Content

1  SAP Cloud Platform Identity Authentication Service. ................................................. 4
  1.1  What is Identity Authentication. ......................................................................... 4
       Product Details. .......................................................................................... 6
       Web-Based Logon Interface. ........................................................................ 7
       Region Availability. ...................................................................................... 8
       Browser Support. ......................................................................................... 9
       Supported Languages. .................................................................................. 11
  1.2  What’s New for Identity Authentication. ............................................................ 12
       Archive. ........................................................................................................ 19
  1.3  Getting Started. .................................................................................................. 32
  1.4  Scenarios. .......................................................................................................... 33
       Business-to-Consumer Scenario. ................................................................. 33
       Business-to-Business Scenario. ................................................................. 36
       Business-to-Employee Scenario. ................................................................. 37
  1.5  Operation Guide. .................................................................................................. 39
       Configuring Applications. .............................................................................. 40
       Configuring Tenant Settings. ......................................................................... 129
       Configuring Password Policies. ..................................................................... 166
       Configuring Privacy Policies. .......................................................................... 173
       Configuring Terms of Use. ............................................................................. 178
       Configuring E-Mail Templates. ...................................................................... 184
       User Management. .......................................................................................... 195
       User Groups. .................................................................................................. 216
       User Provisioning. .......................................................................................... 223
       Managing Administrators. .............................................................................. 237
       Corporate Identity Providers. .......................................................................... 243
       Social Identity Providers. ................................................................................ 268
       Monitoring and Reporting. ............................................................................. 273
       Export Existing Users of a Tenant of SAP Cloud Platform Identity Authentication Service. .......................................................... 281
       SAML 2.0. ........................................................................................................ 283
       OpenID Connect. ............................................................................................. 283
       Troubleshooting for Administrators. ............................................................... 298
  1.6  User Guide. .......................................................................................................... 301
       Two-Factor Authentication. ............................................................................ 303
       Social Authentication. .................................................................................... 306
       Use the Remember Me Option ...................................................................... 308
1.1 Access Applications with Single Sign-On on Mobile Devices. 309
1.2 Change Password. 311
1.3 Troubleshooting for Users. 312
1.4 Developer Guide. 313
1.4.1 API Authentication. 313
1.4.2 API Documentation. 316
1.4.3 Add Logon Overlays in Customer Applications. 396
1.4.4 Configure Clickjacking Protection. 399
1.4.5 Troubleshooting for Developers. 399
1.5 Security. 401
1.6 Security Information. 401
1.7 Data Protection and Privacy. 404
1.8 Integration Scenarios. 409
1.9 Integration with SAP Cloud Platform. 410
1.10 Integration with SAP Web IDE. 417
1.11 Integration with SAP Document Center. 423
1.12 Integration with SAP Identity Management 8.0. 427
1.13 Integration with Microsoft Azure AD. 428
1.14 Get Support. 432
1.15 Updates and Notifications. 432
1 SAP Cloud Platform Identity Authentication Service

1.1 What is Identity Authentication

Secure authentication and single sign-on for users in the cloud.

SAP Cloud Platform Identity Authentication provides you with simple and secure cloud-based access to business processes, applications, and data. It simplifies your user experience through state-of-the-art
authentication mechanisms, secure single sign-on, on-premise integration, and convenient self-service options.

Environment

This service runs in the following environments:

- Neo environment
- Cloud Foundry environment

Features

**Authentication and SSO**

Choose one of the supported authentication methods to protect your application, like Form, SPNEGO, Social or TFA. Use SAML 2.0 protocol to provide SSO for one logon from any device. Integrate your application programmatically using authentication via API.

**Configure Risk-Based Authentication**

Enforce two-factor authentication based on IP ranges, user groups, user type or authentication method to protect access to a business application.

**Delegate Authentication**

Delegate authentication to a 3rd party or on-premise IdP, as default or based on a condition like IdP, e-mail domain, user type or user group, and thus enable SSO across on-premise and the cloud.

**Use API**

Use SCIM REST API to manage users and groups, invite users, customize end-user UI texts in any language.

Prerequisites

To use Identity Authentication, you must obtain a tenant. The tenant represents a single instance of the Identity Authentication that has a specific configuration and data separation.

Tools

For configuration of most features, administrators use the administration console for Identity Authentication, which is a Fiori-based user interface adaptive to most browsers. For more information about the administration console, see Operation Guide [page 39].
# 1.1.1 Product Details

## SAP Cloud Platform Identity Authentication Service Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication with user name and password</td>
<td>Single sign-on to applications with their user name and password.</td>
<td>Scenarios [page 33]</td>
</tr>
<tr>
<td>Single sign-on to applications with their user name and</td>
<td>Users can access multiple cloud applications in the current session by authenticating just</td>
<td>Scenarios [page 33]</td>
</tr>
<tr>
<td>password.</td>
<td>once in the Identity Authentication.</td>
<td></td>
</tr>
<tr>
<td>Social sign-on to applications on SAP Cloud Platform</td>
<td>Users can link their Identity Authentication</td>
<td>Scenarios [page 33], Social Identity Providers [page 268], Social Authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>[page 306].</td>
</tr>
<tr>
<td>Customized branding</td>
<td>Administrators can configure branding styles for UI elements, account with a social</td>
<td>Configure a Tenant Logo [page 134], Configure a Logo for an Application [page 90],</td>
</tr>
<tr>
<td></td>
<td>network account. That way users can be authenticated through a social identity provider,</td>
<td>Define an E-Mail Template Set for an Application [page 96], Configure Registration</td>
</tr>
<tr>
<td></td>
<td>e-mails, and error pages so that they comply with the company’s requirements. account</td>
<td>and Upgrade Forms [page 97]</td>
</tr>
<tr>
<td></td>
<td>with a social network account. That way users can be authenticated through a social</td>
<td></td>
</tr>
<tr>
<td></td>
<td>identity provider, e-mails, and error pages so that they comply with the company’s</td>
<td></td>
</tr>
<tr>
<td></td>
<td>requirements. account with a social network account. That way users can be</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customized privacy policy and terms of use management</td>
<td>Administrators can add customized terms of use and privacy policy, which users have to</td>
<td>Define a Terms of Use Document for an Application [page 182], Define a Privacy</td>
</tr>
<tr>
<td></td>
<td>accept before registering. They are shown on the registration and upgrade forms.</td>
<td>Policy Document for an Application [page 176].</td>
</tr>
<tr>
<td>Customer security policy</td>
<td>Administrators can select a password policy from a list in accordance with the security</td>
<td>Set a Password Policy for an Application [page 168]</td>
</tr>
<tr>
<td>Dedicated customer tenant</td>
<td>Administrators can import new users into Identity Authentication or can update data for</td>
<td></td>
</tr>
<tr>
<td>User import functionality</td>
<td>exiting users.</td>
<td></td>
</tr>
<tr>
<td>User export functionality</td>
<td>Administrators can download information about existing users in the current tenant.</td>
<td>Export Existing Users of a Tenant of SAP Cloud Platform Identity Authentication</td>
</tr>
<tr>
<td>Detailed change logs</td>
<td>Administrators can download a CSV file with information about the history of operations</td>
<td>Service [page 281]</td>
</tr>
<tr>
<td></td>
<td>by tenant administrators.</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>More Information</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>User Management</td>
<td>Administrators can manage the users in the tenant.</td>
<td>User Management [page 195]</td>
</tr>
<tr>
<td>Administrator Management</td>
<td>Administrators can add new administrators and edit administrator authorizations.</td>
<td>Managing Administrators [page 237]</td>
</tr>
<tr>
<td>User Groups</td>
<td>Administrators can create and delete user groups, and assign and unassign users.</td>
<td>User Groups [page 216]</td>
</tr>
<tr>
<td>Corporate User Store</td>
<td>SAP Cloud Platform Identity Authentication service can be configured to use a corporate user store in addition to its own user store.</td>
<td>Configure Connection to a Corporate User Store [page 143]</td>
</tr>
<tr>
<td>Kerberos Authentication</td>
<td>Administrators configure Kerberos authentication to allow users to log on without a username and password when they are in the corporate network.</td>
<td>Configure Kerberos Authentication [page 153]</td>
</tr>
<tr>
<td>Risk-Based Authentication</td>
<td>Administrators define rules for authentication in accordance with the risk.</td>
<td>Configure Risk-Based Authentication [page 82]</td>
</tr>
<tr>
<td>Self-services</td>
<td>Users can use services to maintain or update their user profiles and to log on to applications.</td>
<td>User Guide [page 301]</td>
</tr>
</tbody>
</table>

### 1.1.2 Web-Based Logon Interface

Service providers that delegate authentication to Identity Authentication can use two types of visualization of the web-based user interfaces for the logon pages of their applications.

The two types of visualization of the web-based user interfaces are on a fullscreen of the window and with overlay on top of the application page.

#### Overlay

The use of overlays maintains the application context, by keeping the application page as dimmed background, to provide for minimum disturbance to the work flow. The logon page is open in an iframe over the public page of the application.

#### Fullscreen

The logon page is displayed on fullscreen in the browser when at least one of the following conditions is fulfilled:

- the overlay is not integrated in the application
• the application does not provide a public page
• the user opens directly a protected page of the application

Related Information

Add Logon Overlays in Customer Applications [page 396]

1.1.3 Region Availability

Tenants are deployed on the productive domain accounts.ondemand.com.

The productive domain represents the productive environment. It can be used by customer and partner accounts only.

The productive domain is available on a regional basis, where each region represents the locations of data centers:

• Europe (the central region): accounts.ondemand.com
• North America: accounts.ondemand.com (East)
• Russia: accounts.ondemand.com
• Australia: accounts.ondemand.com

A customer or partner account is associated with a particular data center and this is independent of your own location. For example, you could be located in North America, but operate your account in Europe. Thus you use a data center that is situated in Europe.

Europe and North America regions operate in high availability (HA) mode among the respective data centers. Tenants located in Europe and North America are distributed among the data centers in the regions.

The regions, domains, data centers, and IP addresses are listed below:

<table>
<thead>
<tr>
<th>Region</th>
<th>Domain</th>
<th>Data Center</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td>accounts.ondemand.com</td>
<td>Rot (Germany)/ Amsterdam (Netherlands)</td>
<td>155.56.128.137 / 157.133.170.72</td>
</tr>
<tr>
<td>North America</td>
<td>accounts.ondemand.com</td>
<td>Sterling (United States)/ Toronto (Canada)</td>
<td>157.133.166.69 / 130.214.238.92</td>
</tr>
<tr>
<td>Russia</td>
<td>accounts.ondemand.com</td>
<td>Moscow</td>
<td>130.214.252.71</td>
</tr>
<tr>
<td>Australia</td>
<td>accounts.ondemand.com</td>
<td>Sydney</td>
<td>157.133.168.73</td>
</tr>
</tbody>
</table>
1.1.4 Browser Support

Information on the supported browser version for the administration console, and the end user screens of Identity Authentication.

Supported Browser Versions for Administration Console for SAP Cloud Platform Identity Authentication Service

The Administration Console supports the following browser versions:

- For Microsoft Windows

<table>
<thead>
<tr>
<th>Web Browser</th>
<th>Supported Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Internet Explorer</td>
<td>10 or higher</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>10 (Firefox Extended Support Release - ESR) and latest version</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>latest</td>
</tr>
</tbody>
</table>

- For Macintosh (MAC) OS X

<table>
<thead>
<tr>
<th>Web Browser</th>
<th>Supported Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safari</td>
<td>Safari on MAC OS 10.8 and higher</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>10 (Firefox Extended Support Release - ESR) and latest version</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>latest</td>
</tr>
</tbody>
</table>

**Note**

For security reasons, Safari on MAC OS 10.7 is not supported. Unlike Firefox or Chrome, Safari uses the SSL libraries provided by the operating system. There are known security issues with this version of the SSL libraries.
Supported Browser Versions for SAP Cloud Platform Identity Authentication Service End User Screens

The end user screens, such as logon, forgot password, and so on, of the applications that use Identity Authentication for authentication, support the following browsers:

**Supported Desktop Browsers**

<table>
<thead>
<tr>
<th>Web Browser</th>
<th>Supported Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Internet Explorer</td>
<td>10 or higher</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Latest Version</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>Latest Version</td>
</tr>
<tr>
<td>Safari</td>
<td>Latest Version</td>
</tr>
</tbody>
</table>

**Note**

You cannot use versions 7 and 8 of Microsoft Internet Explorer for some user interfaces (responsive user interfaces).

**Supported Mobile Browsers**

<table>
<thead>
<tr>
<th>Web Browser</th>
<th>Supported Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile or iOS Safari</td>
<td>Latest Version</td>
</tr>
<tr>
<td>Android Browser</td>
<td>Latest Version</td>
</tr>
<tr>
<td>Google Chrome for Android</td>
<td>Latest Version</td>
</tr>
<tr>
<td>Internet Explorer Mobile</td>
<td>11 or higher</td>
</tr>
<tr>
<td>Blackberry Browser</td>
<td>10.0 or higher</td>
</tr>
</tbody>
</table>

The administration console for SAP Cloud Platform Identity Authentication service supports only English language.

The end user screens of the applications that use Identity Authentication for authentication, support the following languages: German, English, Spanish, French, Japanese, Korean, Dutch, Polish, Portuguese, Russian, Chinese, Italian, Welsh, Hebrew, Swedish.
1.1.5 Supported Languages

Information on the supported languages for the administration console, and the end user screens of Identity Authentication.

Supported Languages for Administration Console

The administration console for SAP Cloud Platform Identity Authentication service supports only English language.

Supported Languages for SAP Cloud Platform Identity Authentication Service End User Screens

The end user screens of the applications that use Identity Authentication for authentication, support the following languages: German, English, Spanish, French, Japanese, Korean, Dutch, Polish, Portuguese, Russian, Chinese, Italian, Welsh, Hebrew, Swedish.

<table>
<thead>
<tr>
<th>Name of Language</th>
<th>ID of Language (ISO 639-1 Format)</th>
</tr>
</thead>
<tbody>
<tr>
<td>German</td>
<td>de</td>
</tr>
<tr>
<td>English</td>
<td>en</td>
</tr>
<tr>
<td>Spanish</td>
<td>es</td>
</tr>
<tr>
<td>French</td>
<td>fr</td>
</tr>
<tr>
<td>Japanese</td>
<td>ja</td>
</tr>
<tr>
<td>Korean</td>
<td>ko</td>
</tr>
<tr>
<td>Dutch</td>
<td>nl</td>
</tr>
<tr>
<td>Polish</td>
<td>pl</td>
</tr>
<tr>
<td>Portuguese</td>
<td>pt</td>
</tr>
<tr>
<td>Russian</td>
<td>ru</td>
</tr>
<tr>
<td>Chinese</td>
<td>zh</td>
</tr>
<tr>
<td>Italian</td>
<td>it</td>
</tr>
<tr>
<td>Welsh</td>
<td>cy</td>
</tr>
<tr>
<td>Hebrew</td>
<td>he</td>
</tr>
<tr>
<td>Swedish</td>
<td>sv</td>
</tr>
</tbody>
</table>

The language for the end user screens is set according to the following order of priorities:

1. If the locale is set, the end user screen uses the language set there.
   Setting the locale, sets an Identity Authentication cookie. This cookie is used for all the applications in this session that are configured to use Identity Authentication as identity provider.
The locale can be set in either of the following ways:

- The locale is communicated to Identity Authentication by adding a locale parameter to `SAP_IDS.js`.

  ```html
  ```

- The locale is communicated to Identity Authentication by a direct GET request.

  ```html
  ```

2. If the locale is not set, the end user screen uses the language that the user’s browser is set to.

   - If the language is not in the list of supported languages, the end user screen uses English instead.
   - If the language is in the list of supported languages, the end user screen uses this language.

### 1.2 What's New for Identity Authentication

This page lists the release notes of SAP Cloud Platform Identity Authentication service for 2018. To see the release notes for the previous years, visit [Archive](#).

To get notifications for the new features and fixes every release, subscribe at the [SAP Community wiki](#) by choosing the Watch icon.

#### November 13 2018 - Identity Authentication

**New**

**Customer Documents**

Tenant administrator can view the terms of use and privacy policy documents, and the e-mail templates uploaded in the administration console. See [View a Terms of Use Document](#), [View a Privacy Policy Document](#), and [View E-Mail Template Document](#).
October 30 2018 - Identity Authentication

New
Corporate IdPs
Added *IP Range* in the rules for conditional authentication. See *Configure Conditional Authentication for an Application* [page 119].

New
Corporate IdPs
Corporate IdP can decide whether to use the existing SSO session, or create a new one for every application. See *Forward All SSO Requests to Corporate IdP* [page 263].

New
SAML 2.0
You can add SOAP SLO endpoint when configuring SAML 2.0 application in the administration console. The SOAP Endpoint is called only when the user password is changed via the administration console, forgot password triggered by the user, or API call. See *Configure SAML 2.0 Service Provider* [page 55].

New
SAML 2.0
You can see the index number of the endpoint of the assertion consumer service of the service provider as the target of the SAML response in the administration console. See *What's New for Identity Authentication* [page 12].

25 September 2018 - Identity Authentication

New
Tenant Settings
You can configure your mail server for the e-mails sent for the different application processes. Once you configure the mail server, all e-mails will go through this configuration. See *Configure Mail Server for Application Processes* [page 161].

New
Customer Documents
Tenant administrator can upload terms of use and privacy policy documents, and e-mail templates in Arabic, Croatian, Czech, Slovenian, Greek, Ukrainian, and Slovak. See *Configuring Terms of Use* [page 178], *Configuring Privacy Policies* [page 173], and *Configuring E-Mail Templates* [page 184].
4 September 2018 - Identity Authentication

New
Default Attributes
You can configure attributes with dynamic values to be added into the assertions for the SAML 2.0 applications. See Configure the Default Attributes Sent to the Application [page 71].

New
Conditional Authentication
You can use non-identifier based authentication without having to enter their logon alias or password. See Configure Conditional Authentication for an Application [page 119].

21 August 2018 - Identity Authentication

New
Single Sign-On
Identity Authentication supports OpenID Connect standard for authentication. You can choose what standard to use your application, SAML 2.0, or OpenID Connect. See Create OpenID Connect Application [page 45] and Configure OpenID Connect Application [page 59].

New
REST API
Extended the User Management REST API. You can retrieve information about an SP user in a tenant via API. See SP User Information [page 325].

31 July 2018 - Identity Authentication

New
SAML 2.0
You can set a name ID format via the administration console to be sent to the corporate IdP. The options are None, Default, Unspecified, or E-Mail. See (Optional) Configure the Name ID Format Sent to the Corporate IdP [page 259].
3 July 2018 - Identity Authentication

New

SCIM REST API

Extended Manage Users SCIM REST API with the following attributes: middleName, telephoneVerified, telephoneVerificationAttempts, passwordPolicy, passwordStatus, passwordFailedLoginAttempts, otpFailedLoginAttempts, termsOfUse, privacyPolicy, socialIdentities, passwordLoginTime, loginTime, passwordSetTime. For more information, see Users Search [page 337], User Resource [page 343], Create User Resource [page 348], and Update User Resource [page 358].

Announcement

Social Identity Providers

You should provide your Callback URL in apps.twitter.com. See Configure Social Identity Providers [page 269].

Enhancement

Conditional Authentication

Improved user experience for the conditional authentication flow. After the first logon a persistent cookie is stored in the browser of the user. At consecutive logons, the user is redirected to the corporate logon screen, without the need to provide user identifier first. See Configure Conditional Authentication for an Application [page 119].

15 June 2018 - Identity Authentication

Announcement

Certificate Renewals

On 25 June 2018, certificates on the following regions will be renewed:

- US East (Sterling / Toronto)
- Europe (Rot/ Amsterdam)

The renewed certificates will be issued by DigiCert CA (DigiCert Global Root CA).
16 May 2018 - Identity Authentication

**New**

**User Management**

Extended the user information for terms of use and privacy policy documents visible in the administration console for Identity Authentication in the format `<document name><document version><time stamp>`. For more information about how to view the user information in the administration console, see List and Edit User Details [page 205].

---

**Announcement**

**Availability**

Identity Authentication is now available in two new regions - Russia and Australia. See Region Availability [page 8].

---

**New**

**SCIM REST API**

Extended the Users Search SCIM REST API with the option to filter by groups. For more information about how to view the user information in the administration console, see Users Search [page 337].

---

**New**

**SCIM REST API**

Extended the Groups Search SCIM REST API with the option to paginate the response. For more information about how to view the user information in the administration console, see Groups Search [page 370].

---

**New**

**Monitoring and Reporting**

You can generate Client ID and Client Secret to call the audit log retrieval API to view the audit logs for changes in the personal data in SAP Cloud Platform Identity Authentication service. See Access Audit Logs [page 274].

