SAP Cloud Platform Identity Authentication

Product Overview

January 2019
Introduction

Simplify

Integrate

Protect

Summary
Introduction

Simplify

Integrate

Protect

Summary
SAP Cloud Platform

Key use cases

**Connect**  
People & Data

Deliver delightful user experiences across various digital touchpoints enabling innovation, without disrupting core business processes.

**Extend**  
Cloud & On-Prem Apps

Quickly add new functionality to your existing cloud and on-prem apps to optimize your existing investments.

**Build**  
Differentiating Digital Apps

Rapidly build and run new cloud apps, business services and APIs to solve new problems, engage new customers, and drive new revenue.

**Integrate**  
Apps, Data & Processes

Connect your cloud and on-prem apps to eliminate data silos and make digital access simple, secure, and scalable.

---

© 2019 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
A secure platform

Secure Applications

SAP Cloud Platform

Secure Connectivity

Secure Login

Secure Data

Secure Hybrid Connectivity using SAP Cloud Connector
End-to-end Authentication using Principal Propagation
Encryption of Data in Transit

A secure platform

Authentication & Single Sign-On
Based on Industry Standards
Identity Federation with existing IdPs
Strong 2-Factor Authentication
Hybrid Identity Integration
Secure Login

Choice of world-class data centers
Encryption of Data at Rest
Secure Credentials Store

Secure Connectivity

Secure Data

Strong Authorization Management
Comprehensive set of APIs to ensure secure development
Code Vulnerability Analysis
Self-defending applications using tainting
Secure Applications

Secure Data
A secure platform

Secure Login
Authentication & single sign-on
Based on industry standards
Identity federation with existing IdPs
Strong two-factor authentication
Hybrid identity integration

Secure Applications

SAP Cloud Platform

Secure Data

Secure Connectivity
A secure platform

Secure Applications

- Strong authorization management
- Comprehensive set of APIs to ensure secure development
- Code vulnerability analysis
- Self-defending applications using tainting

Secure Login

SAP Cloud Platform

Secure Connectivity

Secure Data

Choice of world-class data centers

- Encryption of Data at Rest
- Secure Credentials Store
- Secure Data
- Secure Applications

A secure platform

© 2019 SAP SE or an SAP affiliate company. All rights reserved. | PUBLIC
A secure platform

Secure Applications

Secure Connectivity

Secure hybrid connectivity using SAP Cloud Connector
End-to-end authentication using principal propagation
Encryption of data in transit

Secure Data

Secure Login

SAP Cloud Platform
A secure platform

Secure Applications

SAP Cloud Platform

Secure Login

Secure Connectivity

Secure Data

Choice of world-class data centers
Encryption of data at rest
Secure credentials store
A secure platform

Secure Applications

Secure Login

SAP Cloud Platform

Secure Connectivity

Secure Data
A secure platform

SAP Cloud Platform

Proven by various ISO & SOC Certifications
<table>
<thead>
<tr>
<th>Identity Management</th>
<th>Governance, Risk &amp; Compliance</th>
<th>Authentication &amp; Single Sign-on</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP CP Identity Provisioning</td>
<td>SAP Cloud Identity Access Governance</td>
<td>SAP CP Identity Authentication</td>
</tr>
<tr>
<td>SAP Identity Management</td>
<td>SAP Access Control</td>
<td>SAP Single Sign-On</td>
</tr>
<tr>
<td>Authorizations</td>
<td>Request Role</td>
<td>SAP ID Service</td>
</tr>
<tr>
<td>Users</td>
<td>Compliance</td>
<td>SAP Cloud Identity</td>
</tr>
<tr>
<td>Roles</td>
<td>Segregation of Duties</td>
<td>Single Sign-On</td>
</tr>
<tr>
<td>De-Provisioning</td>
<td>Business Roles</td>
<td>Authentication</td>
</tr>
<tr>
<td>SCIM</td>
<td>Role Mining</td>
<td>SAML</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Two-Factor Authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Digital Certificates</td>
</tr>
<tr>
<td>Identity Management</td>
<td>Governance, Risk &amp; Compliance</td>
<td>Authentication &amp; Single Sign-on</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>SAP CP Identity Provisioning</td>
<td>SAP Cloud Identity Access Governance</td>
<td>SAP CP Identity Authentication</td>
</tr>
<tr>
<td>SAP Identity Management</td>
<td>SAP Access Control</td>
<td>SAP Single Sign-On</td>
</tr>
</tbody>
</table>

