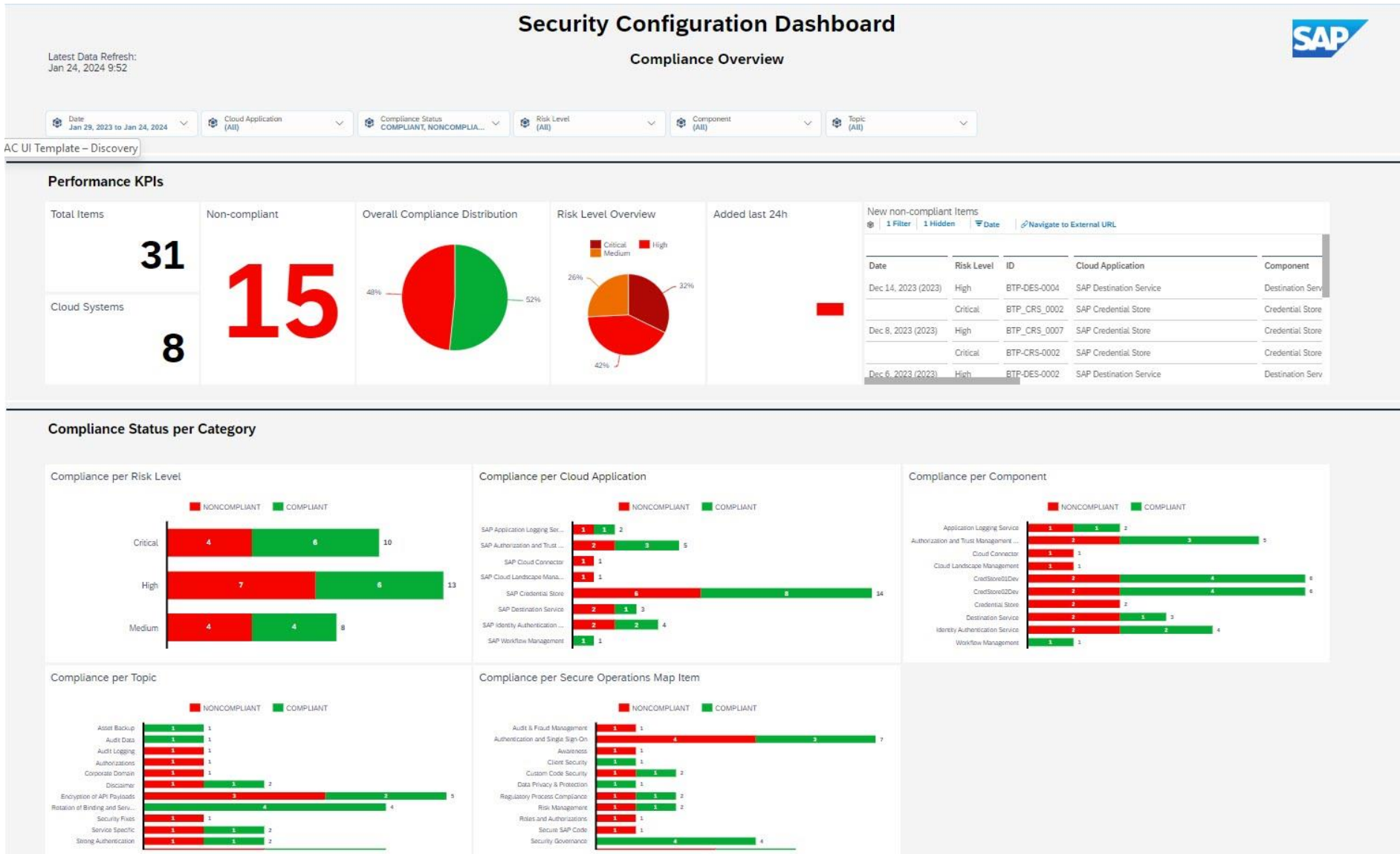
Technical Systems / Configuration Stores of validation / Items of IAS_SYS_APP_CONFIG

Search

Key	Value	Type of Event	Valid since
NAME = branding	VALUE = SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0021	INITIAL	Sep 21, 2023, 4:11:48 PM
NAME = disable_password_authentication	VALUE = configured SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0006	INITIAL	Sep 21, 2023, 4:11:48 PM
NAME = password_policy	VALUE = enterprise SECREC_STATUS = COMPLIANT SECREC_INDEX = BTP-IAS-0002	INITIAL	Sep 21, 2023, 4:11:48 PM
NAME = reCAPTCHA	VALUE = SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0025	INITIAL	Sep 21, 2023, 4:11:48 PM
NAME = social_sign_on	VALUE = OFF SECREC_STATUS = COMPLIANT SECREC_INDEX = BTP-IAS-0005	INITIAL	Sep 21, 2023, 4:11:48 PM
NAME = user_application_access	VALUE = public SECREC_STATUS = NONCOMPLIANT SECREC_INDEX = BTP-IAS-0003	INITIAL	Sep 21, 2023, 4:11:48 PM

SAP Analytics Cloud Dashboard Template

Compliance Overview



SAC Dashboard Template – Trend Analysis View



SAP Analytics Cloud Dashboard Template

- Cloud ALM provides basic search and display functionality for the collected data.
- A dashboard template based on SAP Analytics Cloud to complement this visualization.
- Provided as community content to inspire your own content development
- Extendable by customers and partners.



Accomplishments - Overview

- Requirement for standardized security recommendations and API for major cloud products introduced in SAP development guidelines
- Around 350 Security Recommendations for 12 major SAP Cloud Products and 30 Business Technology Platform services published
- SAP Cloud ALM Analytics API for Configuration & Security Analysis Content released
- First data from SAP Business Technology Platform services delivered via SAP Cloud ALM API:
 - Credential Store
 - Identity Authentication
 - Mobile Service
- SAP Analytics Cloud Security Configuration Dashboard template released

Outlook

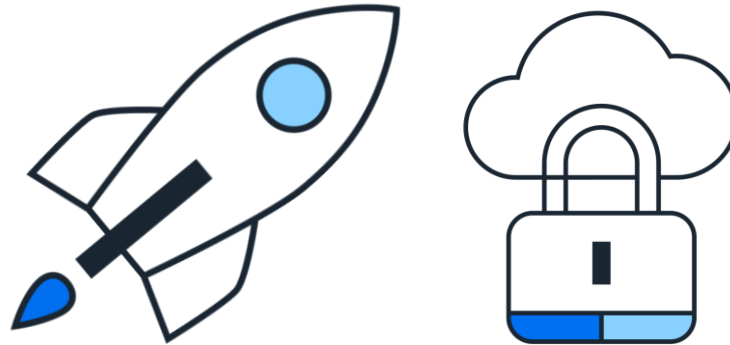


Outlook

- BTP and other products adding security recommendations for further services
- Configuration data exposed for additional BTP services via external SAP Cloud ALM API
- Additional cloud products and services to deliver security configuration data to the SAP Cloud ALM backend for exposure via the external API ongoing
- Collaboration with partners to integrate this data into their solutions

Resources

- Secure configuration [recommendations](#) for key SAP cloud services
- Technology Blogs by SAP
[Secure Configuration Monitoring of SAP Cloud Services](#)



- [SAP Analytics Cloud Security Configuration Dashboard Template](#)
- [SAP Cloud ALM CSA Rollout documentation](#)
- [SAP Cloud ALM API Documentation on API Hub](#)



Thank you.

Contact information:

Wihem Arzac (wihem.arsac@sap.com)

Michael Vogel (m.vogel@sap.com)