---

11 April 2018 - Identity Authentication

**New**

**Branding and Layout**

Protecting Self-Registration with Phone Verification [page 101].
New Authentication
You can configure applications to require e-mail verification. See You can configure phone verification for an application. See Enable E-Mail Verification [page 89].

21 March 2018 - Identity Authentication

New Customer Documents
You can configure phone verification for an application. See Tenant administrator can upload terms of use and privacy policy documents, and e-mail templates in Romanian, Hungarian, Serbian, Azerbaijani, Bulgarian. See Configuring Terms of Use [page 178], Configuring Privacy Policies [page 173], and Configuring E-Mail Templates [page 184].

New Profile Page
A user can view the signed Terms of Use and Privacy Policy documents. See User Guide [page 301].

New Profile Page
Extended the data in the Your Profile Information screen with all user attributes that are kept in SAP Cloud Platform Identity Authentication service. See User Guide [page 301].

New Profile Page
A user can download all the attributes that are kept for him or her in SAP Cloud Platform Identity Authentication service. See User Guide [page 301].

New REST API
Extended the User Management REST API. You can delete SP user in a tenant via API. See SP User Deletion [page 328].
8 March 2018 - Identity Authentication

New

Authenticating Identity Provider
You can allow users to log on via SAP Cloud Platform Identity Authentication service when a corporate identity provider (IdP) is selected as default. See Configure Logon via Identity Authentication when a Corporate IdP is Chosen as Default [page 114].

New

SCIM REST API
SCIM REST API implementation of Identity Authentication was extended. You can create, update, and delete user groups in a tenant. See Create Group Resource [page 375], Update Group Resource [page 377], and Delete Group Resource [page 380].

Announcement

Social Identity Providers
You should update your Valid OAuth redirect URIs list in the Facebook Login Settings by March 14, 2018. See Configure Social Identity Providers [page 269].

22 February 2018 - Identity Authentication

New

SAML 2.0 Configuration
You can define a different location to which logout response messages should be sent. See Configure Trust [page 55].

6 February 2018 - Identity Authentication

New

Conditional Authentication
You can define rules for authenticating identity provider according to e-mail domain, user type, and user group. See Configure Conditional Authentication for an Application [page 119].
9 January 2018 - Identity Authentication

New
Branding and Layout
Implemented Google reCAPTCHA to protect the self-registration form against machine registrations. See Protecting Application Forms with Google reCAPTCHA [page 107].

New
End User Screens
Added Swedish to the supported languages for end user screens. See Supported Languages [page 11].

New
Customer Documents
Tenant administrator can upload terms of use and privacy policy documents, and e-mail templates in Swedish. See Configuring Terms of Use [page 178], Configuring Privacy Policies [page 173], and Configuring E-Mail Templates [page 184].

New
REST API
Added Swedish to the default languages for the predefined master data for each resource, and the predefined texts and messages for end user screens available per tenant in Identity Authentication. See Change Tenant Texts REST API [page 382] and Change Master Data Texts REST API [page 388].

Archived Release Notes

- 2017 [page 20]
- 2016 [page 25]
- 2015 [page 28]
- 2014 [page 31]

1.2.1 Archive

- Release Notes 2017 [page 20]
- Release Notes 2015 [page 28]
- Release Notes 2014 [page 31]
1.2.1.1 Release Notes 2017

The following document provides information about what was released in 2017. For more information about the latest release notes, see What’s New for Identity Authentication [page 12].

29 November 2017 - Identity Authentication

**New**

**Risk-Based Authentication**

Extended the configuration of risk-based authentication with the Authentication Method and User Type options. See Configure Risk-Based Authentication [page 82].

**New**

**User Provisioning**

You can provision users to SAP Cloud Platform Identity Provisioning service instances. For more information, see Configure Identity Provisioning Target Systems for User Provisioning [page 226].

1 November 2017 - Identity Authentication

**New**

**SCIM REST API**

SCIM REST API implementation of Identity Authentication was extended. You can list all the groups, and list the details of a specific group in a tenant. See Groups Search [page 370], and Group Resource [page 373].

18 October 2017 - Identity Authentication

**New**

**IdP-Initiated SSO**

You can enable IdP-initiated logon from all configured corporate identity providers. See Enable IdP-Initiated SSO from All Corporate Identity Providers [page 127].
New SCIM REST API

SCIM REST API implementation of Identity Authentication was extended. You can list all the groups, and list the details of a specific group in a tenant. See Groups Search [page 370], and Group Resource [page 373].

21 September 2017 - Identity Authentication

New E-Mail Templates

You can create and configure custom e-mail template sets via the administration console for SAP Cloud Platform Identity Authentication service. See Configuring E-Mail Templates [page 184].

22 August 2017 - Identity Authentication

New SAML 2.0

You can set a default name ID format via the administration console; the options are Unspecified or E-Mail. See (Optional) Configure the Default Name ID Format Sent to the Application under Configure the Name ID Attribute Sent to the Application [page 67].

7 August 2017 - Identity Authentication

New Password Status

Tenant administrators can unlock locked accounts. See Unlock User Password [page 211].

New Password Status

Tenant administrators can trigger the sending of an e-mail to the user with information how to reset the password. See Send Reset Password E-Mail [page 213].
New
Password Status
Tenant administrators can reset the counter for the number of e-mails with reset password information that can be sent to the user. See Reset Counter for E-Mail Sending [page 214].

New
Password Status
Tenant administrators can set initial password for the user. See Set Initial Password [page 215].

12 June 2017 - Identity Authentication

New
Session Timeout
Tenant administrators can configure the duration of the identity provider (IdP) session via the administration console for Identity Authentication. See Configure Session Timeout [page 136].

Enhancement
SAML 2.0 Configuration
Tenant administrators can select the digest algorithm for signing outgoing messages. See step 7 in Configure Trust [page 55].

15 May 2017 - Identity Authentication

Announcement
Failover Mechanism Improvement
As part of the failover mechanism improvement for Identity Authentication, we will add a new IP address (157.133.170.72) for the domain in Europe. If you have whitelisted the current IP, you also have to whitelist the new IP for the corresponding scenarios to work. See Region Availability [page 8].
11 May 2017 - Identity Authentication

**Enhancement**

**User Creation**

Tenant administrators can set the user type at user creation via the administration console for Identity Authentication. See [Create a New User](#).
7 March 2017 - Identity Authentication

Enhancement
SAP Cloud Platform Identity Authentication service Rebranding
SAP Cloud Identity service is renamed as SAP Cloud Platform Identity Authentication service (in short, Identity Authentication). The renaming includes changes in the following:

- UI texts, labels, and titles
- messages
- e-mail templates
- tenant logo

Enhancement
New SAP Help Portal
Updated the documentation links in the administration console for Identity Authentication. The updated links lead to the Identity Authentication documentation in the New SAP Help Portal.

10 January 2017 - Identity Authentication

Enhancement
System Applications
Certain configuration options for the system applications are read-only. See Configure Trust [page 55], Configure the User Attributes Sent to the Application [page 64], Configure the Name ID Attribute Sent to the Application [page 67], Configure the Default Attributes Sent to the Application [page 71], and Choose Default Identity Provider for an Application [page 112].

Enhancement
Log On Screen Improvement
Redesigned the Log On screen of SAP Cloud Platform Identity Authentication service, changing the place of the Forgot password link.

Parent topic: Archive [page 19]

Related Information

Release Notes 2015 [page 28]
Release Notes 2016

1.2.1.2 Release Notes 2016

Release Notes
The following table provides information about what was released in 2016. For more information about the latest release notes, see What’s New for Identity Authentication [page 12]:

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-12-12</td>
<td>- Added search field for the master lists in the following tiles in the administration console:</td>
</tr>
<tr>
<td></td>
<td>○ Import Users</td>
</tr>
<tr>
<td></td>
<td>○ Applications</td>
</tr>
<tr>
<td></td>
<td>○ Terms of Use Documents</td>
</tr>
<tr>
<td></td>
<td>○ Privacy Policy Documents</td>
</tr>
<tr>
<td></td>
<td>○ Corporate Identity Providers</td>
</tr>
<tr>
<td></td>
<td>- Changed the name of the system application that contains the configurations of the Profile Page to User Profile. For more information about the system applications, see Configuring Applications [page 40].</td>
</tr>
<tr>
<td>2016-11-17</td>
<td>- Extended SCIM REST API with new attributes in accordance with the Custom Attributes Schema Extension. Tenant administrators at Identity Authentication can store, read, create, and update customer specific data in up to 10 custom attributes. For more information, see SCIM REST API [page 334].</td>
</tr>
<tr>
<td></td>
<td>- Added a warning message that appears when the tenant administrator chooses a system application for configuration in the administration console for Identity Authentication. For more information about the application types, see Configuring Applications [page 40].</td>
</tr>
<tr>
<td>2016-10-26</td>
<td>- The screen that appears after successful authentication is simplified.</td>
</tr>
<tr>
<td>2016-10-10</td>
<td>- Extended the attributes that can be sent to the application in the SAML 2.0 assertion with Language, Cost Center, Department, Division, and Employee Number. For more information about the assertion attributes, see Configure the User Attributes Sent to the Application [page 64].</td>
</tr>
<tr>
<td>2016-10-03</td>
<td>- Tenant administrators can change the name format of the identity provider in the administration console for Identity Authentication. For more information, see Tenant SAML 2.0 Configuration [page 130].</td>
</tr>
<tr>
<td>2016-09-14</td>
<td>- Tenant administrators can create, configure, and set a custom password policy for scenarios where Identity Authentication is the authenticating authority. For more information, see Configure Custom Password Policy [page 170].</td>
</tr>
<tr>
<td>2016-08-30</td>
<td>- The SAPUI5 extension SAP Fiori for Tools is applied to the administration console for Identity Authentication. It includes controls like Side Navigation, Tool Header, and Block Layout. Navigation entries in the administration console have an icon, and features belonging to the same category are grouped together.</td>
</tr>
<tr>
<td>2016-08-16</td>
<td>- Identity Authentication protects the applications against clickjacking when using embedded frames for the logon pages. For more information, see Configure Clickjacking Protection [page 399].</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>2016-08-05</td>
<td>● Tenant administrator can change user type via the administration console for Identity Authentication. For more information, see <em>List and Edit User Details</em> [page 205].&lt;br&gt;● Tenant administrator can upload terms of use and privacy policy documents, and e-mail templates in all supported languages. For more information, see <em>Configuring Terms of Use</em> [page 178], <em>Configuring Privacy Policies</em> [page 173], and <em>Define an E-Mail Template Set for an Application</em> [page 96].</td>
</tr>
<tr>
<td>2016-07-18</td>
<td>● The master data texts of <em>Identity Authentication</em> can be changed and updated via API. For more information, see <em>Change Master Data Texts REST API</em> [page 388].&lt;br&gt;● <em>Identity Authentication</em> provides support for languages written in Right-To-Left (RTL) direction. For more information about the supported languages, see <em>Supported Languages</em> [page 11].</td>
</tr>
<tr>
<td>2016-07-04</td>
<td>● Extended the user import via CSV file with the <code>language</code> column. Tenant administrator can specify the language of the user via CSV file import. The user receives the activation e-mail in that language. For more information, see <em>Import or Update Users for a Specific Application</em> [page 196].</td>
</tr>
<tr>
<td>2016-06-20</td>
<td>● You can specify a link to be used by the application to redirect the user after successful logout when <em>Identity Authentication</em> acts as an IdP proxy. For more information, see <em>Configure Logout URL</em> [page 255].&lt;br&gt;● You can change the user attributes taken from Microsoft Active Directory. You can also add additional attributes that are defined in the SCIM Enterprise User Schema Extension. For more information, see <em>Configure SAP Cloud Platform</em> [page 143].</td>
</tr>
<tr>
<td>2016-06-06</td>
<td>● Tenant administrators can edit the E-Mail information in the administration console for <em>Identity Authentication</em>. For more information, see <em>List and Edit User Details</em> [page 205].&lt;br&gt;● Added new attributes that are sent to the remote system in user provisioning. For more information about the supported attributes and the mapping between <em>Identity Authentication</em> and SAP Jam, see <em>Provision Users to Target Systems</em> [page 228].</td>
</tr>
<tr>
<td>2016-05-25</td>
<td>● Country field in registration and upgrade form is required when Zip/Postal Code is filled in. For more information, see <em>Configure Registration and Upgrade Forms</em> [page 97].&lt;br&gt;● Extended SCIM REST API with the possibility to create and update users with no password and no activation e-mail sending. Added new attributes: <code>sendMail</code>, <code>mailVerified</code>. For more information, see <em>SCIM REST API</em> [page 334].&lt;br&gt;● Extended the SCIM REST API with <code>corporateGroups</code> attribute. For more information, see <em>SCIM REST API</em> [page 334].</td>
</tr>
<tr>
<td>2016-05-10</td>
<td>● Extended SCIM REST API with new attributes: <code>employeeNumber</code>, <code>costCenter</code>, <code>organization</code>, <code>division</code>, <code>department</code>, <code>manager</code>, in accordance with the Enterprise User Schema Extension. For more information, see <em>SCIM REST API</em> [page 334].&lt;br&gt;● Supports Employee Number as NameID attribute. For more information, see <em>Configure the Name ID Attribute Sent to the Application</em> [page 67].&lt;br&gt;● Added Italian and Welsh to the supported languages for end user screens. For more information, see <em>Supported Languages</em> [page 11].</td>
</tr>
<tr>
<td>2016-04-26</td>
<td>● Extended SCIM REST API with <code>passwordStatus</code>, <code>userType</code>, <code>sourceSystem</code>, and <code>socialIdentities</code> attributes. For more information, see <em>SCIM REST API</em> [page 334].&lt;br&gt;● Extended the number of user attributes with a new section <em>Employee Information</em> in <em>User Details</em> view of the administration console. For more information, see <em>List and Edit User Details</em> [page 205].</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 2016-04-11 | ● The tenant texts of Identity Authentication can be changed and updated via API. For more information, see Change Tenant Texts REST API [page 382].  
  ● You can define rules for authentication for the administration console for Identity Authentication according to different risk factors. For more information, see Configure Risk-Based Authentication [page 82]. |
| 2016-03-31 | ● Tenant administrators can check if the SAP Jam Target System is configured properly by testing the connection. For more information, see User Provisioning [page 223].  
  ● Tenant administrators can delete a selected target system or several target systems in a tenant of SAP Cloud Platform Identity Authentication service. For more information, see Delete Target System [page 235].  
  ● Tenant administrators can search users in the administration console choosing between simple and advanced search. For more information, see Search Users [page 203]. |
| 2016-03-20 | ● Tenant administrators can delete a selected user group in a tenant of Identity Authentication. For more information, see Delete User Groups [page 222]. |
| 2016-02-29 | ● Tenant administrators can provision users to SAP Jam instances. For more information, see User Provisioning [page 223].  
  ● Tenant administrators can delete a selected application in a tenant of Identity Authentication. For more information, see Delete Applications [page 53].  
  ● Tenant administrators can delete a selected corporate identity provider in a tenant of Identity Authentication. For more information, see Delete Corporate Identity Providers [page 261]. |
| 2016-02-15 | ● Tenant administrators can assign user groups to corporate identity providers so that only users part of these groups can access the application. For more information, see the Assign User Groups to Corporate Identity Providers section in Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 266]. |
| 2016-02-01 | ● SCIM REST API implementation of Identity Authentication is updated and supports full set of attributes to create, update, and delete user resources. For more information, see Create User Resource [page 348], Update User Resource [page 358], and Delete User Resource [page 368].  
  ● Tenant administrators can enable or disable a check if a user authenticated by a corporate identity provider exists in the cloud user store of Identity Authentication. For more information, see the Enable Identity Federation with Identity Authentication User Store section in Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 266]. |
| 2016-01-18 | ● Tenant administrators can define rules for authentication in accordance with the risk. For more information, see Configure Risk-Based Authentication [page 82].  
  ● Tenant administrators can enable or disable the reload of the parent page of the application after a successful logon. For more information, see Enable or Disable Reload Parent Page Option [page 95].  
  ● SCIM REST API implementation of Identity Authentication supports create, update, and delete of user resources. For more information, see Create User Resource [page 348], Update User Resource [page 358], and Delete User Resource [page 368]. |

Parent topic: Archive [page 19]
### Related Information

- Release Notes 2017 [page 20]
- Release Notes 2015 [page 28]
- Release Notes 2014 [page 31]

### 1.2.1.3 Release Notes 2015

Release Notes

The following table provides information about what was released in 2015. For more information about the latest release notes, see What’s New for Identity Authentication [page 12]:

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2015-12-08 | - Tenant administrators can delete one or more corporate identity providers in a tenant of Identity Authentication. For more information, see Delete Corporate Identity Providers [page 261].  
- Added a new tenant administrator’s role - Manage Groups. For more details how to assign administrator roles, see Edit Administrator Authorizations [page 241]. |
| 2015-11-23 | - Tenant administrators can add systems in the administration console for Identity Authentication to act as administrators. For more information, see Add System as Administrator [page 240].  
- Tenant administrators can configure the validity of the link sent to a user in the different application processes. For more information, see Configure E-Mail Link Validity [page 135].  
- Tenant administrators can edit the user details information in the administration console for Identity Authentication. For more information, see List and Edit User Details [page 205]. |
| 2015-10-27 | - Tenant administrators can view monthly statistics on the user logons. For more information, see View Usage Statistics [page 273].  
- Added optional parameter in the User Management REST API allowing the option not to send the activation e-mail. For more information, see User Registration [page 320].  
- Redesigned end user interfaces providing usability improvements and fixes. The UI now works fine in both an iFrame and when shown in full browser window. Improved responsive behavior and markup, and refactored CSS for easier implementation and maintenance. |
| 2015-10-12 | - Added a new tenant administrator’s role - Manage Users. For more details how to assign administrator roles, see Edit Administrator Authorizations [page 241].  
- Tenant administrators can delete one or more user groups in a tenant of Identity Authentication. For more information, see Delete User Groups [page 222].  
- Tenant administrators can change the certificate used by the identity provider to digitally sign the messages for the applications. For more information, see Tenant SAML 2.0 Configuration [page 130].  
- Tenant administrators can configure Kerberos authentication for Identity Authentication to allow users to log on without username and password when they are in the corporate network. For more information, see Configure Kerberos Authentication [page 153]. |
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-09-28</td>
<td>• Tenant administrators can [Configure Trusted Domains](page 138) in the administration console for Identity Authentication</td>
</tr>
</tbody>
</table>
| 2015-09-14 | • Users can use *Remember me* option to log in to applications. For more details, see [Use the Remember Me Option](page 308).  
  • Users can access applications with single sign-on on mobile devices. For more details, see [Access Applications with Single Sign-On on Mobile Devices](page 308). See also [Mobile Single Sign-On](page 129).  
  • Administrators can list the users that are assigned to a given user group. For more details, see [List Users in User Groups](page 219). |
| 2015-08-31 | • Tenant administrator can disable IdP-Initiated process on tenant level. For more information see, [Configure IdP-Initiated SSO](page 162).  
  • SCIM REST API implementation of Identity Authentication supports:  
    ○ pagination and search by more than one attribute, and one attribute can be included into the filter more than one time  
    ○ tenant administrator can retrieve a known user  
    ○ location attribute is returned and in the search results  
  For more information, see [SCIM REST API](page 334). |
| 2015-08-04 | • Tenant administrator can list user groups in the tenant. For more information, see [List User Groups](page 218).  
  • Tenant administrator can create new user groups via the administration console for Identity Authentication. For More information, see [Create a New User Group](page 217).  
  • Tenant administrator can assign or unassign groups for a user via the administration console for Identity Authentication. For more information, see [Assign Groups to a User](page 220), [Unassign Users from Groups](page 221).  
  • Tenant administrator can add users to user groups via the `groups` column in the CSV file. For more information, see [Import or Update Users for a Specific Application](page 196).  
  • Applications can search users by attribute via the SCIM REST API. For more information, see [Users Search](page 337).  
  • Tenant administrator configures the `groups` attribute to be sent with the SAML 2.0 assertion. For more information, see [Configure the User Attributes Sent to the Application](page 64). |
| 2015-07-06 | • Tenant administrator creates new users in the administration console for Identity Authentication. For more information, see [Create a New User](page 202).  
  • Tenant administrator can configure social providers separately. For more information, see [Configure Social Identity Providers](page 269). |
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2015-06-22 | - When an application uses HTTP basic authentication for API calls, the password locks for 60 min after 5 failed logon attempts with wrong value.  
- When searching for users, the system displays the first 20 users in the tenant sorted by their user ID number. If the users are more than 20, the list can be expanded. For more information, see [Search Users](#) [page 203].  
- Tenant administrator deletes users in the administration console for Identity Authentication. For more information, see [Delete Users](#) [page 207].  
- You can now configure Identity Authentication to connect to your corporate user store to request additional user information. That might be necessary when the information about your users is not available in the user store of Identity Authentication. For more information, see [Configure Connection to a Corporate User Store](#) [page 143]. |
| 2015-06-08 | - Administrator sets a password for HTTP basic authentication when Identity Authentication API is used. For more information, see [Configure Credentials for HTTP Basic Authentication](#) [page 79].  
- Administrator can set custom attributes with a CSV file. For more information, see [Import or Update Users for a Specific Application](#) [page 196]. |
| 2015-05-26 | - Identity Authentication adds additional user attributes to the standard set of user attributes:  
  - on the user registration form  
  - in the assertion attributes configuration in the administration console  
  - in the SAML 2.0 assertions  
  For the full list of the attributes, see [Configure Registration and Upgrade Forms](#) [page 97].  
- Application sets custom attributes via the user registration service. For more details, see [User Registration](#) [page 320].  
- Tenant administrator configures custom attributes to be sent with the SAML 2.0 assertion. For more information, see [Configure the User Attributes Sent to the Application](#) [page 64]. |
| 2015-04-13 | - Administrator configures applications for two-factor authentication.  
  **i Note**  
  This functionality has been updated. Now it is part of the [Risk Based Authentication](#). For more information, see [Configure Risk-Based Authentication](#) [page 82].  
- Administrator deactivates all user mobile devices that generate passcodes for applications with two-factor authentication. For more information, see [Deactivate User Devices for TOTP Two-Factor Authentication](#) [page 210].  
- Administrator unlocks user passcode for two-factor authentication. For more information, see [Unlock User TOTP Passcode](#) [page 210].  
- User activates and deactivates mobile devices that generate passcodes for access to applications with two-factor authentication. For more information, see [Two-Factor Authentication](#) [page 303], [Activate a Device for TOTP Two-Factor Authentication](#) [page 303], [Deactivate Devices Configured for TOTP Two-Factor Authentication](#) [page 305]. |
### Date  | Description
--- | ---
2015-02-19 | Add users as administrators in the administration console for Identity Authentication. For more information, see Add Administrators [page 238].
2015-02-16 | List administrators in the administration console for Identity Authentication. For more information, see List Administrators [page 237].
2015-02-02 | Edit administrators’ roles in the administration console for Identity Authentication. For more information, see Edit Administrator Authorizations [page 241].
2015-03-16 | Configure trusted identity provider in the administration console for Identity Authentication. For more information, see Configure Trust with Corporate Identity Provider [page 256].
2015-03-02 | Delete one or more applications in a tenant of Identity Authentication. For more information, see Delete Applications [page 53].
2015-03-02 | Configure and visit the Home URL of an application. For more information, see Configure an Application’s Home URL [page 50], Visit an Application’s Web Page [page 52].
2015-03-02 | Import or update users for an application, and send activation e-mails. For more information, see Import or Update Users for a Specific Application [page 196].
2015-03-30 | Choose an identity provider for a specific application. The tenant administrator can choose between the default identity provider and a corporate identity provider. For more information, see Choose Default Identity Provider for an Application [page 112].
2015-03-30 | Search, view, and list the users, and view detailed information about them in the administration console for Identity Authentication. For more information, see List and Edit User Details [page 205].