**Setting the stage**

**Accessing the applications**
End User

Secure Authentication & Single Sign-On

SAP Cloud Platform

Identity Authentication

Identity Provisioning

Corporate Identity Provider

Identity Store (e.g., HR)
- Users, Groups, Roles
- Cloud or On-Premise

Management of Identities and Authorizations*

* For a detailed list of applications currently supported by Identity Provisioning, please refer to the online documentation.
Identity and Access Management as a service from SAP

Solution overview

A complete cloud identity suite enabling organizations to easily manage user on-boarding and access

---

**SAP Cloud Platform Identity Provisioning**
- Cloud-based service for identity lifecycle management
- Managing users, roles, and groups in cloud- and hybrid landscapes
- Based on SCIM industry standard

**SAP Cloud Platform Identity Access Governance**
- Access governance solution on SAP Cloud Platform
- Visibility into access issues for on-premise and cloud applications

**SAP Cloud Platform Identity Authentication**
- Single sign-on to browser-based applications (cloud and on-premise)
- Various authentication options
- Different user store integration scenarios
SAP Cloud Platform Identity Authentication Service

Simplify
Optimal user experience

Integrate
 Seamlessly integrate into existing infrastructure

Protect
Secure application access
SAP Cloud Platform Identity Authentication Service (IAS)

Product overview

Simplify
- Single sign-on for a beautiful user experience
- Convenient user self-services

Integrate
- Integration with existing user stores
- Leverage open security standards
- Branding of end user UIs

Protect
- Various authentication options
- Access protection to applications
- Password and privacy policies
Introduction

Simplify

Integrate

Protect

Summary
Beautiful logon screens ...
Simplified.

Log On

E-Mail

Password

Remember me

Log On
User self-services

Convenient user self-services
- Self-registration (optional)
- Account confirmation via email
- Forgot password

User profile self-services
- Edit details & change password
- Mobile device activation (for 2FA)
- (Un-)Link social accounts

Product features
- Responsive UIs
- Multi-language support
Based on open security standards

Interoperable with all applications supporting SAML 2.0 or OpenID Connect standard
Delegated authentication
IAS as a proxy to a corporate identity provider (IdP)

Identity provider proxy
- Authentication is delegated to corporate identity provider login
- Reuse of existing single sign-on infrastructure
- Easy and secure authentication for employee scenarios
- Federation based on the SAML 2.0 standard
Delegated authentication
Authentication with an on-premise user store

On-premise user store
- Users credentials from:
  - Active Directory (through LDAP)
  - AS ABAP (through SCIM*)
- No user provisioning to the cloud required
- Internal network ports do not need to be exposed to the Internet
- In addition, usual product features can be used:
  - UI configuration, policies, two-factor authentication

* requires AS Java + SAP Single Sign-On (which enables SCIM interface)
Delegated authentication
Re-use of Windows Domain Authentication (SPNEGO)

SPNEGO authentication

- Users authenticated with Microsoft Active Directory enjoy single sign-on to cloud applications without re-authentication
- Reuse of existing corporate identity infrastructure
- Secure authentication and SSO for cloud and on-premise web applications

SPNEGO: Simple and Protected GSSAPI Negotiation Mechanism
Delegated authentication
Conditional authentication

Forwarding of requests to connected IdPs based on

- IP-address range
- Email address domain
- User type
- Group membership

A persistent cookie is stored in the client’s browser to ease the subsequent login processes.
Delegated authentication
IdP-initiated authentication

IAS as a proxy to multiple IdPs

- Allow partner users to login via their corporate IdP
- Authentication is initiated by the corporate IdP
- Optional check for correct user group assignment possible*

* In this case, sync of users from IdPs to groups in IAS is required.
How can users be created?