### Related Information

- Release Notes 2017 [page 20]
- Release Notes 2014 [page 31]

### 1.2.1.4 Release Notes 2014

Release Notes

The following table provides information about what was released in 2014. For more information about the latest release notes, see What’s New for Identity Authentication [page 12]:


Parent topic: Archive [page 19]
Date | Description
--- | ---
2014-12-08 | • Change the tenant’s display name. For more information, see Change a Tenant’s Display Name [page 139].
| • Users created via CSV upload receive activation mail.
| • Application specific logo. For more information, see Configure a Logo for an Application [page 90].
| • Global tenant logo. For more information, see Configure a Tenant Logo [page 134].
| • Configure SAML 2.0 trust by uploading metadata or by entering the service provider’s information manually. For more information, see Configure Trust [page 55].
| • Set up the user attributes that are sent to the application in the SAML 2.0 assertion. For more information, see Configure the User Attributes Sent to the Application [page 64].
| • Configure attributes with default values for the application. For more information, see Configure the Default Attributes Sent to the Application [page 71].
| • Choose which user attributes to be on the registration and upgrade forms of the application. For more information, see Configure Registration and Upgrade Forms [page 97].
| • Upload certificate for REST API authentication.
| • Log on with social network accounts. For more information, see Enable or Disable Social Sign-On for an Application [page 76], Configure Social Identity Providers [page 269].

2014-09-01 | • Initial release.

Parent topic: Archive [page 19]

Related Information

Release Notes 2017 [page 20]
Release Notes 2015 [page 28]

1.3 Getting Started

SAP Cloud Platform Identity Authentication service is offered as part of some SAP Cloud Platform packages or as a standalone product.

For more information how to get Identity Authentication, see SAP Cloud Platform Pricing and Packaging Options, or contact your SAP sales representative.

After you purchase a subscription for the Identity Authentication tenant, you receive an e-mail. The e-mail contains a link to the landing page of the administration console for Identity Authentication. You can confirm the registration of your first administrator user.
1.4 Scenarios

SAP Cloud Platform Identity Authentication service supports scenarios for consumers (business-to-consumer scenarios), for partners (business-to-business scenarios), and for employees (business-to-employee scenarios).

1.4.1 Business-to-Consumer Scenario

The business-to-consumer scenario is related to any actions performed by the consumer, such as registration to applications and consumer retailing. In this scenario, administrators facilitate the consumer processes, but they do not act on the consumer’s behalf.

This scenario includes the following features:

- Authentication with user name and password
- A secure single sign-on to cloud applications
- Social sign-on to cloud applications
- Self-registration of consumers
- Invitation of consumers
- Branding elements on all the forms for logon, registration, password update, and account activation
Example

Michael Adams is an administrator at retail company A. He would like to configure his system such that users can register on their own and then purchase from the company’s site. Michael also wants to allow users to access his Company A Purchasing application by self-registration. To do this, Michael logs on to the administration console for SAP Cloud Platform Identity Authentication service, navigates to Applications >> Company A Purchasing >> Authentication and Access >> User Application Access. He selects the Public radio button to allow user self-registration for his Company A Purchasing application. Michael also allows users to authenticate through a social provider by providing the keys and secrets for the social providers after he chooses the Social Identity Providers tile. He then enables social sign-on by choosing the Applications tile and navigating to Company A Purchasing >> Authentication and Access. Furthermore, Michael configures custom terms of use and privacy policy for the Company A Purchasing application. To do this, he chooses the Terms of Use Documents and Privacy Policy Documents tiles and adds the new plain text files in English language versions. He then returns to Applications >> Company A Purchasing view and sets the new terms of use and privacy policy documents for the application under the Authentication and Access tab.

Michael also decides to use a custom branding style for the buttons on his logon and registration forms. To do this, he opens the Branding Style page under the Branding and Layout tab in the Application view and selects the branding styles.

Donna Moore is a customer who wants to purchase goods from company A for the first time. When she accesses company A’s application, she is redirected to the company’s logon page. Because she is not registered yet, she has to choose the Register Now link to start the registration process. A registration form then appears, prompting Donna to enter her names, e-mail, and address and to accept the organization’s terms of use and privacy policy. When she submits the form, she receives an e-mail with instructions on how to activate her registration. Once she activates her registration, she is able to log on to the retailing application with her user credentials.
1. Configures user access to the application.
2. Registers or provides credentials.
3. Delegates self-registration or authentication.
4. Activates account.
5. Confirms authentication.

**Related Information**

- Operation Guide [page 39]
- Developer Guide [page 313]
- Configure User Access to the Application [page 87]
- Configuring Privacy Policies [page 173]
- Configuring Terms of Use [page 178]
- Configure a Branding Style for an Application [page 93]
1.4.2 Business-to-Business Scenario

The business-to-business scenario is related to services for business partners. Unlike the business-to-consumer scenario, consumer self-registration is not allowed, and the administrator of the company is usually the one that triggers the user registration process. The administrator invites partners or registers them on their behalf.

This scenario includes the following features:

- Authentication with user name and password
- A secure SSO to cloud applications
- Social sign-on to cloud applications
- Invitation of partners by administrators
- On-behalf registration of partners by administrators
- Branding elements on all the forms for logon, password update, and account activation
- Customized privacy policy and terms of use documents
- Partner security policy
- User import and export

Example

Donna Moore is a tenant administrator at company A. This company is a goods and services retailer. She would like to invite five transportation companies to join her organization in helping the distribution of goods and services to distant locations. The distributors will purchase from the Company A Distribution application. For this purpose, Donna registers these distributors on their behalf, logs on to the administration console for Identity Authentication, navigates to Applications ➔ Company A Distribution page, and chooses Authentication and Access ➔ User Application Access. She selects the Private radio button in order to restrict access to just these users. The partners then activate their registration via the on-behalf registration e-mail and can log on to the Company A Distribution application.
1. Invites or registers partner.
2. Activates account.
3. Provides credentials.
4. Delegates authentication.
5. Confirms authentication.

Related Information

Operation Guide [page 39]
Developer Guide [page 313]
Configure User Access to the Application [page 87]

1.4.3 Business-to-Employee Scenario

The business-to-employee scenario is related to services for employees of an organization. Employees can access various applications with one logon. Furthermore, administrators can upload employees data by using the user import functionality.

The scenario includes the following features:
- Authentication with user name and password
- A secure SSO to cloud applications
- Branding elements on all the forms for logon and password update
- Customized privacy policy and terms of use documents
- Employee security policy
- User import and export
- Database restricted for employees only

**Example**

Julie Armstrong is an administrator at company B. She wants to configure a leave request application to be used by the employees of the company. For this purpose, she imports the employees by opening the Import Users page in the administration console for Identity Authentication and selecting a CSV file containing the employees. Once she has imported all the new users into the system, she sends them an e-mail with instructions how to activate their accounts via the Forgot Password process. She also configures the trust on SAP Cloud Platform.

Julie wants only the employees to access the application. She selects the Internal radio button after she chooses Authentication and Access > User Application Access for the leave request application in the administration console.

As an employee of company B, Michael accesses an SAP Cloud Platform application to make a leave request. When he opens the application, he has to choose the Forgot Password link to activate his account. After activation, Michael provides a user name and password to log on to the leave request application with. He is redirected to Identity Authentication for authentication. Identity Authentication verifies his credentials and sends a response back to the SAP Cloud Platform application. As a result, Michael logs on and enters his leave request.
1. Imports users.
2. Activates account.
3. Provides credentials.
4. Delegates authentication.
5. Confirms authentication.

Related Information

Import or Update Users for a Specific Application [page 196]
Integration with SAP Cloud Platform [page 410]
Configure User Access to the Application [page 87]
Tenant SAML 2.0 Configuration [page 130]

1.5 Operation Guide

This guide is for administrators. It explains how administrators can configure SAP Cloud Platform Identity Authentication service so that users can have all enhanced features for each scenario. For these configurations,
administrators mainly use the administration console for Identity Authentication, a Fiori-based user interface adaptive to most browsers.

**Related Information**

- Configuring Applications [page 40]
- Configuring Tenant Settings [page 129]
- Configuring Privacy Policies [page 173]
- Configuring Terms of Use [page 178]
- User Management [page 195]
- User Groups [page 216]
- User Provisioning [page 223]
- Managing Administrators [page 237]
- Corporate Identity Providers [page 243]
- Social Identity Providers [page 268]
- Export Change Logs with a History of Administration Operations [page 277]
- Export Existing Users of a Tenant of SAP Cloud Platform Identity Authentication Service [page 281]
- Troubleshooting for Administrators [page 298]
- View Usage Statistics [page 273]

### 1.5.1 Configuring Applications

This section describes how you can configure the user authentication, access to an application, and use a branding style in accordance with your company requirements. It also explains the trust configuration between SAP Cloud Platform Identity Authentication service and a service provider or client (relying party).

**Types of Applications**

In SAP Cloud Platform Identity Authentication service you can create and configure your own custom applications (SAML 2.0 or OpenID Connect).

Apart from the custom applications that you can create, the tenant of Identity Authentication has two additional system applications. They are predefined with the creation of the tenant. These applications are: Administration Console, and User Profile, previously called SAP Cloud Identity.

**i Note**

In some tenants, the User Profile application still bears its previous name, SAP Cloud Identity.
→ Tip

If Administration Console or User Profile are not in the list of the system applications you may request them. To do this, report an incident on SAP Support Portal Home under the component BC-IAM-IDS.

⚠️ Caution

Please be careful when you make configuration changes to the system applications. Certain configuration options for the system applications are read-only.

For more information, how to create a custom application, see Create a New Application [page 43].

The Administration Console application contains the configurations of the administration console for SAP Cloud Platform Identity Authentication service.

As a tenant administrator you can change the default configurations:

- to configure stronger protection for the administration console for SAP Cloud Platform Identity Authentication service via the Risk-Based Authentication option.
- to configure stronger password requirements for the tenant administrators of the administration console for SAP Cloud Platform Identity Authentication service.
- to customize the look and feel of the logon page of the administration console for SAP Cloud Platform Identity Authentication service.

The User Profile application contains the configurations of the Profile Page.

As a tenant administrator you can change the default configurations:

- to define custom e-mail template sets for users created via the Add User option in the administration console for Identity Authentication, or via the SCIM REST API.
- to customize the look and feel of the logon page of the Profile Page.

### Configuring Applications

<table>
<thead>
<tr>
<th>To learn about</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to create an application and configure its display name</td>
<td><a href="#">Create a New Application</a></td>
</tr>
<tr>
<td></td>
<td><a href="#">Change an Application’s Display Name</a></td>
</tr>
<tr>
<td></td>
<td><a href="#">Configure an Application’s Home URL</a></td>
</tr>
<tr>
<td></td>
<td><a href="#">Visit an Application’s Web Page</a></td>
</tr>
<tr>
<td>How to delete an application</td>
<td><a href="#">Delete Applications</a></td>
</tr>
</tbody>
</table>

SAP Cloud Platform Identity Authentication Service

SAP Cloud Platform Identity Authentication Service
<table>
<thead>
<tr>
<th>To learn about</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to configure trust</td>
<td>● Configure Trust [page 55]</td>
</tr>
<tr>
<td></td>
<td>● Configure the Name ID Attribute Sent to the Application [page 67]</td>
</tr>
<tr>
<td></td>
<td>● Configure the User Attributes Sent to the Application [page 64]</td>
</tr>
<tr>
<td></td>
<td>● Configure the Default Attributes Sent to the Application [page 71]</td>
</tr>
<tr>
<td>How to manage authentications</td>
<td>● Authentication [page 75]</td>
</tr>
<tr>
<td>How to configure API Authentication</td>
<td>● Configure a Certificate for API Authentication [page 80]</td>
</tr>
<tr>
<td></td>
<td>● Configure Credentials for HTTP Basic Authentication [page 79]</td>
</tr>
<tr>
<td>How to manage Terms of Use and Privacy Policies</td>
<td>On a tenant level</td>
</tr>
<tr>
<td></td>
<td>● Configuring Terms of Use [page 178]</td>
</tr>
<tr>
<td></td>
<td>● Configuring Privacy Policies [page 173]</td>
</tr>
<tr>
<td></td>
<td>Specific for the application</td>
</tr>
<tr>
<td></td>
<td>● Define a Terms of Use Document for an Application [page 182]</td>
</tr>
<tr>
<td></td>
<td>● Define a Privacy Policy Document for an Application [page 176]</td>
</tr>
<tr>
<td>How to configure branding styles and layout</td>
<td>On a tenant level</td>
</tr>
<tr>
<td></td>
<td>● Configure a Tenant Logo [page 134]</td>
</tr>
<tr>
<td></td>
<td>Specific for the application</td>
</tr>
<tr>
<td></td>
<td>● Display Application Name on Logon Page [page 91]</td>
</tr>
<tr>
<td></td>
<td>● Configure a Logo for an Application [page 90]</td>
</tr>
<tr>
<td></td>
<td>● Configure a Branding Style for an Application [page 93]</td>
</tr>
<tr>
<td></td>
<td>● Define an E-Mail Template Set for an Application [page 96]</td>
</tr>
<tr>
<td></td>
<td>● Configure Registration and Upgrade Forms [page 97]</td>
</tr>
<tr>
<td>How to configure access</td>
<td>● Configure an Application’s Home URL [page 50]</td>
</tr>
<tr>
<td></td>
<td>● Visit an Application’s Web Page [page 52]</td>
</tr>
<tr>
<td></td>
<td>● Configure User Access to the Application [page 87]</td>
</tr>
<tr>
<td></td>
<td>● Protecting Application Forms with Google reCAPTCHA [page 107]</td>
</tr>
<tr>
<td></td>
<td>● Set a Password Policy for an Application [page 168]</td>
</tr>
<tr>
<td></td>
<td>● Import or Update Users for a Specific Application [page 196]</td>
</tr>
<tr>
<td>How to choose an identity provider for an application</td>
<td>● Authenticating Identity Provider for an Application [page 111]</td>
</tr>
</tbody>
</table>
1.5.1.1  Create a New Application

You can create a new application and customize it to comply with your company requirements.

Context

You can create two types of applications in SAP Cloud Platform Identity Authentication service:

Create SAML 2.0 Application [page 43]
  You can create a new SAML 2.0 application and customize it to comply with your company requirements.

Create OpenID Connect Application [page 45]
  You can create a new OpenID Connect application.

Related Information

Configure Trust [page 55]
Configuring Applications [page 40]
Troubleshooting for Administrators [page 298]

1.5.1.1.1  Create SAML 2.0 Application

You can create a new SAML 2.0 application and customize it to comply with your company requirements.

Context

When you create a new application. It is set as SAML 2.0 by default.
To create a new SAML 2.0 application, proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.onemand.com/admin pattern.
**Tenant ID** is an automatically generated ID by the system. The first administrator created for the tenant receives an activation email with a URL in it. This URL contains the **tenant ID**.

2. Choose the **Applications** tile.
3. Choose the **+Add** button on the left-hand panel to add a new application to the list.

**Note**

The display name of the application appears on the logon and registration pages.

Once the application has been created, the system displays the message **Application <name of application> created**.

**Results**

The newly created application appears on the list with the applications on the left. It is selected and you can proceed with its configuration.

**Next Steps**

1. Configure the SAML 2.0 trust with the service provider. For more information, see **Configure SAML 2.0 Service Provider** [page 55].
2. (Optional) If necessary, configure the application. For more information, see **Configuring Applications** [page 40].

**Task overview:** Create a New Application [page 43]

**Related Information**

Create OpenID Connect Application [page 45]
Troubleshooting for Administrators [page 298]
1.5.1.2 Create OpenID Connect Application

You can create a new OpenID Connect application.

Context

To create a new OpenID Connect application you have to add a new application to the list of applications in SAP Cloud Platform Identity Authentication service, and then set the type of application to OpenID Connect.

To create a new OpenID Connect application, choose your scenario and follow the procedure below.

For more information about what Identity Authentication supports for OpenID Connect, and how to configure the different flows, see OpenID Connect [page 283].

Create OpenID Connect Application for Authentication Code Flow [page 46]
Create a new OpenID Connect application for authentication code flow.

Create OpenID Connect Application for Resource Owner Credential Flow [page 47]
You can create a new OpenID Connect application.

Task overview: Create a New Application [page 43]

Related Information

Create SAML 2.0 Application [page 43]
1.5.1.1.2.1 Create OpenID Connect Application for Authentication Code Flow

Create a new OpenID Connect application for authentication code flow.

Context

To create a new OpenID Connect application follow the procedure below:

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern. 
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
3. Choose the +Add button on the left-hand panel to add a new application to the list.

   i Note
   The display name of the application is displayed on the logon and registration pages.

   Once the application has been created, the system displays the message Application <name of application> created.

   The newly created application appears on the list with the applications on the left. It is selected and you can set its type to OpenID Connect.

4. Choose Trust SINGLE SIGN-ON Type

   △ Caution
   Make sure that the application you want to configure as OpenID connect is selected on the left.

5. Select OpenID Connect.
6. Save your selection.

   The system displays the message Application <name of application> updated.

   i Note
   (Optional) If necessary, configure additional settings for the application. For more information about the supported configurations for the OpenID Connect applications, see the following links:
Task overview: Create OpenID Connect Application [page 45]

Related Information

Create OpenID Connect Application for Resource Owner Credential Flow [page 47]
OpenID Connect [page 283]

1.5.1.1.2.2 Create OpenID Connect Application for Resource Owner Credential Flow

You can create a new OpenID Connect application.

Context

To create a new OpenID Connect application you have to add a new application to the list of applications in SAP Cloud Platform Identity Authentication service, and then set the type of application to OpenID Connect.

To create a new OpenID Connect application, choose your scenario and follow the procedure there.
Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   ![Note](image)
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   
   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the *Applications* tile.

3. Choose the +*Add* button on the left-hand panel to add a new application to the list.

   ![Note](image)
   The display name of the application is displayed on the logon and registration pages.

   Once the application has been created, the system displays the message Application <name of application> created.

   The newly created application appears on the list with the applications on the left. It is selected and you can set its type to OpenID Connect.

4. Choose ![Trust](image) SINGLE SIGN-ON ![Type](image)

   ![Caution](image)
   Make sure that the application you want to configure as OpenID connect is selected on the left.

5. Select *OpenID Connect*.

6. Save your selection.

   The system displays the message Application <name of application> updated.

   ![Note](image)
   (Optional) If necessary, configure additional settings for the application. For more information about the supported configurations for the OpenID Connect applications, see the following links:
   - Configure the User Attributes Sent to the Application [page 64]
   - Configure the Default Attributes Sent to the Application [page 71]
   - Configure Credentials for HTTP Basic Authentication [page 79]
   - Configure a Certificate for API Authentication [page 80]
   - Configure Risk-Based Authentication [page 82]
   - Configure User Access to the Application [page 87]
   - Enable E-Mail Verification [page 89]
   - Configuring Password Policies [page 166]

**Task overview:** Create OpenID Connect Application [page 45]
1.5.1.2 Change an Application's Display Name

Prerequisites

You are assigned the Manage Applications role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   i Note
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern. Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   i Note
   
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
   
   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Click the name of the application and change it in the pop-up dialog.

5. Save your changes.

   Once the application has been updated, the system displays the message Application <name of application> updated.
Related Information

Troubleshooting for Administrators [page 298]
Create a New Application [page 43]

1.5.1.3  Configure an Application's Home URL

You can configure the Home URL of an application in the administration console for SAP Cloud Platform Identity Authentication service.

Context

Users are redirected to the Home URL after activating their accounts, when they are created via a CSV file import or the user registration service of Identity Authentication. Initially, the Home URL for an application is not configured in the administration console for Identity Authentication. Once the Home URL has been set, you can change it.

→ Recommendation

From a usability perspective we recommend you to use URL of a protected page.

→ Remember

Home URL is necessary when you import new users in Identity Authentication. Identity Authentication needs to send activation e-mails to the new users and the home URL has to be mentioned in the e-mails. To access the application, the users have to activate their accounts. For more information see Import or Update Users for a Specific Application [page 196].

To configure the Home URL, proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   → Note

   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
This operation opens a list of the applications.

3. Choose the application that you want to edit.

   **i Note**
   
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
   
   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Select the *Home URL* anchor text.
   
   - If you are configuring the URL for the first time, type the address in the dialog box that appears.
   - If you are editing the URL, choose *Edit* from the list item, and type the new address in the dialog box.

   **→ Tip**
   
   From a usability perspective we recommend you to use URL for a protected page.

5. Save your changes.

   ![Application URL Edit Dialog](image)

   Once the application has been updated, the system displays the message *Application <name of application> updated.*

**Related Information**

Invitation REST API [page 317]
User Registration [page 320]
1.5.1.4 Visit an Application's Web Page

You can navigate to an application's Web site directly from the administration console for SAP Cloud Platform Identity Authentication service.

Prerequisites

You have configured Home URL for the application in question. For more information, see Related Information.

Context

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   \[\text{i Note}\]
   
   The URL has the \text{https://<tenant ID>.accounts.ondemand.com/admin} pattern.
   
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   \[\text{i Note}\]
   
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.

   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Select the Home URL anchor text.

5. Choose Visit.

   The Web page for the application opens in a new window.
1.5.1.5  Delete Applications

As a tenant administrator, you can delete one or more custom applications in a tenant of SAP Cloud Platform Identity Authentication service.

Prerequisites

- You are assigned the Manage Applications role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
- You have at least one custom application that you want to delete.

Context

A Delete Applications operation removes the application and all of its configurations from the tenant of Identity Authentication.

Note

You can only delete custom applications. The system applications in your tenant are hidden when you enter Delete Applications mode in the administration console for Identity Authentication.

To delete one or more applications, choose one of the following options:

Delete Multiple Applications

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

Note

The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.
2. Choose the **Applications** tile.
   This operation opens a list of the applications.

3. Choose the icon in the left-hand panel.
   This operation activates the **Delete Applications** mode.

4. Select the application or applications that you want to delete.
5. Choose the **Delete** button.
6. Confirm the operation in the pop-up dialog.
   Once the application or applications have been deleted, the system displays the message `<number>` applications deleted.

---

### Delete Single Application

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   The URL has the `https://<tenant ID>.accounts.ondemand.com=admin` pattern.

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the **Applications** tile.
   This operation opens a list of the applications.

3. Select the application that you want to delete.

   **Tip**
   Type the name of the application in the search field to filter the list items.

4. Choose the **Delete** button in the right-hand panel to delete the selected application.
5. Confirm the operation in the pop-up dialog.
   Once the application has been deleted, the system displays the message `1 application deleted`. 
1.5.1.6 Configure Trust

This document is intended to help you configure a trusted service provider (SP) or client (relying party) in the administration console for SAP Cloud Platform Identity Authentication service.

Context

The trust is configured by uploading the service provider metadata (for the SAML 2.0 applications), or by entering the information manually (for the SAML 2.0 or OpenID Connect applications). Depending on the SSO type, you can configure a SAML 2.0 trusted service provider or Open ID Connect trusted client in the administration console for SAP Cloud Platform Identity Authentication service:

Configure SAML 2.0 Service Provider [page 55]
This document is intended to help you configure a SAML 2.0 service provider (SP) in the administration console for SAP Cloud Platform Identity Authentication service. The trust is configured by uploading the service provider metadata, or by entering the information manually. You can enter manually the name of the service provider, its endpoints, and its signing certificate.

Configure OpenID Connect Application [page 59]
This document is intended to help you configure an OpenID Connect application in the administration console for SAP Cloud Platform Identity Authentication service.

Related Information

Troubleshooting for Administrators [page 298]
Integration with SAP Cloud Platform [page 410]

1.5.1.6.1 Configure SAML 2.0 Service Provider

This document is intended to help you configure a SAML 2.0 service provider (SP) in the administration console for SAP Cloud Platform Identity Authentication service. The trust is configured by uploading the service provider metadata, or by entering the information manually. You can enter manually the name of the service provider, its endpoints, and its signing certificate.

Prerequisites

You have the service provider metadata. See the service provider documentation for more information or contact the administrator of the service provider.
Tip
For more information how to download the metadata for SAP Cloud Platform when it acts as a service provider (SP), see Application Identity Provider.

Remember
If your scenario includes the enabling of the Trust All Corporate Identity Providers option in the administration console, the service provider metadata must contain the assertion consumer (ACS) endpoint that can process unsolicited SAML responses.

With SAP Cloud Platform, the endpoint is the URL of the application’s protected page. This endpoint must be either set as a default ACS endpoint of the service provider in Identity Authentication, or chosen by its index when performing IdP-initiated SSO. For more information, see Configure IdP-Initiated SSO [page 162].

Example

```xml
<ns3:AssertionConsumerService index="1" isDefault="false"
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://<application URL>/protected.jsp"/>
```

Context
To configure a SAML 2.0 trusted service provider in the administration console for SAP Cloud Platform Identity Authentication service, proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
   This operation opens a list of the applications.

3. Choose the application that you want to edit.
4. Choose the Trust tab.
5. Under SINGLE SIGN-ON, choose SAML 2.0 Configuration.
6. Upload the service provider metadata XML file or manually enter the communication settings negotiated between Identity Authentication and the service provider.

→ Remember
If your scenario includes the enabling of the Trust All Corporate Identity Providers option, the assertion consumer (ACS) endpoint with the URL of the application’s protected page, and the index must be included in the service provider metadata.

i Note
Use a file with an extension .xml.
If you use SAP Cloud Platform as a service provider, see Integration with SAP Cloud Platform [page 410] for more information how to download its metadata.

On service provider metadata upload, the fields are populated with the parsed data from the XML file. The minimum configuration is to complete the Name field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata File</td>
<td>The metadata XML file of the service provider.</td>
</tr>
<tr>
<td>Name</td>
<td>The entity ID of the service provider.</td>
</tr>
<tr>
<td>Assertion Consumer Service Endpoint</td>
<td>The SP’s endpoint URL that receives the response with the SAML assertion from Identity Authentication.</td>
</tr>
</tbody>
</table>

i Note
You can see the index number of the endpoint of the assertion consumer service of the service provider as the target of the SAML response.

| Single Logout Endpoint         | The SP’s endpoint URL that receives the logout response or request (for a multiple SPs scenario) from Identity Authentication for the termination of all current sessions. |

This field has the following attributes:
- **Binding** - specifies the SAML binding supported by the logout endpoint.
  - HTTP-POST
  - HTTP-REDIRECT
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>○ SOAP</td>
<td>The SOAP Endpoint is called only when the user password is changed.</td>
</tr>
<tr>
<td>○ URL</td>
<td>specifies the location of the logout endpoint.</td>
</tr>
<tr>
<td>○ Response URL</td>
<td>(optional) specifies a different location to which logout response messages should be sent.</td>
</tr>
<tr>
<td>Signing Certificate</td>
<td>A base64-encoded certificate used by the service provider to sign digitally SAML protocol messages sent to Identity Authentication.</td>
</tr>
</tbody>
</table>

**Restriction**

The Metadata File, Name, Assertion Consumer Service Endpoint, and Single Logout Endpoint fields are not editable for the system applications.

7. **Optional:** Choose the digest algorithm for signing outgoing messages from the dropdown list in the Algorithm section. You have the following options:
   - SHA-1 - the default option
   - SHA-256

8. Save your selection.

Once the application has been changed, the system displays the message Application <name of application> updated.

**Next Steps**

Configure trust on the service provider side.

1. Download the SAML 2.0 metadata of Identity Authentication.

   **Note**
   For more information about how to download the SAML 2.0 metadata describing Identity Authentication as identity provider see Tenant SAML 2.0 Configuration [page 130].

2. Configure the service provider to trust Identity Authentication.

   **Note**
   See the service provider documentation for more information about how to configure the trust.

   **Tip**
   If you use SAP Cloud Platform as a service provider, see Integration with SAP Cloud Platform [page 410].

**Task overview:** Configure Trust [page 55]
1.5.1.6.2 Configure OpenID Connect Application

This document is intended to help you configure an OpenID Connect application in the administration console for SAP Cloud Platform Identity Authentication service.

Context

For more information about what Identity Authentication supports for OpenID Connect, and how to configure the different flows, see OpenID Connect [page 283].

- Configure OpenID Connect Application for Authorization Code Flow [page 60]
  This document is intended to help you configure an OpenID Connect application in the administration console for SAP Cloud Platform Identity Authentication service for the authorization code flow.

- Configure OpenID Connect Application for Resource Owner Credential Flow [page 62]
  This document is intended to help you configure an OpenID Connect application in the administration console for SAP Cloud Platform Identity Authentication service for the resource owner credential flow.

Task overview: Configure Trust [page 55]

Related Information

Configure SAML 2.0 Service Provider [page 55]
1.5.1.6.2.1 Configure OpenID Connect Application for Authorization Code Flow

This document is intended to help you configure an OpenID Connect application in the administration console for SAP Cloud Platform Identity Authentication service for the authorization code flow.

Prerequisites

You have an OpenID Connect application in the administration console for Identity Authentication. For more information, see Create OpenID Connect Application [page 45].

Context

The trust is configured by entering the information manually. You can enter manually the name of the client (relying party), and its redirect URIs.

Note

The steps are one and the same, both for the authorization code flow and the resource owner credential flow.

To configure an OpenID Connect trusted application in the administration console for SAP Cloud Platform Identity Authentication service proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   Note

   The URL has the https:\/<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   Note

   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.

5. Under SINGLE SIGN-ON, choose OpenID Connect Configuration.

6. Manually enter the communication settings negotiated between Identity Authentication and the client.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The issuer in the OpenID Provider metadata.</td>
</tr>
<tr>
<td>Redirect URI</td>
<td>The redirection URI to which the response will be sent. You can add up to five redirect URIs.</td>
</tr>
</tbody>
</table>

7. Save your selection. Once the application has been changed, the system displays the message Application <name of application> updated.

**Remember**

Configure trust on the client side. See the client documentation for more information about how to configure the trust. For more information how to view the OpenID Connect settings of Identity Authentication, see Tenant OpenID Connect Configuration [page 132].

**Next Steps**

- Configure HTTP basic authentication for the application. For more information about the configuration, see Configure Credentials for HTTP Basic Authentication [page 79].

**Task overview:** Configure OpenID Connect Application [page 59]

**Related Information**

Configure OpenID Connect Application for Resource Owner Credential Flow [page 62]

OpenID Connect [page 283]
1.5.1.6.2.2 Configure OpenID Connect Application for Resource Owner Credential Flow

This document is intended to help you configure an OpenID Connect application in the administration console for SAP Cloud Platform Identity Authentication service for the resource owner credential flow.

Prerequisites

You have an OpenID Connect application in the administration console for Identity Authentication. For more information, see Create OpenID Connect Application [page 45].

Context

The trust is configured by entering the information manually. You can enter manually the name of the client (relying party), and its redirect URIs.

- **i Note**: The steps are one and the same, both for the authorization code flow and the resource owner credential flow.

To configure an OpenID Connect trusted application in the administration console for SAP Cloud Platform Identity Authentication service proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   - **i Note**: The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern. `Tenant ID` is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the `tenant ID`.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   - **i Note**: Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.

5. Under SINGLE SIGN-ON, choose OpenID Connect Configuration.

6. Manually enter the communication settings negotiated between Identity Authentication and the client.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The issuer in the OpenID Provider metadata.</td>
</tr>
<tr>
<td>Redirect URI</td>
<td>The redirection URI to which the response will be sent. You can add up to five redirect URIs.</td>
</tr>
</tbody>
</table>

**Note**

The Redirect URI configuration is not mandatory for the Resource Owner Credential Flow and can be skipped.

7. Save your selection. Once the application has been changed, the system displays the message Application <name of application> updated.

**Next Steps**

- Configure HTTP basic authentication for the application. For more information about the configuration, see Configure Credentials for HTTP Basic Authentication [page 79].

Task overview: Configure OpenID Connect Application [page 59]

**Related Information**

Configure OpenID Connect Application for Authorization Code Flow [page 60]
OpenID Connect [page 283]
1.5.1.7 Configure the User Attributes Sent to the Application

After configuring the user attributes to be collected by the registration and upgrade forms, you have to specify how these attributes are sent to the application.

Context

SAP Cloud Platform Identity Authentication service defines default names for these assertion attributes, but you can change them in accordance with your requirements.

You configure the attributes by defining which assertion attribute corresponds to the user attribute that you set for the registration and upgrade forms. You can also specify multiple assertion attributes for each user attribute. You perform this mapping to help the application use the same user attribute for different scenarios that require several assertion attributes.

The attributes are also put in the id_token if the application is OpenID connect. For more information, see OpenID Connect [page 283].

By default, Identity Authentication sets the following assertion attribute names:

<table>
<thead>
<tr>
<th>User Attribute</th>
<th>Assertion Attribute Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salutation</td>
<td>title</td>
</tr>
<tr>
<td>First Name</td>
<td>first_name</td>
</tr>
<tr>
<td>Middle Name</td>
<td>middle_name</td>
</tr>
<tr>
<td>Last Name</td>
<td>last_name</td>
</tr>
<tr>
<td>E-mail</td>
<td>mail</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>telephone</td>
</tr>
<tr>
<td>Language</td>
<td>language</td>
</tr>
<tr>
<td>Login Name</td>
<td>login_name</td>
</tr>
<tr>
<td>Display Name</td>
<td>display_name</td>
</tr>
<tr>
<td>User ID</td>
<td>uid</td>
</tr>
<tr>
<td>User Type</td>
<td>type</td>
</tr>
<tr>
<td>Street Address</td>
<td>street</td>
</tr>
<tr>
<td>Street Address 2</td>
<td>street2</td>
</tr>
<tr>
<td>City</td>
<td>city</td>
</tr>
<tr>
<td>ZIP/Postal Code</td>
<td>zip</td>
</tr>
</tbody>
</table>

Note

For example, consumer, partner, or employee.
<table>
<thead>
<tr>
<th>User Attribute</th>
<th>Assertion Attribute Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>country</td>
</tr>
<tr>
<td>State/Province</td>
<td>state</td>
</tr>
<tr>
<td>Cost Center</td>
<td>cost_center</td>
</tr>
<tr>
<td>Department</td>
<td>department</td>
</tr>
<tr>
<td>Division</td>
<td>division</td>
</tr>
<tr>
<td>Employee Number</td>
<td>employee_number</td>
</tr>
<tr>
<td>Company</td>
<td>company</td>
</tr>
<tr>
<td>Company Street Address</td>
<td>company_street</td>
</tr>
<tr>
<td>Company Street Address 2</td>
<td>company_street_2</td>
</tr>
<tr>
<td>Company City</td>
<td>company_city</td>
</tr>
<tr>
<td>Company ZIP/Postal Code</td>
<td>company_zip</td>
</tr>
<tr>
<td>Company Country</td>
<td>company_country</td>
</tr>
<tr>
<td>Company State/Province</td>
<td>company_region</td>
</tr>
<tr>
<td>Company Industry</td>
<td>industry</td>
</tr>
<tr>
<td>Company Relationship</td>
<td>relationship</td>
</tr>
<tr>
<td>Job Function</td>
<td>job_function</td>
</tr>
<tr>
<td>Groups</td>
<td>groups</td>
</tr>
<tr>
<td>Corporate Groups</td>
<td>corporate_groups</td>
</tr>
</tbody>
</table>

**i Note**

This attribute is applicable for the corporate user store scenarios and contains the groups the user in the corporate user store is assigned to.

<table>
<thead>
<tr>
<th>Contact by E-mail</th>
<th>contact_preference_mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact by Telephone</td>
<td>contact_preference_telephone</td>
</tr>
<tr>
<td>Application Custom Attribute 1</td>
<td>app_custom_attribute_1</td>
</tr>
<tr>
<td>Application Custom Attribute 2</td>
<td>app_custom_attribute_2</td>
</tr>
<tr>
<td>Application Custom Attribute 3</td>
<td>app_custom_attribute_3</td>
</tr>
<tr>
<td>Application Custom Attribute 4</td>
<td>app_custom_attribute_4</td>
</tr>
<tr>
<td>Application Custom Attribute 5</td>
<td>app_custom_attribute_5</td>
</tr>
</tbody>
</table>

**Remember**

Custom attributes must not be used to store sensitive personal data.
The **User Attribute** column lists the attributes that can be shown on the registration and upgrade forms. The **Assertion Attribute Name** lists the attributes that are sent in the assertion.

The configured custom attributes are also put in the `id_token` if the application is OpenID connect. For more information, see OpenID Connect [page 283].

The configured custom attributes can be seen at the user profile page at https://<tenant ID>.accounts.ondemand.com/ after choosing View My Data.

The configuration of the user attributes for the system applications is disabled. The default settings for these applications are First Name, Company, Last Name, and E-Mail.

To configure the assertion attributes, proceed as follows:

### Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

   **Tenant ID** is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the **tenant ID**.

2. Choose the **Applications** tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   **i Note**
   
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.

   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the **Trust** tab.
5. Under **SINGLE SIGN-ON**, choose **Assertion Attributes**.
6. Add and modify the names of the assertion attributes that you want to customize.
7. Save your configuration.

   If the operation is successful, you receive the message **Assertion attributes updated**.

**Related Information**

- Configure Registration and Upgrade Forms [page 97]
- Troubleshooting for Administrators [page 298]
- Create a New Application [page 43]
- SAML 2.0 [page 283]

### 1.5.1.8 Configure the Name ID Attribute Sent to the Application

This is a profile attribute that SAP Cloud Platform Identity Authentication service sends to the application as a name ID. The application then uses this attribute to identify the user.

**Context**

The user is identified in one of the following ways:

- By user ID

  **i Note**
  
  This is the default setting.

- By e-mail
- By display name
- By login name
- By employee number.

**i Note**

User ID, E-Mail, Display Name, and Login Name are unique for the tenant.

The configuration of the name ID attribute for the system applications is disabled. The default setting for these applications is **User ID**.

**Caution**

Identity Authentication does not check the Employee Number attribute for uniqueness. Be sure that the users receive unique employee numbers.
When the application uses corporate IdP for authentication, and Identity Federation is disabled, the name ID attribute configurations in the administration console for Identity Authentication are not relevant. In such scenarios Identity Authentication sends to the application the name ID attribute that comes from the corporate identity provider without changing it. For more information about the corporate identity provider scenario, see Corporate Identity Providers [page 243] and Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 266].

Optionally, you can configure the default name identifier format of the name ID attribute. Name ID Attribute
To set the name ID attribute, proceed as follows:

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**

   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   **i Note**

   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.