- **Manual creation**
- **CSV-upload**
- **Sync through IPS***
- **Self-registration**
- **Identity Authentication**
- **Programmatically through SCIM**
- **Manual creation**

* IPS: SAP Cloud Platform Identity Provisioning
Branding and customization

Customization features
- Company logo
- Application name and logo
- Color style
- Terms of use & privacy policy
- Adjust UI texts via API
- Email templates

Product features
- Responsive UIs
- Multi-language support
Logon overlays in customer applications

Logon screen as an overlay (compared to a browser redirect to navigate away from application)

- Can programmatically be integrated by the application
- Out-of-the-box integration for SAP Cloud Portal
Introduction

Simplify

Integrate

Protect

Summary
Authentication options

Basic authentication
- User ID / email and password

Re-use of Windows Domain Logon
- Use of Kerberos token for single sign-on

Two-factor authentication
- Second factor on mobile device

Delegated logon
- Social IdPs
- Corporate IdP
Two-factor authentication with SAP Authenticator

Authentication with one-time passwords
- Provide two means of identification
- OTP required for login in addition to password or security token
- Second factor for high security scenarios

Based on SAP Authenticator mobile app
- OTP (6-digit) created on mobile device
- Available for iOS and Android
- RFC 6238 compatible
  (compatible with Authenticator apps from Google and Microsoft)
Control access to the application

- User
- Member of user group
- Authentication method
- IP-address range
- User type
- Assignment to application
- Self-registered?
- Email verified?
- Allow
- Deny
- Two-factor authentication
- IAS
- Application
Control access to the application

- User type: "employee"
- Assignment to application
- Self-registered?
- Email verified?
- IP-address range
- Authentication method
- Member of user group
- Allow to application
- Application
Control access to the application

User → IAS → Application

- User type
- IP-address range “10.55.0.0/16”
- Assignment to application
- Self-registered?
- Email verified?
- Authentication method
- Member of user group “Admin”
- Two-factor authentication
Protecting self-registration with Google reCAPTCHA / phone verification

Access protection for applications

- Protect the registration to applications from spam and abuse
- Prevent bots from automated fake user registrations to your websites
- Further information
  - Google reCAPTCHA
  - Phone verification
Custom password policies can be configured

Custom password policy configuration
User & group management

User administration
- Web based user management
- User search
- Mass user import/export
- Monitor user access

User groups administration
- Define user groups
- Assign users to groups

Integration
- Programmatic integration via SCIM REST APIs
Summary
Support? Ask the community!

SAP Cloud Platform Identity Authentication
https://www.sap.com/community/topics/cloud-platform-identity-authentication.html

SAP Cloud Platform Identity Provisioning
https://www.sap.com/community/topics/cloud-platform-identity-provisioning.html
SAP Cloud Platform Identity Authentication Service

Simplify
Optimal user experience

Integrate
Seamlessly integrate into existing infrastructure

Protect
Secure application access
Thank you.
## Acronym glossary

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Full Text</th>
<th>Acronym</th>
<th>Full Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>B2B</td>
<td>Business to Business</td>
<td>OTP</td>
<td>One-time password</td>
</tr>
<tr>
<td>B2C</td>
<td>Business to Consumer</td>
<td>REST</td>
<td>Representational State Transfer</td>
</tr>
<tr>
<td>B2E</td>
<td>Business to Employee</td>
<td>RSA</td>
<td>RSA is a public-key cryptosystem</td>
</tr>
<tr>
<td>C4C</td>
<td>SAP Cloud for Customer</td>
<td>SAML</td>
<td>Security Assertion Markup Language</td>
</tr>
<tr>
<td>HCP</td>
<td>SAP HANA Cloud Platform</td>
<td>SCIM</td>
<td>System for Cross-domain Identity Management</td>
</tr>
<tr>
<td>HR / HCM</td>
<td>Human Resources, Human Capital Management</td>
<td>SF / SFSF</td>
<td>SuccessFactors</td>
</tr>
<tr>
<td>IAM / IDM</td>
<td>Identity Access Management / Identity Management</td>
<td>SPNEGO</td>
<td>Simple and Protected GSSAPI Negotiation Mechanism (GSSAPI: Generic Security Service Application Program Interface)</td>
</tr>
<tr>
<td>IBP</td>
<td>SAP Integrated Business Planning</td>
<td>SSO</td>
<td>Single Sign-On</td>
</tr>
<tr>
<td>IdP / SP</td>
<td>Identity Provider / Service Provider (SAML)</td>
<td>TCO</td>
<td>Total Cost of Ownership</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
<td>TFA / 2FA</td>
<td>Two-factor-authentication</td>
</tr>
<tr>
<td>OAuth</td>
<td>Open Authorization Framework</td>
<td>X.509</td>
<td>in cryptography, X.509 is a standard for a public key infrastructure (PKI)</td>
</tr>
</tbody>
</table>