   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.

5. Under SINGLE SIGN-ON, choose NameID Attribute.

6. Select the attribute from the following:
   - User ID
   - E-Mail
   - Display Name
   - Login Name
   - Employee Number

   **Caution**

   If you select Login Name, or Employee Number Name ID, and the selected attribute has no value set for the user, the user is not able to log on the application. The message "HTTP Status 401 –
Unauthorized is displayed when the user provides credentials and logs on. For more information how to edit the user details, see List and Edit User Details [page 205].

7. Save your selection.

Once the application has been changed, the system displays the message Application <name of application> updated.

(Optional) Configure the Default Name ID Format Sent to the Application

The tenant administrator can set a default name ID format via the administration console for SAP Cloud Platform Identity Authentication service.

Context

The name ID format is used in the Format attribute of the NameID element that Identity Authentication sends to the application with the SAML assertion. This is the default name ID format. It is used only in case the application or the service provider does not request another name ID format with the SAML authentication request.

Identity Authentication supports the following name ID formats:

<table>
<thead>
<tr>
<th>Name ID Format</th>
<th>URI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unspecified</td>
<td>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</td>
<td>Identity Authentication does not use a specific format to express the identity of the user. The application receives the value of the user attribute that is selected as name ID attribute. By default this is the default Name ID format.</td>
</tr>
</tbody>
</table>
### Name ID Format

<table>
<thead>
<tr>
<th>Name ID Format</th>
<th>URI</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail address</td>
<td>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</td>
<td>The format of the name ID is an e-mail address. You can configure this setting when you have chosen as name ID attribute a user attribute that contains e-mail.</td>
</tr>
</tbody>
</table>

**i Note**

Identity Authentication does not check if the content of the name ID attribute is e-mail address. You can decide which name ID attribute to configure for the application. Make sure that it contains e-mail address in case you want to conform to the SAML2 specification.

**→ Remember**

When the application uses corporate IdP for authentication, and Identity Federation is disabled, the default name ID attribute configurations in the administration console for Identity Authentication are not relevant. In such scenarios Identity Authentication sends to the application name ID format that comes from the SAML assertion sent from the corporate IdP without changing it. For more information about the corporate identity provider scenario, see Corporate Identity Providers [page 243] and Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 266].

To set the default name ID format, proceed as follows:

### Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**

   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the Applications tile.
This operation opens a list of the applications.

3. Choose the application that you want to edit.

**i Note**

Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.

If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the **Trust** tab.

5. Under **SINGLE SIGN-ON**, choose **Default Name ID Format**.

6. Select the default name ID format from the following:
   - Unspecified
   - E-Mail

7. Save your selection.

Once the application has been changed, the system displays the message Application <name of application> updated.

**Related Information**

Troubleshooting for Administrators [page 298]
Create a New Application [page 43]
Configure Trust [page 55]

**1.5.1.9 Configure the Default Attributes Sent to the Application**

In addition to the user attributes, you can also configure attributes with default values for the application.

**Context**

The attributes are sent from SAP Cloud Platform Identity Authentication service to the application in the assertion. You can set default attributes `location` and `company` with values *Europe* and *Company A* for example, so that the application displays Europe and Company A on its main page.

The attributes are also put in the `id_token` if the application is OpenID connect. For more information, see OpenID Connect [page 283].
For the SAML 2.0 applications, you can configure attributes with dynamic values to be added into the assertions. Expand the Supported Attributes table below to see the attributes that can take dynamic values:

<table>
<thead>
<tr>
<th>Attribute Display Name</th>
<th>Attribute Technical Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salutation</td>
<td>title</td>
</tr>
<tr>
<td>First Name</td>
<td>firstName</td>
</tr>
<tr>
<td>Middle Name</td>
<td>middleName</td>
</tr>
<tr>
<td>Last Name</td>
<td>lastName</td>
</tr>
<tr>
<td>E-mail</td>
<td>mail</td>
</tr>
<tr>
<td>Telephone Number</td>
<td>telephone</td>
</tr>
<tr>
<td>Language</td>
<td>language</td>
</tr>
<tr>
<td>Logon Name</td>
<td>loginName</td>
</tr>
<tr>
<td>Display Name</td>
<td>displayName</td>
</tr>
<tr>
<td>User ID</td>
<td>uid</td>
</tr>
<tr>
<td>User Type</td>
<td>type</td>
</tr>
<tr>
<td>Street Address</td>
<td>street</td>
</tr>
<tr>
<td>Street Address 2</td>
<td>street2</td>
</tr>
<tr>
<td>City</td>
<td>city</td>
</tr>
<tr>
<td>ZIP/Postal Code</td>
<td>zip</td>
</tr>
<tr>
<td>Country</td>
<td>country</td>
</tr>
<tr>
<td>State/Province</td>
<td>state</td>
</tr>
<tr>
<td>Cost Center</td>
<td>costCenter</td>
</tr>
<tr>
<td>Department</td>
<td>department</td>
</tr>
<tr>
<td>Division</td>
<td>division</td>
</tr>
<tr>
<td>Employee Number</td>
<td>personnelNumber</td>
</tr>
<tr>
<td>Company</td>
<td>company</td>
</tr>
<tr>
<td>Company Street Address</td>
<td>companyStreet</td>
</tr>
<tr>
<td>Company Street Address 2</td>
<td>companyStreet2</td>
</tr>
<tr>
<td>Company City</td>
<td>companyCity</td>
</tr>
<tr>
<td>Company ZIP/Postal Code</td>
<td>companyZip</td>
</tr>
<tr>
<td>Company Country</td>
<td>companyCountry</td>
</tr>
<tr>
<td>Company State/Province</td>
<td>companyRegion</td>
</tr>
<tr>
<td>Company Industry</td>
<td>industry</td>
</tr>
<tr>
<td>Job Function</td>
<td>jobFunction</td>
</tr>
<tr>
<td>Attribute Display Name</td>
<td>Attribute Technical Name</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Groups</td>
<td>companyGroups</td>
</tr>
<tr>
<td>i Note</td>
<td>corporateGroups</td>
</tr>
<tr>
<td>Tip</td>
<td>The attributes companyGroups and corporateGroups support regular expressions, so that they can be filtered.</td>
</tr>
<tr>
<td>Contact by E-mail</td>
<td>contactPreferenceEmail</td>
</tr>
<tr>
<td>Contact by Telephone</td>
<td>contactPreferenceTelephone</td>
</tr>
<tr>
<td>Custom Attribute 1</td>
<td>customAttribute1</td>
</tr>
<tr>
<td>Custom Attribute 2</td>
<td>customAttribute2</td>
</tr>
<tr>
<td>Custom Attribute 3</td>
<td>customAttribute3</td>
</tr>
<tr>
<td>Custom Attribute 4</td>
<td>customAttribute4</td>
</tr>
<tr>
<td>Custom Attribute 5</td>
<td>customAttribute5</td>
</tr>
<tr>
<td>Custom Attribute 6</td>
<td>customAttribute6</td>
</tr>
<tr>
<td>Custom Attribute 7</td>
<td>customAttribute7</td>
</tr>
<tr>
<td>Custom Attribute 8</td>
<td>customAttribute8</td>
</tr>
<tr>
<td>Custom Attribute 9</td>
<td>customAttribute9</td>
</tr>
<tr>
<td>Custom Attribute 10</td>
<td>customAttribute10</td>
</tr>
</tbody>
</table>

Examples for attributes with dynamic values:

If you set $\{uid\}$ as a value, the SAML response will return the ID of the user to the application:

```xml
<Attribute Name="User ID">
    <AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                       xsi:type="xs:string">
        P123456
    </AttributeValue>
</Attribute>
```

If you set $\{customAttribute1\}$ as a value, the SAML response will return the first custom attribute of the user to the application, if there is such. If the user does not have a custom attribute, the response will contain an empty attribute:
Example

<Attribute Name="Custom Attribute">
  <AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                   xsi:type="xs:string">
    {customAttribute1}
  </AttributeValue>
</AttributeValue>

If you set ${companyGroups:regex[Admin]} as a value, the SAML response will return the groups, that contain "Admin" in the name:

Example

<Attribute Name="Groups">
  <AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                   xsi:type="xs:string">
    Admins
  </AttributeValue>
  <AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
                   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                   xsi:type="xs:string">
    Administrators
  </AttributeValue>
</AttributeValue>

→ Remember

Identity Federation When the application uses corporate IdP for authentication, and is disabled, the default attributes configurations in the administration console for Identity Authentication are not relevant. For more information about the corporate identity provider scenario, see Corporate Identity Providers [page 243] and Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 266].

The configuration of the default attributes for the system applications is disabled.

To configure default attributes, proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

  i Note

  The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

  Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.
i Note
Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.
5. Under SINGLE SIGN-ON, choose Default Attributes.
6. Add the default attributes with their values to be sent to the application.

Remember
Always use the Attribute Technical Name to configure attributes with dynamic values.

7. Save your configuration.
If the operation is successful, you receive the message Default attributes updated.

Related Information
Configure the User Attributes Sent to the Application [page 64]
Troubleshooting for Administrators [page 298]
Create a New Application [page 43]
SAML 2.0 [page 283]

1.5.1.10 Authentication

<table>
<thead>
<tr>
<th>To learn about</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to define rules for authentication in accordance with the risk</td>
<td>Configure Risk-Based Authentication [page 82]</td>
</tr>
<tr>
<td>Enable social sign-on authentication for an application</td>
<td>Enable or Disable Social Sign-On for an Application [page 76]</td>
</tr>
<tr>
<td>How to allow users to log on to an application from the corporate network without entering their username and password</td>
<td>Enable or Disable Kerberos Authentication for an Application [page 78]</td>
</tr>
<tr>
<td>How to configure the type of authentication when API methods of SAP Cloud Platform Identity Authentication service are used</td>
<td>API Authentication [page 79]</td>
</tr>
</tbody>
</table>
1.5.10.1 Enable or Disable Social Sign-On for an Application

Social sign-on allows users to link their SAP Cloud Platform Identity Authentication service accounts with social network accounts. To link the accounts, users have to choose the social provider button on the logon page of a cloud application. When authenticated via their social identity provider, users are prompted to allow their accounts to be linked with the social network accounts. After this initial setup, users can log on to the application without additional authentication.

Prerequisites

You have set the keys and secrets for the social providers. For more information, see Configure Social Identity Providers [page 269].

Context

Identity Authentication allows account linking with the following social providers:

- Twitter
- Facebook
- LinkedIn
- Google

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern. Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   i Note
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Authentication and Access tab.
5. Under AUTHENTICATION, enable or disable social sign-on.

Once the application has been updated, the system displays the message Application <name of application> updated.

Results

With Social Sign-On users can log on to the application via one of the social providers. They can see this option on the logon page.

Which social identity providers logos appear on the logon page of the application depend on the configurations you have made. For more information, see Configure Social Identity Providers [page 269].
1.5.1.10.2 Enable or Disable Kerberos Authentication for an Application

You enable Kerberos authentication to allow users to log on to an application from the corporate network without entering their username and password.

Prerequisites

You have configured Kerberos authentication for the tenant. For more information, see Configure Kerberos Authentication [page 153].

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   - **i Note**
     - The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
     - *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the Applications tile.
   - This operation opens a list of the applications.

3. Choose the application that you want to edit.

   - **i Note**
     - Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
     - If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Authentication and Access tab.

5. Under AUTHENTICATION, enable or disable SPNEGO authentication.

   - Once the application has been updated, the system displays the message *Application <name of application> updated.*
1.5.10.3 API Authentication

Developers can choose the type of authentication when API methods of SAP Cloud Platform Identity Authentication service are used.

The certificate to be used for authentication by the REST APIs of Identity Authentication must be requested from the SAP Support Portal.

1.5.10.3.1 Configure Credentials for HTTP Basic Authentication

This document describes how developers set basic authentication when API methods of SAP Cloud Platform Identity Authentication service are used.

Context

You can use a user ID and a password to authenticate when REST API calls to the tenant of Identity Authentication are used. The system automatically generates a user ID when the password is set for the first time.

i Note

The password must meet the following conditions:

- Minimum length of 8 characters
- Characters from at least three of the following groups:
  - Lower-case Latin characters (a-z)
  - Upper-case Latin characters (A-Z)
  - Base 10 digits (0-9)
  - Non-alphabetic characters (!@#$%...)

The password is locked for 60 min after 5 failed logon attempts with wrong value.
Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   **i Note**
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
   If you do not have a created application in your list, you can create one. For more information, see [Create a New Application](#page-43).

4. Choose the Trust tab.

5. Under API AUTHENTICATION, choose HTTP Basic Authentication.

6. Enter your new password in the fields.

   **i Note**
   If you are setting the password for API authentication for the first time, these fields are empty.

7. Save your entries.
   Once the password has been saved, the system displays a message informing you of this.

1.5.10.3.2 Configure a Certificate for API Authentication

This document describes how developers configure the certificate used for authentication when API methods of SAP Cloud Platform Identity Authentication service are used.

Prerequisites

You have requested a client certificate from the [SAP Support Portal](#).
Context

For the configuration, you have to provide the base64-encoded certificate as a file or plain text.

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   
   **Tenant ID** is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   **i Note**
   
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
   
   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.

5. Under **API AUTHENTICATION**, choose **Certificate for API Authentication**.

6. Upload or enter the base64-encoded certificate.

   **i Note**
   
   For the upload, you have to use .cer or .crt files.

7. Save your entries.

   Once the certificate has been uploaded, the system displays the message Certificate for API authentication updated.

Related Information

Create a New Application [page 43]
Invitation REST API [page 317]
User Management REST API [page 319]
1.5.10.4 Configure Risk-Based Authentication

You can define rules for authentication according to different risk factors. The configured rules manage authentication according to IP range (specified in CIDR notation), group membership, authentication method, and type of the authenticating user.

**Authentication Rules**

The added rules are displayed sorted by priority. When a user tries to access the application, the rules evaluate if the user meets the criteria of the rule. The evaluation starts with the rule with the highest priority, until the criteria of a rule are met. If the criteria of a rule are met, the rest of the rules are not evaluated.

**Default Authentication Rule**

If none of the authentication rules meets the criteria, the default authentication rule is applied. For the default authentication rule, you can only configure Action. The rule is valid for any IP range, Group, Authentication Method, or User Type.

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **Note**
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   
   **Tenant ID** is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
   
   This operation opens a list of the applications.

3. Choose the list item of the application that you want to edit.

   **Note**
   
   If you do not have a created application in your list, you can create one. For more details, see Related Information.

   **Caution**
   
   The list also includes the Administration Console application. If you enable risk-based authentication for that application, make sure that you, as a tenant administrator, meet the authentication rules and the default authentication rule. Otherwise when you log out of the administration console you will not be able to log in it again if you don’t meet the rules.

   If Administration Console is not in the list of the applications you may request it. To do this, report an incident with a subject on SAP Support Portal Home under the component BC-IAM-IDS.

4. Choose the Authentication and Access tab.
5. Under **AUTHENTICATION**, choose **Risk-Based Authentication**.

6. Configure the authentication rules and the default authentication rule. To configure the authentication rules, choose one of the following (optional):

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a new rule</td>
<td>See Add a New Rule [page 85]</td>
</tr>
<tr>
<td>Edit an existing rule</td>
<td>Choose the icon next to the rule you want to edit.</td>
</tr>
<tr>
<td>Delete an existing rule</td>
<td>Choose the delete icon next to the rule you want to delete.</td>
</tr>
<tr>
<td>Reprioritize rules</td>
<td>Use the arrows to reprioritize the rules.</td>
</tr>
</tbody>
</table>

**Note**
By default any user can log on from any IP.

7. Save your changes.

Once the application has been updated, the system displays the message **Authentication rules updated**.

---

**Examples**

**Example 1 (Setting TOTP Two-Factor Authentication)**

Donna Moore is an administrator of company A. She wants to configure Identity Authentication to always ask the company employees for a password and a TOTP passcode (two-factor authentication) to log on to a Leave Request application. For this purpose, Donna sets only a **Default Action**:

**Default Authentication Rule**

**Default Action**: TOTP Two-Factor Authentication

Michael Adams is an employee of company A and as such he wants to create a leave request. He is prompted to provide two factors (password and passcode generated by an authenticator app on his mobile device) to log on to the Leave Request application. Two factors are required regardless of whether Michael is in the corporate network or on a business trip. Michael’s manager, Julie Armstrong, receives a notification that Michael has created a leave request. She approves it by logging on to the application with two factors (password and passcode generated by her mobile device).

**Example 2**

Donna Moore is an administrator of company A. She wants to configure Identity Authentication to allow employees to access the Leave Request application from the corporate network with SPNEGO, and from any
other network with passcode. All IPs in the company start with 189.101. She would also like to create a rule for the managers to access the application with two authentication factors. In addition she wants to restrict the access to all the users with type Customer. For this purpose, Donna creates the following rules:

**Authentication Rules**

<table>
<thead>
<tr>
<th>Action</th>
<th>IP Range</th>
<th>Group</th>
<th>Authentication Method</th>
<th>User Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Customer</td>
</tr>
<tr>
<td>Allow</td>
<td>189.101.112.1/16</td>
<td>Employees</td>
<td>SPNEGO</td>
<td>Any</td>
</tr>
<tr>
<td>TOTP Two-Factor Authentication</td>
<td>Any</td>
<td>Employees</td>
<td>Any</td>
<td>Any</td>
</tr>
<tr>
<td>TOTP Two-Factor Authentication</td>
<td>Any</td>
<td>Managers</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

**Default Authentication Rule**

Default Action: Deny

Michael Adams, as an employee of company A, accesses the application in his office and logs on with SPNEGO. When he is on a business trip, he can create leave requests by providing two factors. The two factors are SPNEGO and a passcode generated by an authenticator app on his iPhone. Michael’s manager, Julie Armstrong, receives a notification that Michael has created a leave request. She approves it by logging on to the application with two factors (a password and a passcode generated by her Android phone). Donna Moore, a customer of company A, tries to access the corporate portal, and receives a message that she is not authorized for access.

**Related Information**

Add a New Rule [page 85]
Create a New Application [page 43]
Unlock User TOTP Passcode [page 210]
Two-Factor Authentication [page 303]
1.5.10.4.1 Add a New Rule

You can add rules for authentication according to different risk factors.

Context

Each rule contains the following information:

- **Action**
  This action is performed if the IP range, or the Groups membership, or the Authentication Method of the authenticating user meet the defined criteria.
  You can choose one of the following actions:
  - **Allow**
    SAP Cloud Platform Identity Authentication service allows the authentication of the user in accordance with the rule conditions.
  - **Deny**
    SAP Cloud Platform Identity Authentication service denies the authentication of the user in accordance with the rule conditions. You can set this action for a test application for example, or before an application goes live.
    As long as this rule is valid, when users try to log on to the application, they get the following message: *Sorry, but you are currently not authorized for access.*
  - **TOTP Two-Factor Authentication**
    SAP Cloud Platform Identity Authentication service asks two factors to authenticate the user.
    If you set TOTP two-factor authentication, users are required to provide a time-based one-time password (TOTP) called a passcode in addition to their primary credentials. Users also has to install an authenticator application, for example SAP Authenticator, on their mobile devices to generate TOTP passcodes.

  - **i Note**
    TOTP asscodes are time-based and valid for one logon attempt only.

- **IP Range**
  Define the range of allowed IP addresses or proxies that the user logs on from. The value has to be specified in Classless Inter-Domain Routing (CIDR) notation.

  - **i Note**
    By default the field is empty, meaning that any IP is allowed.

  - **Example**
    Enter 123.45.67.1/24 to allow users to log on from any IP starting with 123.45.67.

    If no IP range is defined, the rule is valid for all IP ranges.

- **Group**
  Specify a cloud or on-premise group, which the authenticating user has to be a member of. If no group is selected, the rule is valid for all users.
If the rule is valid for an on-premise group, type in the name of the corporate user store group, for which this rule should be valid.

The cloud groups have to be configured in the administration console for SAP Cloud Platform Identity Authentication service. For more information, see User Groups [page 216].

- **Authentication Method**
  - Specify the authenticating method, which the authenticating user has to use. If no method is selected, the rule is valid for any of the methods.

- **User Type**
  - Specify the type, which the authenticating user must have. If no user type is selected, the rule is valid for any of the types.

The fields **IP Range**, **Group**, **Authentication Method**, and **User Type** are not mandatory, but at least one of them has to be specified.

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.onemond.com/admin` pattern.
   
   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the **Applications** tile.

   This operation opens a list of the applications.

3. Choose the list item of the application that you want to edit.

   **i Note**
   
   If you do not have a created application in your list, you can create one. For more details, see Related Information.

   **Caution**
   
   The list also includes the Administration Console application. If you enable risk-based authentication for that application, make sure that you, as a tenant administrator, meet the authentication rules and the default authentication rule. Otherwise when you log out of the administration console you will not be able to log in again if you don’t meet the rules.

   If Administration Console is not in the list of the applications you may request it. To do this, you need to report an incident with a subject on SAP Support Portal Home under the component BC-IAM-IDS.

4. Choose the **Authentication and Access** tab.

5. Under **AUTHENTICATION**, choose **Risk-Based Authentication**.

6. Choose **Add Rule**.
7. Fill in the fields on the New Risk-Based Authentication Rule window.
8. Confirm your changes.

Related Information

Create a New Application [page 43]

1.5.1.10.5 Configure User Access to the Application

Context

You can configure the application to restrict access to specific users only. The following access configurations are possible:

- **Public**
  All users are allowed to log on. Unregistered users start the self-registration process by choosing the Register Now link on the logon page.

  - **i Note**
    You have to add as trusted the domains for those applications that allow self-registration to the users. For more information, see Configure Trusted Domains [page 138].

  - **Tip**
    You can protect the self-registration form against machine registrations via reCAPTCHA. For more information, see Protecting Application Forms with Google reCAPTCHA [page 107].

- **Internal** - this is the default setting.
  Only existing users are allowed to log on. Users that are not in the user store of SAP Cloud Platform Identity Authentication service cannot log on. When this option is chosen, self-registration is not possible.

  - **Tip**
    For more information how to add new users in the user store of Identity Authentication, see Create a New User [page 202]. You can also import new users in Identity Authentication via a CSV file. For more information, see Import or Update Users for a Specific Application [page 196].

- **Private**
  Only users registered by an application can log on. To register users for a specific application, you have to import these users via a CSV file. For more information, about the user import, see Import or Update Users for a Specific Application [page 196].
Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern. Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
   This operation opens a list of the applications.
3. Choose the application that you want to edit.

   i Note
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Authentication and Access tab.
6. Set the radio button for the users you want to allow to log on.
7. Save your selection.
   If the application is updated, the system displays the message Application <name of application> updated.

Related Information

Troubleshooting for Administrators [page 298]
Create a New Application [page 43]
Risk-Based Authentication as an Alternative to Restrict User Access Option in SAP Cloud Platform Identity Authentication Service
1.5.1.10.6 Enable E-Mail Verification

Tenant administrators can configure applications to require verification of the user’s e-mail address.

**Context**

Applications can be configured to require users to have their e-mail addresses verified before they can log on. In some cases, when you can create new users. If you want to make sure that a user has a valid e-mail address, even if the e-mail address has not been verified, you should enable the e-mail verification option in the administration console for Identity Authentication.

**i Note**

You can check whether the user’s e-mail address has been verified by choosing User Management > User Details > Personal Information in the administration console. The E-Mail Verified box is checked if the user’s e-mail address has been verified. For more information about the user details, see List and Edit User Details [page 205].

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern. Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern. Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

3. Choose the application that you want to edit.

   **i Note**
   
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the **Authentication and Access** tab.
5. Under **AUTHENTICATION**, enable **E-Mail Verification**.

Once the application has been updated, the system displays the message **Application <name of application> updated**.

**Results**

When the user tries to log on, he or she is asked to verify the e-mail address first. Once the e-mail address has been verified, the user can log on to the application.

### 1.5.1.11 Configure a Logo for an Application

You can configure a custom logo for a specific application by uploading an image. Furthermore, you can remove a configured logo and leave the display name only as a title for the application.

The logo is displayed on the application’s logon page and can be included into the e-mails sent to users.

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern. 

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the **Applications** tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   **i Note**
   
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.

   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].
4. Choose the *Branding and Layout* tab.
5. Under *BRANDING*, choose *Logo*.
6. To set a custom logo, upload an image with the required format.
   
   You can use one of the following formats for the image: `<name>.png`, `<name>.gif`, and `<name>.jpeg`.

   **Note**
   
   The image must be smaller than 100 KB and with a maximum size of 300x100.

7. To remove a configured logo, choose the *Remove Logo* button.
8. Save your configuration.

### Related Information

- Create a New Application [page 43]
- Troubleshooting for Administrators [page 298]

### 1.5.1.12 Display Application Name on Logon Page

This section shows you how to display or hide the name of the application from the logon page.

#### Prerequisites

You are assigned the *Manage Applications* role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].

#### Context

The application's display name appears on the left side of the logon and registration pages of the applications that use Identity Authentication for authentication. You set this name when you first create your application in the administration console for Identity Authentication, and you can change it later. For more information, see Create a New Application [page 43] and Change an Application's Display Name [page 49].

By default, the display name of the application is set to appear on the logon page.
Caution
Be careful when you switch off the display of the application name. The users might not be sure which application they are providing their credentials for.

Tip
Instead of leaving the left side of the logon page blank you can add an application’s logo. For more information, see Configure a Logo for an Application [page 90].

To configure the appearance of the application’s name on the logon page, proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
   This operation opens a list of the applications.
3. Choose the application that you want to edit.

   **i Note**
   
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.

   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the **Branding and Layout** tab.

5. Under **BRANDING**, enable or disable the appearance of the application name on the logon page.

   Once the application has been updated, the system displays the message **Application <name of application> updated**.

**Results**

Depending on your choice, the display name of the application is visible or hidden on the logon page.

### 1.5.1.13 Configure a Branding Style for an Application

For the configuration of the branding style, you can choose a style for the logon, registration, and upgrade forms. You can also customize the buttons on these forms.

**Context**

You can use one of the following styles:

- **Default Theme**
  
  This predefined theme includes white and brand blue coloring based on SAP Fiori’s color palette.

  **i Note**
  
  This is the default setting.

- **Custom Theme**
  
  The custom theme allows you to configure a custom branding style for the buttons and information messages. It uses the Default theme for all other elements on the screens and error pages. For this configuration, you can customize:

  - the top and bottom background color of the button
  - the background color of the information message in the forms
  - the button’s and information message’s border line color
  - and the color of the button’s text
Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the *Applications* tile.
   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   **i Note**
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.

   If you do not have a created application in your list, you can create one. For more information, see [Create a New Application [page 43]].

4. Choose the *Branding and Layout* tab.

5. Under *BRANDING*, choose the *Branding Style* list item

6. Select the color theme.

   If your option is *Custom Theme*, configure the colors. To configure the colors, you can use the color picker or enter the color’s hexadecimal value.

   See the table below for more information about the buttons and screens that can be customized.

<table>
<thead>
<tr>
<th>Color Picker</th>
<th>Customized Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>Background Top Color</td>
<td>○ button’s background top color in all screens</td>
</tr>
<tr>
<td></td>
<td>○ information’s message background color in the <em>Forget Password</em> screen</td>
</tr>
<tr>
<td>Background Bottom Color</td>
<td>○ button’s background bottom color in all screens</td>
</tr>
<tr>
<td></td>
<td>○ the button’s background color when the mouse is hovered on it in all screens</td>
</tr>
<tr>
<td></td>
<td>○ information’s message border color in the <em>Forget Password</em> screen</td>
</tr>
<tr>
<td>Border Color</td>
<td>the button's border color in all screens</td>
</tr>
<tr>
<td>Text Color</td>
<td>the text in the buttons in all screens</td>
</tr>
</tbody>
</table>

7. Save your selection

   Once the application has been changed, the system displays the message *Theme changed to <name of theme>*.
1.5.1.14 Enable or Disable Reload Parent Page Option

You can enable or disable the reload of the application's parent page after a successful logon.

Context

The Reload Parent Page option specifies whether the application's parent page reloads or not after a successful logon via an overlay page.

i Note

By default the Reload Parent Page option is enabled. Disable the option if you would like to embed the logon page in your custom iFrame.

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   i Note
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   i Note
   
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
   
   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].
4. Choose the *Branding and Layout* tab.
5. Under *LOGIN PAGE BEHAVIOR*, configure the *Reload Parent Page* option.

Once the application has been updated, the system displays the message *Application <name of application> updated.*

### 1.5.1.15 Define an E-Mail Template Set for an Application

Tenant administrators can define the e-mail template set that the application uses.

**Context**

Initially, the application uses a default template set with an English language version for all the templates in the set. This template set is named *Default*. If you want to use another e-mail template set, assign it to the respective application.

<table>
<thead>
<tr>
<th>i Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Both the HTML and TXT formats are included in the e-mails sent to a user. What the user sees, depends on the settings of his or her e-mail client.</td>
</tr>
</tbody>
</table>

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

<table>
<thead>
<tr>
<th>i Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The URL has the <code>https://&lt;tenant ID&gt;.accounts.ondemand.com/admin</code> pattern.</td>
</tr>
<tr>
<td><em>Tenant ID</em> is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the <em>tenant ID</em>.</td>
</tr>
</tbody>
</table>

2. Choose the *Applications* tile.
   
   This operation opens a list of the applications.

3. Choose the application that you want to edit.

<table>
<thead>
<tr>
<th>i Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.</td>
</tr>
<tr>
<td>If you do not have a created application in your list, you can create one. For more information, see <em>Create a New Application</em> [page 43].</td>
</tr>
</tbody>
</table>
4. Choose the **Branding and Layout** tab.
5. Under **E-MAIL CONFIGURATIONS**, choose **E-Mail Template Set**.
6. Select the radio button of the e-mail template set the application will use.
7. Save your selection.

Once the application has been updated, the system displays the message Application <name of application> updated.

### Next Steps

(Optional) Configure custom mail server. To use own mail server for the e-mails sent for the different application processes, you should configure your mail server in the administration console for Identity Authentication.

For more information, see [Configure Mail Server for Application Processes](page 161).

### Related Information

- [Troubleshooting for Administrators](page 298)
- [Create a New Application](page 43)

### 1.5.1.16 Configure Registration and Upgrade Forms

In the administration console, you can configure which user attributes Identity Authentication sends to the service provider or client (relying party) to be displayed on application’s registration and upgrade forms. After the user has filled in the form, the information from these attributes is recorded in the user’s profile. This is why these attributes are also called profile attributes and are handled by the profile services.

**i Note**

The user ID attribute cannot be controlled by the user. Because of that it is not included on the registration and upgrade forms, but is available in the user’s profile.

### Context

To configure the profile attributes, you need to specify which personal, company, and contact information the application prompts the user to provide when registering or upgrading. The information that the user has to provide depends on the status of the attribute (required or optional). You configure which attributes are displayed as required or optional in the administration console for Identity Authentication.
The list of the attributes includes:

**PERSONAL INFORMATION**

- Salutation
- First Name
- Middle Name
- Last Name
- E-mail
- Password

**Note**

The Last Name, E-mail, and Password attributes are always required for user registration or upgrade, so they are not configurable.

- Phone

**Note**

The Phone attribute becomes required and not configurable for user registration or upgrade, when Phone Verification via SMS is enabled. For more information, see Configure Registration and Upgrade Forms [page 97].

If you disable Phone Verification via SMS, the Phone attribute remains required for user registration or upgrade. To make it optional, or remove it, follow the procedure in this document.

- Street Address
- Street Address 2
- City
- Zip/Postal Code
- Country

**Note**

The Country parameter is required when the Zip/Postal Code is filled in by the user in the registration form. For example, this is the situation when both Zip/Postal Code and Country are optional, and the user fills in the Zip/Postal Code field. If the user deletes the information in the Zip/Postal Code the Country parameter becomes optional.

- State/Province

**Note**

The State/Province attribute is configurable only if the Country attribute is enabled.

**COMPANY INFORMATION**

- Company
- Street Address
- Street Address 2
- City
• ZIP/Postal Code
• Country

**i Note**

The Country parameter is required when the Zip/Postal Code is filled in by the user in the registration form. For example, this is the situation when both Zip/Postal Code and Country are optional, and the user fills in the Zip/Postal Code field. If the user deletes the information in the Zip/Postal Code the Country parameter becomes optional.

• State/Province

**i Note**

The State/Province attribute is configurable only if the Country attribute is enabled.

• Industry
• Relationship
• Job Function

**CONTACT PREFERENCES**

• By E-mail
• By Telephone

**i Note**

The CONTACT PREFERENCES attributes define if the self-registration form contains a section Contact Preferences. This section asks the user if he or she would like to be contacted by e-mail or phone, or both.

The presence of this section depends also on the Country attribute. The legislation in some countries requires the user to explicitly agree that he or she would like to be contacted by e-mail or phone, or both.

Based on the specific configuration, the following options are possible:

- If one or both CONTACT PREFERENCES parameters are enabled, and both Country parameters are disabled the Contact Preferences section will appear in the registration form.
- If one or both Country parameters and one or both CONTACT PREFERENCES parameters are enabled, the Contact Preferences section will appear in the registration form if the user types at least one country which requires the user to explicitly agree that he or she would like to be contacted by e-mail or phone, or both.
- If both CONTACT PREFERENCES parameters are disabled, the "Contact Preferences" section will not appear in the registration form.

For the full set of the countries that do not require the user to explicitly agree that he or she would like to be contacted by e-mail or phone copy the respective URL listed below, replace `<tenant ID>` with your Tenant ID, and open the edited URL in a Web browser.
In addition to these profile attributes, the registration and upgrade forms include terms of use and privacy policy documents that are configured separately.

To configure profile attributes, proceed as follows:

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
   
   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   **i Note**
   
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
   
   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Branding and Layout tab.

5. Under APPLICATION FORMS CUSTOMIZATION, choose Registration Form.

6. Configure which attributes the form displays as required or optional, and save your selection.

   If the operation is successful, you receive the message **Registration form updated.**
1.5.1.17 Protecting Self-Registration with Phone Verification

Tenant administrators can configure applications to require new self-registered users to verify themselves via SMS codes sent to their mobile phones.

**Context**

Applications with self-registration process can verify newly created users via a code sent as an SMS to their mobile phones. The applications can therefore protect against users creating numerous dummy accounts.

Newly created users are required to provide their phone numbers during the self-registration process. For more information about how to allow self-registration, see Configure User Access to the Application [page 87].

Existing users are required to provide their phone numbers in the upgrade form.

→ Remember

Once the phone is verified, the user cannot change it any more on the profile page. This can be done by the administrator via the administration console. For more information, see List and Edit User Details [page 205].

Example

Michael Adams is an administrator at retail company A. He has configured his system in such a way that users can register on their own and then purchase from the company’s site. He allows users to access his Company A Purchasing application by self-registration.

Michael also wants to restrict users to create dummy accounts. To do this, he configures SAP Authentication 365 service and enables the Phone Verification via SMS option in the administration console for Identity Authentication.

Donna Moore is a customer who wants to purchase goods from company A for the first time. When she accesses company A’s application, she is redirected to the company’s logon page. Because she is not registered yet, she has to choose the Register button to start the registration process. A registration form then appears, prompting Donna to enter her name, e-mail address, and telephone number, and to accept the organization’s terms of use and privacy policy. The telephone number is required when the Phone Verification via SMS option is enabled. When she submits the form, she receives an e-mail with instructions on how to activate her registration. Once she has activated her registration, she receives a code via SMS. At the same time she is redirected to a page where she is prompted to verify her phone number by entering...
the code she received. Once she has verified the phone number, she is able to log on to the retailing application with her user credentials.

Julie Armstrong is a customer who has an account for company A, but she has never provided her phone number. When she accesses company A’s application, she is redirected to the company’s logon page. After she provides her credentials, Julie is required to enter her phone number. She receives a code via SMS, and at the same time is redirected to a page where she is prompted to verify the phone by entering the code she received. Once she has verified the phone number, she is able to log on to the retailing application with her user credentials.

Configuration of phone verification in the administration console for Identity Authentication comprises two consecutive steps. As a prerequisite, you must have an account in SAP Authentication 365.

1. Configure SAP Authentication 365 in Administration Console [page 103]
2. Enable Phone Verification for an Application [page 104]

1. Configure SAP Authentication 365 in Administration Console [page 103]
   Configure SAP Authentication 365 to enable Phone Verification via SMS in the administration console.
2. Enable Phone Verification for an Application [page 104]
   Tenant administrators can enable phone verification via SMS code for an application.

Related Information

Protect your customers with SMS based end-to-end two factor authentication service
SAP Authentication 365 - Useful Links
1.5.17.1 Configure SAP Authentication 365 in Administration Console

Configure SAP Authentication 365 to enable *Phone Verification via SMS* in the administration console.

**Prerequisites**

- You have an account in SAP Authentication 365.
- You are assigned the *Manage Tenant Configuration* role. For more information about how to assign administrator roles, see [Edit Administrator Authorizations](#) [page 241].

**Context**

SAP Authentication 365 service enables multichannel two-factor authentication (2FA), adding another layer of security to customers' online accounts, beyond their login and password. The service enables you to configure tokens – such as one-time passwords (OTPs), personal identification numbers (PINs), and verification codes – that are tailored to businesses and particular use cases. For more information, see [SAP Authentication 365](#).

For the integration between Identity Authentication and SAP Authentication 365, you must make the following configuration steps in the administration console:

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   ![Note]
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   
   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

   2. Under *Applications and Resources*, choose the *Tenant Settings* tile.
   3. Choose the *SAP Authentication 365 Configuration* list item.
   4. Enter the required information.
   5. Save your entries.

   If the operation is successful, you receive the message *SAP Authentication 365 saved.*

**Task overview:** [Protecting Self-Registration with Phone Verification](#) [page 101]
Next task: Enable Phone Verification for an Application [page 104]

1.5.1.17.2 Enable Phone Verification for an Application

Tenant administrators can enable phone verification via SMS code for an application.

Prerequisites

- You have an account in SAP Authentication 365.
- You have configured SAP Authentication 365 service. For more information, see Configure SAP Authentication 365 in Administration Console [page 103].

Context

This option requires the user to provide his or her phone number in the registration or upgrade forms. When this feature is enabled, the Phone attribute becomes required and is not configurable for user registration or upgrade. For more information, see Configure Registration and Upgrade Forms [page 97].

Once the phone number has been verified, the user cannot change it any more on the profile page. This can be done by the administrator via the administration console. For more information, see List and Edit User Details [page 205].

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern. Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   i Note
   
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the **Branding and Layout** tab.

5. Under **APPLICATION FORMS CUSTOMIZATION**, enable **Phone Verification via SMS**.

If the operation is successful, you receive the following message: Application `<Application Name>` updated. The slider is switched to **ON**.

**Note**

If you do not want to use phone verification via SMS for an application, you can drag the slider next to it to **OFF**.

6. **Optional**: Configure rules to skip phone verification for user types and save your changes. To configure the authentication rules, choose one of the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a new rule</td>
<td>See Add a New Phone Verification Rule [page 106].</td>
</tr>
<tr>
<td>Delete an existing rule</td>
<td>Choose the delete 🗑️ icon next to the rule you want to delete.</td>
</tr>
</tbody>
</table>

If the operation is successful, the system displays the message **Verification rules updated**.

**Results**

Newly created users are required to provide their phone numbers during the self-registration process.

Existing users are required to provide their phone numbers in the upgrade form.

Users should enter the code sent by SMS to their phones in order to finish the validation process.

**Remember**

Once the phone number has been verified, the user cannot change it on the profile page.

**Task overview**: Protecting Self-Registration with Phone Verification [page 101]

**Previous task**: Configure SAP Authentication 365 in Administration Console [page 103]
1.5.1.17.2.1 Add a New Phone Verification Rule

You can add rules to skip phone verification for user types.

Context

Each rule contains the following information:

- **Action**
  You can choose the *Skip* action. Users of the selected user type in the rule will not be prompted to verify their phones when the *Phone Verification Via SMS* option is enabled.

- **User Type**
  Specify the type, which the user must have.

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **Note**
   The URL has the **https://<tenant ID>.accounts.ondemand.com/admin** pattern.
   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the *Applications* tile.
   This operation opens a list of the applications.

3. Choose the list item of the application that you want to edit.

   **Note**
   If you do not have a created application in your list, you can create one. For more details, see Related Information.

   **Caution**
   The list also includes the *Administration Console* application. If you enable risk-based authentication for that application, make sure that you, as a tenant administrator, meet the authentication rules and the default authentication rule. Otherwise when you log out of the administration console you will not be able to log in it again if you don't meet the rules.

   If *Administration Console* is not in the list of the applications you may request it. To do this, you need to report an incident with a subject on SAP Support Portal Home under the component BC-IAM-IDS.
4. Choose the Branding and Layout tab.
5. Under Application Forms Customization, choose hone Verification Via SMS.
6. Choose Add Rule.
7. Fill in the fields on the New Verification Rule window.
8. Confirm your changes.
9. Choose Save.

If the operation is successful, the system displays the message Verification rules updated.

Related Information

Add a New Phone Verification Rule [page 106]
Protecting Self-Registration with Phone Verification [page 101]

1.5.1.18 Protecting Application Forms with Google reCAPTCHA

Tenant administrators can use Google reCAPTCHA to protect the application forms of Identity Authentication from spam and abuse.

SAP Cloud Platform Identity Authentication service has integrated Google’s Invisible reCAPTCHA service. The aim is to prevent software applications that run automated tasks to flood Identity Authentication.

→ Remember

At present, you can protect the registration form of Identity Authentication.

To use reCAPTCHA for your registration form, you must have allowed self-registration for the application. For more information, see Configure User Access to the Application [page 87]. Choose Public access.

reCAPTCHA is provided in the form of a widget that is visible on the protected application form. If the reCAPTCHA service suspects that the user is not a human, a popup with a challenge appears prompting the user to solve a CAPTCHA. By default, only the most suspicious traffic is affected. For more details about Google reCAPTCHA, see Related Information.

Configuration of reCAPTCHA for the different application forms of Identity Authentication comprises three consecutive steps:

1. Get Site key and Secret key from Google
2. Configure reCAPTCHA in administration console
3. Enable reCAPTCHA for application forms

- Get Site Key and Secret Key from Google for reCAPTCHA [page 108]
Configure Google reCAPTCHA in Administration Console [page 109]

Enable Google reCAPTCHA for Application Forms [page 110]

1. Get Site Key and Secret Key from Google for reCAPTCHA [page 108]
   Register the domain of the application and get a Site key and Secret key from Google.

2. Configure Google reCAPTCHA in Administration Console [page 109]
   Configure Google reCAPTCHA for your Identity Authentication tenant.

3. Enable Google reCAPTCHA for Application Forms [page 110]
   Enable Google reCAPTCHA for the specific form or forms of the application.

Related Information

Google reCAPTCHA
reCAPTCHA
Making the Internet safer and faster: Introducing reCAPTCHA Android API

1.5.1.18.1 Get Site Key and Secret Key from Google for reCAPTCHA

Register the domain of the application and get a Site key and Secret key from Google.

Prerequisites

You have a Google account.

Procedure

1. Log on to your Google account.
3. Select the Invisible reCAPTCHA radio button.
4. Register your domain.

→ Remember

Your domain is the URL of your Identity Authentication tenant. It has the <tenant ID>.accounts.ondemand.com pattern.

Tenant ID is automatically generated by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.
5. Save your Site key and your Secret key. You need them for the configuration steps in the administration console for Identity Authentication.

**Task overview:** Protecting Application Forms with Google reCAPTCHA [page 107]

**Next task:** Configure Google reCAPTCHA in Administration Console [page 109]

### 1.5.1.18.2 Configure Google reCAPTCHA in Administration Console

Configure Google reCAPTCHA for your Identity Authentication tenant.

**Prerequisites**

You have registered the domain of the application and received a Site key and Secret key from Google. For more information, see Get Site Key and Secret Key from Google for reCAPTCHA [page 108].

**Procedure**

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   **Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Under *Applications and Resources*, choose the *Tenant Settings* tile.
3. Choose the *Google reCAPTCHA* list item.
4. Enter the *Site Key* and *Secret Key* you received from Google for reCAPTCHA.
5. Save your changes.

**Task overview:** Protecting Application Forms with Google reCAPTCHA [page 107]

**Previous task:** Get Site Key and Secret Key from Google for reCAPTCHA [page 108]

**Next task:** Enable Google reCAPTCHA for Application Forms [page 110]
Enable Google reCAPTCHA for Application Forms

Enable Google reCAPTCHA for the specific form or forms of the application.

Prerequisites

- You have registered the domain of the application and received a Site key and Secret key from Google. For more information, see Get Site Key and Secret Key from Google for reCAPTCHA [page 108].
- You have configured the Google reCAPTCHA option in the administration console for Identity Authentication. For more information, see Configure Google reCAPTCHA in Administration Console [page 109].

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The URL has the https://&lt;tenant ID&gt;.accounts.ondemand.com/admin pattern.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.</td>
</tr>
</tbody>
</table>

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].</td>
</tr>
</tbody>
</table>

4. Choose the Branding and Layout tab.

5. Under APPLICATION FORMS CUSTOMIZATION, choose Google reCAPTCHA Protection.

6. Enable Google reCAPTCHA protection for the relevant application form.

<table>
<thead>
<tr>
<th>Remember</th>
</tr>
</thead>
<tbody>
<tr>
<td>At present, you can enable Google reCAPTCHA protection for the registration form.</td>
</tr>
</tbody>
</table>

7. Save your configuration.
If the operation is successful, you receive the following message: Application <Application Name> updated. The slider next to enabled application form is switched to **ON**.

**Note**

If you do not want to use reCAPTCHA protection for an application form, you can drag the slider next to it to **OFF**.

**Task overview:** Protecting Application Forms with Google reCAPTCHA [page 107]

**Previous task:** Configure Google reCAPTCHA in Administration Console [page 109]

### 1.5.1.19 Authenticating Identity Provider for an Application

This document shows you how to choose an authenticating identity provider for an SAML 2.0 application.

**Context**

You have the following options for an authenticating identity provider in the administration console for SAP Cloud Platform Identity Authentication service:

- **Local Identity Provider**
  
  SAP Cloud Platform Identity Authentication is set as the default local identity provider.
  
  The local identity provider gives you access to all application settings in the administration console for Identity Authentication

- **Corporate Identity Provider**
  
  SAP Cloud Platform Identity Authentication service can act as a proxy to delegate authentication to the external corporate identity provider.

Based on your scenario you can:

- **Choose Default Identity Provider**
- **Configure Logon via Identity Authentication**
- **Configure Conditional Authentication**
- **Enable IdP-Initiated SSO from All Corporate IdPs**

- **Choose Default Identity Provider for an Application** [page 112]
- **Configure Logon via Identity Authentication when a Corporate IdP is Chosen as Default** [page 114]
- **Configure Conditional Authentication for an Application** [page 119]
- **Enable IdP-Initiated SSO from All Corporate IdPs** [page 127]
Configure Logon via Identity Authentication when a Corporate IdP is Chosen as Default [page 114]
You can allow users to log on via SAP Cloud Platform Identity Authentication service when a corporate identity provider (IdP) is chosen as default.

Configure Conditional Authentication for an Application [page 119]
Tenant administrator can define rules for authenticating identity provider according to e-mail domain, user type, user group, and IP range (specified in CIDR notation).

Enable IdP-Initiated SSO from All Corporate Identity Providers [page 127]
Tenant administrators can enable IdP-initiated single sign-on (SSO) from all configured corporate identity providers (IdPs).

Related Information

Corporate Identity Providers [page 243]
Configure Trust with Corporate Identity Provider [page 256]
Edit Administrator Authorizations [page 241]

1.5.1.19.1 Choose Default Identity Provider for an Application

You choose between a local identity provider and a corporate identity provider to be the default identity provider for your application.

Prerequisites

- You are assigned the Manage Corporate Identity Providers role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
- You have a configured corporate identity provider. For more information how to configure a corporate identity provider, see Related Information.
- You haven’t added any rules for authentication. For more information, see Configure Conditional Authentication for an Application [page 119].

Context

In this scenario you choose which is the default identity provider. It can be either the local identity provider (SAP Cloud Platform Identity Authentication) or a corporate identity provider.

Initially SAP Cloud Platform Identity Authentication is set as the default local identity provider.

This choice gives you access to all application settings in the administration console for Identity Authentication.
If the choice is a corporate identity provider, SAP Cloud Platform Identity Authentication service acts as a proxy to delegate authentication to the external corporate identity provider. For more information, see Corporate Identity Providers [page 243]

When you select a corporate identity provider, you are not able to access the custom configurations for the applications. The Authentication and Access and Branding and Layout tabs will not be visible.

<table>
<thead>
<tr>
<th>Restriction</th>
</tr>
</thead>
<tbody>
<tr>
<td>The option to choose an identity provider for the system applications is disabled. The default setting for these applications is SAP Cloud Platform Identity Authentication.</td>
</tr>
</tbody>
</table>

To choose a default identity provider for an application, proceed as follows:

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

<table>
<thead>
<tr>
<th>i Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The URL has the https://&lt;tenant ID&gt;.accounts.ondemand.com/admin pattern.</td>
</tr>
</tbody>
</table>

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the Applications tile.
   
   This operation opens a list of the applications.

3. Choose the application that you want to edit.

<table>
<thead>
<tr>
<th>i Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.</td>
</tr>
</tbody>
</table>

   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.
5. Under CONDITIONAL AUTHENTICATION, choose Conditional Authentication.
6. Select from the drop down the identity provider that the application will use as the default identity provider.
7. Save your changes.

   Once the application has been updated, the system displays the message Conditional Authentication updated.

   The application will use only the chosen identity provider for authentication.

   If you select the local identity provider, you will able to access the custom configurations for the applications.
If you select a corporate identity provider, you will not be able to access the custom configurations for the applications. The Authentication and Access and Branding and Layout tabs will not be visible. The user will be prompted to provide credentials in a single logon page.

8. **Optional:** (When a corporate identity provider is chosen as default identity provider) Enable the Allow Identity Authentication Users Log On option. For more information see, *Enable the Allow Identity Authentication Users Log On Option [page 117]*.

**Task overview:** *Authenticating Identity Provider for an Application [page 111]*

**Related Information**

- Configure Logon via Identity Authentication when a Corporate IdP is Chosen as Default [page 114]
- Configure Conditional Authentication for an Application [page 119]
- Enable IdP-Initiated SSO from All Corporate Identity Providers [page 127]
- Configure Logon via Identity Authentication when a Corporate IdP is Chosen as Default [page 114]

### 1.5.1.19.2 Configure Logon via Identity Authentication when a Corporate IdP is Chosen as Default

You can allow users to log on via SAP Cloud Platform Identity Authentication service when a corporate identity provider (IdP) is chosen as default.

**Context**

When a corporate identity provider is chosen as default, Identity Authentication acts as a proxy to delegate authentication to that external corporate identity provider. In this scenario, Identity Authentication acts as a SAML 2.0 identity provider to the service provider (application), and as a service provider to the corporate identity provider. When a user, for example an employee who exists in the user store of the corporate identity provider tries to access protected resource in the application, he or she is redirected by Identity Authentication to the corporate identity provider. The user is logged on, after providing the correct corporate credentials.

You can extend this scenario, allowing users that are stored in Identity Authentication to log on with their cloud credentials. These cloud users access the application, and are authenticated via Identity Authentication. Thus, in the extended scenario, the employees, log on to the application with their corporate credentials, while the external users, such as clients, or partners are authenticated via Identity Authentication. The IdP-initiated logon link that the external users should use to access the application is provided in the administration console of the Identity Authentication tenant.

---

**i Note**

If you have configured a connection to a corporate user store, users with user records in Identity Authentication also can log on when the Allow Identity Authentication Users Log On option is enabled.
To configure the logon via Identity Authentication when a corporate identity provider is chosen as default, follow the procedures below:

**i Note**

If you have already configured a corporate identity provider as default identity provider, skip Choose a Corporate Identity Provider as Default [page 116] and proceed with Enable the Allow Identity Authentication Users Log On Option [page 117].

1. **Choose a Corporate Identity Provider as Default [page 116]**
   You choose a corporate identity provider to be the default identity provider for your application.

2. **Enable the Allow Identity Authentication Users Log On Option [page 117]**
   You can enable the **Allow Identity Authentication Users Log On** Option. Thus users can log on with their SAP Cloud Platform Identity Authentication service credentials, when a corporate identity provider is selected as default.

**Task overview:** Authenticating Identity Provider for an Application [page 111]

**Related Information**

Choose Default Identity Provider for an Application [page 112]
Configure Conditional Authentication for an Application [page 119]
Enable IdP-Initiated SSO from All Corporate Identity Providers [page 127]
Corporate User Store [page 139]
1.5.1.19.2.1 Choose a Corporate Identity Provider as Default

You choose a corporate identity provider to be the default identity provider for your application.

Prerequisites

- You are assigned the Manage Corporate Identity Providers role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
- You have a configured corporate identity provider. For more information how to configure a corporate identity provider, see Corporate Identity Providers [page 243].

Context

To choose a corporate identity provider as default, follow the procedures:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   Note
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.

   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.

5. Under CONDITIONAL AUTHENTICATION, choose Conditional Authentication.

6. Select from the drop down the corporate identity provider that the application will use as the default identity provider.
7. Save your changes. Once the application has been updated, the system displays the message Conditional Authentication updated.

Results

When the choice is a corporate identity provider, you are not able to access the custom configurations for the applications. The Authentication and Access and Branding and Layout tabs are not visible.

Task overview: Configure Logon via Identity Authentication when a Corporate IdP is Chosen as Default [page 114]

Next task: Enable the Allow Identity Authentication Users Log On Option [page 117]

1.5.1.19.2.2 Enable the Allow Identity Authentication Users Log On Option

You can enable the Allow Identity Authentication Users Log On Option. Thus users can log on with their SAP Cloud Platform Identity Authentication service credentials, when a corporate identity provider is selected as default.

Prerequisites

You have chosen a corporate identity provider as default. For more information, see Choose a Corporate Identity Provider as Default [page 116].

Context

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

> Note

The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
   This operation opens a list of the applications.
3. Choose the application that you want to edit.

   **Note**
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.
5. Under CONDITIONAL AUTHENTICATION, enable the Allow Identity Authentication Users Log On option.

   **Note**
   By default this option is disabled.

   Once the application has been updated, the system displays the message Application <name of application> updated.

**Results**

When you enable Allow Identity Authentication Users Log On, the Authentication and Access and Branding and Layout tabs appear. You can access the custom configurations for the application.

**Task overview:** Configure Logon via Identity Authentication when a Corporate IdP is Chosen as Default [page 114]

**Previous task:** Choose a Corporate Identity Provider as Default [page 116]
1.5.19.3 Configure Conditional Authentication for an Application

Tenant administrator can define rules for authenticating identity provider according to e-mail domain, user type, user group, and IP range (specified in CIDR notation).

Prerequisites

You are assigned the Manage Applications role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].

Context

Tenant administrator can control the access to an application by defining different rules for the authenticating identity provider. Based on these rules users are authenticated either via a corporate identity provider or via SAP Cloud Platform Identity Authentication.

Rules

The added rules are displayed sorted by priority.

If a rule contains only IP Range, and it is first in list or only one, Identity Authentication does not request the user to provide user identifier in the logon screen. The system evaluates whether that user meets all the criteria of the rule. The evaluation starts with the rule with the highest priority, until the criteria of a rule are met. If the criteria of a rule are met, the rest of the conditions are not evaluated.

If apart from IP Range the rule contains other conditions, or it is not the first in the list, Identity Authentication requests the user to provide user identifier in the logon screen. When a user types the user identifier in the log on page, the system evaluates whether that user meets all the criteria of the rule. The evaluation starts with the rule with the highest priority, until the criteria of a rule are met. If the criteria of a rule are met, the rest of the conditions are not evaluated.

→ Remember

Rules can be defined only if the default identity provider is SAP Cloud Platform Identity Authentication.

If you have already defined rules, they won’t be considered if you change the default identity provider from SAP Cloud Platform Identity Authentication to a corporate identity provider.

If the user is already existing in Identity Authentication, authentication requests via X509 certificate, SPNEGO, existing session, remember me, and token will be processed by Identity Authentication in case of successful authentication no matter of the conditional authentication rules.

Default Identity Provider

If non-prompt based authentication (X509 certificate, SPNEGO, existing session, remember me, and token) is successful, the user is authenticated without checking the rules via Identity Authentication. Otherwise, the user will be asked to provide identifier to evaluate the conditional authentication rules.
If none of the rules meets the criteria, SAP Cloud Platform Identity Authentication is chosen for authentication.

**Conditional Authentication Flow**

The tenant administrator has configured Conditional Authentication in the administration console for Identity Authentication. In this setup, the employees should be authenticated via SAP Cloud Platform Identity Authentication, while the customers via the corporate identity provider.

**Authentication via Corporate Identity Provider**

1. The user tries to access the application.
2. The application redirects the request to SAP Cloud Platform Identity Authentication to check the rules.
3. SAP Cloud Platform Identity Authentication requests the user to provide user identifier in the logon screen.

   → Remember
   
   If the rule contains only **IP Range** SAP Cloud Platform Identity Authentication does not request the user to provide user identifier in the logon screen. This step is skipped for this scenario.
   
   If apart from **IP Range** the rule contains other conditions, this step is executed.

4. The user provides user identifier. Identity Authentication stores the user identifier in a persistent cookie in the browser. The persistent cookie expires in three months.

   → Remember
   
   If the rule contains only **IP Range** SAP Cloud Platform Identity Authentication does not request the user to provide user identifier in the logon screen. This step is skipped for this scenario.
   
   If apart from **IP Range** the rule contains other conditions, this step is executed.

5. According to the rules, the user should be authenticated via the corporate identity provider. Identity Authentication sends the user identifier as **login_hint** parameter to the corporate identity provider.

   → Remember
   
   The user identifier from step 3 is required at the first logon. After that, based on the persistent cookie, the user is redirected directly to the logon screen of the corporate identity provider.
If the user wants to log on with another identifier, he or she must delete the browser cookies. When the persistent cookie expires, the user is again requested to provide user identifier in the logon screen.

6. If the corporate identity provider supports the `login_hint` parameter, then it requests only the user password. If the corporate identity provider does not support the `login_hint` parameter, it requires both the user identifier and password.

7. Depending on the support of the `login_hint`, user provides only password, or both user identifier and password.

8. The corporate identity provider grants access to the user.

**Result**

The user logs on to the application.

**Authentication via Identity Authentication with X509 certificate.**

1. The user tries to access the application with provided X509 certificate.
2. The application redirects the request to SAP Cloud Platform Identity Authentication where the certificate is taken as credential, and user is authenticated without checking the rules.
3. Identity Authentication grants access to the user.

**Result**

The user logs on to the application via X509 certificate

**Authentication via Identity Authentication**
1. The user tries to access the application.
2. The application redirects the request to SAP Cloud Platform Identity Authentication to check the rules.
3. Identity Authentication request the user to provide user identifier in the log on screen.

→ Remember

If the rule contains only IP Range SAP Cloud Platform Identity Authentication does not request the user to provide user identifier in the logon screen. This step is skipped for this scenario.

If apart from IP Range the rule contains other conditions, this step is executed.

4. The user provides user identifier.

→ Remember

If the rule contains only IP Range SAP Cloud Platform Identity Authentication does not request the user to provide user identifier in the logon screen. This step is skipped for this scenario.

If apart from IP Range the rule contains other conditions, this step is executed.

5. According to the rules, the user should be authenticated via Identity Authentication. The user is prompted to provide password. The user identifier is prefilled in the logon screen.

6. User provides password.
7. Identity Authentication grants access to the user.

Result

The user logs on to the application.

i Note

Social sign-on and account linking is supported only when the user does not meet the configured rules for conditional authentication.
Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   i Note
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.

5. Under CONDITIONAL AUTHENTICATION, choose Conditional Authenticating Identity Providers.

6. Configure the rules. To configure the rules, choose one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a new rule</td>
<td>See Add a New Authentication Rule [page 124].</td>
</tr>
<tr>
<td>Edit an existing rule</td>
<td>Choose the icon next to the rule you want to edit.</td>
</tr>
<tr>
<td>Delete an existing rule</td>
<td>Choose the delete icon next to the rule you want to delete.</td>
</tr>
<tr>
<td>Reprioritize rules</td>
<td>Use the arrows to reprioritize the rules.</td>
</tr>
</tbody>
</table>

7. Choose the default identity provider.

   ! Restriction
   Rules can be defined only if the default identity provider is SAP Cloud Platform Identity Authentication.

8. Save your changes.

   Once the application has been updated, the system displays the message Conditional Authentication updated.
Setting Conditional Authentication

Donna Moore is an administrator of Company A. She wants to configure Identity Authentication so that the employees who log on with their corporate e-mails to be authenticated via the company's corporate identity provider. The clients and partners of Company A should be authenticated via SAP Cloud Platform Identity Authentication service. For this purpose, Donna creates the following authentication rule:

<table>
<thead>
<tr>
<th>Authentication Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Provider</td>
</tr>
<tr>
<td>Company A Corporate IdP</td>
</tr>
</tbody>
</table>

Default Identity Provider: SAP Cloud Platform Identity Authentication

Michael Adams is an employee of Company A and as such he wants to create a leave request. He chooses the logon link on the application and is prompted to provide his e-mail. After that he chooses Continue and is redirected to the logon screen of Company A. There he has to provide his user identifier and password. After providing the correct credentials he logs on to the application.

Julie Armstrong is a customer of Company A. She accesses the company's application and chooses the logon link on the application and is prompted to provide her e-mail. After that she chooses Continue and is redirected to the log on screen of Identity Authentication where she is prompted to provide her password. Her e-mail is prefilled by the system. After providing the correct password she logs on to the application.

Task overview: Authenticating Identity Provider for an Application [page 111]

Related Information

Choose Default Identity Provider for an Application [page 112]
Configure Logon via Identity Authentication when a Corporate IdP is Chosen as Default [page 114]
Enable IdP-Initiated SSO from All Corporate Identity Providers [page 127]

1.5.1.19.3.1 Add a New Authentication Rule

You can add rules for authentication against different identity providers.

Prerequisites

You are assigned the Manage Applications role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
Each rule contains the following information:

- **Identity Provider**
  Define the identity provider that will be used for authentication. The dropdown list includes the local identity provider and all corporate identity providers that are created in the administration console for Identity Authentication. The corporate identity providers must be configured in the administration. For more information, see Corporate Identity Providers [page 243].

  ➔ Remember
  This field is required.

- **Domain**
  Specify the domain of the e-mail address that comes after the @ symbol. If no domain entered, the rule is valid for any domain.

- **User Group**
  Specify the user group, which the authenticating user must be part of. If no user group is selected, the rule is valid for any of the groups.
  The user groups must be configured in the administration console for SAP Cloud Platform Identity Authentication service. For more information, see User Groups [page 216].

  i Note
  The authenticating user must exist in the user store of Identity Authentication for the User Group criteria to be checked properly.

- **User Type**
  Specify the type, which the authenticating user must have. If no user type is selected, the rule is valid for any of the types.

  i Note
  The authenticating user must exist in the user store of Identity Authentication for the Type criteria to be checked properly.

- **IP Range**
  Define the range of allowed IP addresses or proxies that the user logs on from. The value must be specified in Classless Inter-Domain Routing (CIDR) notation.

  i Note
  By default the field is empty, meaning that any IP is allowed.

  ❖ Example
  Enter 123.45.67.1/24 to allow users to log on from any IP starting with 123.45.67.

  If no IP range is defined, the rule is valid for all IP ranges.

  ➔ Remember
  The fields Domain, User Group, User Type, and IP Range are not mandatory, but at least one of them has to be specified.
**Procedure**

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   **i Note**

   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern. *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   **i Note**

   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.

   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.

5. Under *CONDITIONAL AUTHENTICATION*, choose *Conditional Authenticating Identity Providers*.


7. Fill in the fields on the New Rule window.

8. Confirm your changes.

**Related Information**

Create a New Application [page 43]
1.5.1.19.4 Enable IdP-Initiated SSO from All Corporate Identity Providers

Tenant administrators can enable IdP-initiated single sign-on (SSO) from all configured corporate identity providers (IdPs).

Prerequisites

- You are assigned the Manage Applications role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
- You have more than one corporate identity provider, which is configured in the administration console. For more information how to configure a corporate identity provider, see Configure Trust with Corporate Identity Provider [page 256].
- (For SAML 2.0 applications) You have added the assertion consumer (ACS) endpoint with the URL of the application’s protected page, and the index, in the metadata of that application. The ACS endpoint that you added should look like the following example:

```xml
<ns3:AssertionConsumerService index="1" isDefault="false" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://<application URL>/protected.jsp"/>
```

For more information how to configure your ACS endpoint in the administration for SAP Cloud Platform Identity Authentication service, see Configure SAML 2.0 Service Provider [page 55].

Context

Applications can be configured to trust all the corporate identity providers configured in the administration console when identity provider (IdP) initiated single sign-on (SSO) is used. The user accesses the application via URL provided by the corporate identity provider.

To enable IdP-initiated SSO with all corporate identity providers configured in the administration console for SAP Cloud Platform Identity Authentication service follow the procedure below:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   **i Note**
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.

5. Under CONDITIONAL AUTHENTICATION, enable the Trust All Corporate Identity Providers option.

   **i Note**
   By default this option is disabled.

   Once the application has been updated, the system displays the message Application <name of application> updated.

**Results**

The application trusts all corporate identity providers that are configured in the administration console for Identity Authentication.

Task overview: Authenticating Identity Provider for an Application [page 111]

**Related Information**

Choose Default Identity Provider for an Application [page 112]
Configure Logon via Identity Authentication when a Corporate IdP is Chosen as Default [page 114]
Configure Conditional Authentication for an Application [page 119]
Configure IdP-Initiated SSO with Corporate Identity Providers [page 244]
1.5.1.20 Mobile Single Sign-On

This document provides information about the mobile single sign-on (SSO) option.

The mobile single sign-on (SSO) option allows users to access applications protected with two-factor authentication without manually entering the one-time password (OTP) via SAP Authenticator.

Mobile single sign-on is applicable only when the applications are accessed via identity provider (IdP)-initiated single sign-on (SSO). For more details about IdP-initiated SSO, see Related Information.

You also have to comply with the URL requirements for these applications. Users can add applications in SAP Authenticator by scanning a QR code. The code can be sent to them by the administrator, or by typing the application’s URL. The URL must have the following format:

https://<tenant_ID>.accounts.ondemand.com/saml2/idp/sso?sp=<sp_name>\&RelayState=<sp_specific_value>\&index=<index_number>\&j_username=[user name]\&j_otpcode=[passcode]

**Note**

The QR code represents this URL. When SAP Authenticator calls the URL, it replaces [username] in the URL with the specified account name and [passcode] with two consecutive passcodes.

Related Information

Configure IdP-Initiated SSO [page 162]
Use the Remember Me Option [page 308]
One-Time Password Authentication User Guide

1.5.2 Configuring Tenant Settings

Initially, the tenants are configured to use default settings. This section describes how you as a tenant administrator can make custom tenant configurations.

Configuring Tenant Settings

<table>
<thead>
<tr>
<th>To learn about</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to configure a custom global logo on the forms for logon, registration, upgrade, password update, and account activation for all applications in a tenant</td>
<td>Configure a Tenant Logo [page 134]</td>
</tr>
<tr>
<td>How to configure the tenant’s name</td>
<td>Change a Tenant’s Display Name [page 139]</td>
</tr>
<tr>
<td>How to view and download tenant SAML 2.0 metadata</td>
<td>Tenant SAML 2.0 Configuration [page 130]</td>
</tr>
</tbody>
</table>
To learn about | See
---|---
How to view and edit the tenant OpenID Connect configuration | Tenant OpenID Connect Configuration [page 132]
How to upload a new signing certificate | Tenant SAML 2.0 Configuration [page 130]
How to configure the validity of the link sent to a user in the different application processes. | Configure E-Mail Link Validity [page 135]
How to configure the duration of the session. | Configure Session Timeout [page 136]
The corporate user store scenario and how to configure SAP Cloud Platform Identity Authentication service to connect with your corporate user store | Corporate User Store [page 139] and Configure Connection to a Corporate User Store [page 143]
How to configure Kerberos authentication | Configure Kerberos Authentication [page 153]
How to configure mail server to send e-mails for the application processes | Configure Mail Server for Application Processes [page 161]
How to disable or enable IdP-Initiated process via the administration console for SAP Cloud Platform Identity Authentication service. | Configure IdP-Initiated SSO [page 162]
How to protect an application when using responsive UIs, or embedded frames | Configure Trusted Domains [page 138]

### 1.5.2.1 Tenant SAML 2.0 Configuration

You as a tenant administrator can view and download the tenant SAML 2.0 metadata. You can also change the name format and the certificate used by the identity provider to digitally sign the messages for the applications.

**Context**

To view and download the tenant SAML 2.0 metadata, or to change the name format, or the default certificate, proceed as follows:

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern. Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Under Applications and Resources, choose the Tenant Settings tile.
3. Choose the SAML 2.0 Configuration list item. The SAML 2.0 Configuration page that opens displays the name of the identity provider, its endpoints, and its signing certificate.
4. You can choose between the following options:
   - To download the identity provider’s metadata, press the Download Metadata File button.
   - To change the default signing certificate, upload the new certificate as a file, or insert it as a text, and save your changes.

The new certificate must be a valid Base64-encoded X.509 certificate (.cer or .crt). Its public key must be the same as the public key of the default certificate. The certificate should not include the BEGIN and END tags.

If the change of the certificate is successful, the system displays the message Tenant <name of tenant> updated.

- To change the name format of the identity provider, choose the Name field, select the name format from the dropdown list, and save your changes. The dropdown list offers two options:

<table>
<thead>
<tr>
<th>Default Type</th>
<th>URL Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;tenant ID&gt;.accounts.ondemand.com</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com</td>
</tr>
</tbody>
</table>

By default Identity Authentication uses self signed certificates. The signing certificate can be a server’s self-signed certificate, a public root certificate, or a certificate belonging to a commercial Certificate Authority (CA).

To apply for a certificate, belonging to a commercial CA, you need a certificate signing request (CSR). To request the CSR, report an incident on SAP Support Portal Home with a component BC-IAM-IDS.

The new certificate must be a valid Base64-encoded X.509 certificate (.cer or .crt). Its public key must be the same as the public key of the default certificate. The certificate should not include the BEGIN and END tags.

Caution

You should change the name of the identity provider on the service provider side every time you change the name format of the identity provider in the administration console. If you have set
trusts with more than one service provider, change the name in every service provider. For more information about how to edit the name, see the documentation of the respective service providers.

If the change of the name is successful, the system displays the message Tenant <name of tenant> updated.

Related Information

Configuring Tenant Settings [page 129]
Troubleshooting for Administrators [page 298]
SAML 2.0 [page 283]

1.5.2.2 Tenant OpenID Connect Configuration

You as a tenant administrator can view the tenant OpenID Connect configuration. You can also change the name format, and the certificate used by the identity provider to digitally sign the messages for the applications.

Context

To view, or to change the name format, authorization or token endpoint, or the default certificate, proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Under Applications and Resources, choose the Tenant Settings tile.
3. Choose the OpenID Connect Configuration list item. The OpenID Connect Configuration page that opens displays the name of the identity provider, its endpoints, and its signing certificate.
4. You can choose between the following options:

- To change the default signing certificate, upload the new certificate as a file, or insert it as a text, and save your changes.

  **Note**

  By default Identity Authentication uses self signed certificates. The signing certificate can be a server’s self-signed certificate, a public root certificate, or a certificate belonging to a commercial Certificate Authority (CA).

  The new certificate must be a valid Base64-encoded X.509 certificate (.cer or .crt). Its public key must be the same as the public key of the default certificate. The certificate should not include the BEGIN and END tags.

  If the change of the certificate is successful, the system displays the message Tenant <name of tenant> updated.

- To change the name format of the identity provider, choose the Name field, select the name format from the dropdown list, and save your changes.

  The dropdown list offers two options:

<table>
<thead>
<tr>
<th>Default Type</th>
<th>URL Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;tenant ID&gt;.accounts.ondemand.com</code></td>
<td><code>https://&lt;tenant ID&gt;.accounts.ondemand.com</code></td>
</tr>
</tbody>
</table>

  **Note**

  Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

  **Caution**

  You should change the name of the identity provider on the client (relying party) side every time you change the name format of the identity provider in the administration console. If you have set trusts with more than one client, change the name in every client. For more information about how to edit the name, see the documentation of the respective clients.

  If the change of the name is successful, the system displays the message Tenant <name of tenant> updated.

- To change the authorization or token endpoint, edit the respective fields and save your changes.

  If the change of the name is successful, the system displays the message Tenant <name of tenant> updated.

**Related Information**

- Configuring Tenant Settings [page 129]
- Troubleshooting for Administrators [page 298]
1.5.2.3 Configure a Tenant Logo

You can configure a custom global logo on the forms for logon, registration, upgrade, password update, and account activation for all applications in a tenant.

This logo is displayed in the footer or header of the form that your users access to log on or to register to an application. If you do not specify a company-specific tenant logo, the forms will display the default SAP logo. SAP has configured the following default tenant logo.

To configure a custom tenant logo, proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Under Applications and Resources, choose the Tenant Settings tile.
3. Choose the Logo list item.
4. Upload an image with height 36 pixels.

   i Note
   The image file must have one of the following extensions: .png, .gif, or .jpeg.

   i Note
   If the height of the image is larger than 36 pixels, the user forms show the logo proportionally resized to a height of 36 pixels. Thus the quality will be preserved.

   If the height of the image is lower than 36 pixels, the user forms resize the image. Otherwise the quality will be deteriorated.

5. Save your configuration.

   If the operation is successful, you will receive the following message: Tenant logo updated.
6. To restore the default logo, choose Restore Default.
If this operation is successful, you will receive the following message: Default logo restored.

1.5.2.4 Configure E-Mail Link Validity

As a tenant administrator, you can configure the validity of the link sent to a user in the various application processes.

Context

The tenant administrator can specify how long the link sent to a user in the various application processes will be valid for. The link in the e-mail can be set to expire after between 1 and 23 hours, or 1 and 30 days. SAP Cloud Platform Identity Authentication service has predefined the following validity periods:

Default E-Mail Link Validity Periods

<table>
<thead>
<tr>
<th>Application Process</th>
<th>Default Validity Period</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Registration</td>
<td>21 Days</td>
</tr>
<tr>
<td>On-Behalf Registration</td>
<td>21 Days</td>
</tr>
<tr>
<td>Invitation</td>
<td>28 Days</td>
</tr>
<tr>
<td>Forgot Password</td>
<td>2 Hours</td>
</tr>
<tr>
<td>Locked Password</td>
<td>2 Hours</td>
</tr>
<tr>
<td>Reset Password</td>
<td>2 Hours</td>
</tr>
</tbody>
</table>

To change the validity period of the links, follow the procedure below:

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   i Note
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Under Applications and Resources, choose the Tenant Settings tile.
3. Choose the E-Mail Link Validity list item.
4. Choose an application process and set the validity period of the e-mail link for it.
   a. From the dropdown list on the right, select either Days or Hours.
   b. From the dropdown list on the left, select a number for this.

   **Note**
   You can choose a value between 1 and 23 for Hours, and 1 and 30 for Days.

   You can repeat the step for all processes.

5. Save your changes.

**Results**

If the operation is successful, the system displays the message E-mail link validity updated.

### 1.5.2.5 Configure Session Timeout

As a tenant administrator, you can configure when the session created at the identity provider (IdP) expires.

**Context**

The session timeout feature enables closing of the session at the IdP when the configured period has passed. The configuration determines how long the IdP keeps the session alive.

By default, the timeout session for Identity Authentication is 12 hours.

When the IdP session has expired, and the application session has also expired, or the user tries to access a second application, IdentityAuthentication forces the user to provide his or her credentials.
1. Tries to access protected resource.
2. Sends request to check if the user has rights to access.
3. Opens Log On screen; forces user to provide credentials.
4. Provides credentials.
5. Grants access.
6. User accesses content.

To configure the session timeout period via the administration console for Identity Authentication follow the procedure below:

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   
   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Under *Applications and Resources*, choose the *Tenant Settings* tile.
3. Choose the *Session Timeout* list item.
4. Set the session timeout period.
   
   a. From the dropdown list on the right, select either *Minutes or Hours*.
   
   b. From the dropdown list on the left, select a number for your choice.

   **i Note**
   
   You can choose a value between 5 and 59 for *Minutes*, and 1 and 12 for *Hours*.
   
   The default value is 12 hours.

5. Save your changes.

   If the operation is successful, the system displays the message *Session timeout updated.*
1.5.2.6 Configure Trusted Domains

Service providers that delegate authentication to Identity Authentication can protect their applications when using embedded frames, also called overlays, or when allowing user self-registration.

Context

If you want to use overlays in your applications, you should add the domains of these applications as trusted in the administration console for Identity Authentication. Otherwise the user will receive an error message when trying to access the overlays of these applications.

You also have to add as trusted the domains for those applications that allow self-registration to the users. For more information about the various access configurations in the administration console for Identity Authentication, see Configure User Access to the Application [page 87].

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Tenant Settings tile.
3. Choose the Trusted Domains list item.
4. Press the + Add button.
5. Type the URL of the trusted host in the field.
   
   You can type either the full name of the host or you can use the wild card * function. See the examples:
   
   mycompany.ondemand.com
   
   *.example.com
6. Save your changes.
   
   If the operation is successful the system displays the message Trusted Domains updated.

Related Information

Add Logon Overlays in Customer Applications [page 396]
1.5.2.7  Change a Tenant's Display Name

You can configure the tenant's name from the administration console for SAP Cloud Platform Identity Authentication service.

Context

If you have not specified a specific tenant name, you will see the tenant ID instead.
To configure the tenant's display name or to change it, proceed as follows:

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Under Applications and Resources, choose the Tenant Settings tile.
3. Choose the name of the tenant and change it in the pop-up dialog.
4. Save your changes.
   Once the tenant has been updated, the system displays the message Tenant <name of tenant> updated.

Related Information

Configuring Tenant Settings [page 129]
Troubleshooting for Administrators [page 298]

1.5.2.8  Corporate User Store

If you have an existing on-premise user store, you can configure Identity Authentication to use the corporate user store in addition to its own cloud user store. This integration allows users to authenticate with their
corporate credentials from the corporate user store, without the need to use another set of credentials for their cloud access.

**Overview**

Identity Authentication can connect with the following corporate user stores:

- Microsoft Active Directory
- SAP NetWeaver AS JAVA, with the following variants:
  - SAP NetWeaver AS JAVA - UME
  - Multiple Active Directories connected to SAP NetWeaver AS JAVA - UME
  - SAP NetWeaver AS ABAP connected to SAP NetWeaver AS JAVA - UME

This scenario works with an SAP Cloud Platform application named proxy and provided by an SAP Cloud Platform subaccount named sci. The proxy application on SAP Cloud Platform uses the OAuth authentication mechanism when communicating with Identity Authentication. The connection between SAP Cloud Platform and the corporate user store is carried out with an SAP Cloud Platform Connector.
The Corporate User Store option is configured properly. A user tries to access a trusted application for the first time with the on-premise credentials, Login Name and Password entered correctly. This user is authenticated successfully against the corporate user store. With this initial successful authentication of the user, a partial user record is created in the user store for Identity Authentication. It is created with user details taken from the corporate user store. The cloud user store does not copy the user’s credentials. For more details about what data is copied from the corporate user store, see User Records [page 142]. With subsequent logins, the user is always authenticated against the corporate user store, and the user record is updated.

For the first logon with on-premise credentials, the user enters his or her Login Name and a Password. For subsequent logins the user can use either his or her Login Name, E-Mail, or User ID, and the Password.
The user in the corporate user store must have the `mail` attribute.

The tenant administrator needs to monitor and prevent the coexistence of a cloud and on-premise user with one and the same e-mail address. The tenant administrator has to instruct the users to logon for the first time with their `Login Name`, not with the `E-Mail`.

If a user with a user record in the cloud user store is deleted in the corporate user store, the user cannot authenticate using Identity Authentication. The user record for this user remains in the cloud user store, and the tenant administrator can delete it via the administration console for Identity Authentication. For more information, see `Delete Users` [page 207].

For all users from the corporate user store, a second factor for authentication can be enabled for some applications, or cloud user groups can be assigned. For more details, see `Configure Risk-Based Authentication` [page 82] and `Assign Groups to a User` [page 220].

**Control Access to Applications and Resources**

In the scope of the **Corporate User Store** scenario, you can manage access to applications and their resources based on the groups available in the corporate user store.

The corporate user groups are sent to an application in the SAML 2.0 assertion. `corporate_groups` is the attribute that contains the groups that the user in the corporate user store is assigned to. For more details about how the groups are sent to the application in the SAML 2.0 assertion, see `Configure the User Attributes Sent to the Application` [page 64].

If your application is deployed on the SAP Cloud Platform, the corporate user store groups, relevant for the application, and contained in the `corporate_groups` attribute in the SAML 2.0 assertion, can be mapped to assertion-based groups created in SAP Cloud Platform cockpit. For more information, see the 4. (If Using an Identity Provider) *Define the Group-to-Role Mapping* section in Managing Roles.

You can also restrict access to applications based on membership in a corporate user group by setting different rules via risk-based authentication. For more information, see `Configure Risk-Based Authentication` [page 82].

**1.5.2.8.1 User Records**

When a user has been successfully authenticated for the first time with the credentials from the corporate user store, a record for that user is created in Identity Authentication. That user record is created with details from the corporate user store. In this record, the user is created with a `User Type` employee. This `User Type` cannot be changed.

For more information about the attributes taken from the Active Directory and their mapping to the user store of Identity Authentication, see `Configure SAP Cloud Platform When Connecting to an LDAP User Store` in Configure SAP Cloud Platform [page 143].
1.5.2.8.2 Configure Connection to a Corporate User Store

To configure connection to a corporate user store, you have to make the following configurations in SAP Cloud Platform and in Identity Authentication.

For more details about how to configure these systems, see:
- Configure SAP Cloud Platform [page 143]
- Configure SAP Cloud Platform Identity Authentication Service [page 152]

1.5.2.8.3 Configure SAP Cloud Platform

Context

The configuration of SAP Cloud Platform depends on the type of the user store. You have two options: LDAP user store and SAP NetWeaver AS Java user store.

Configure SAP Cloud Platform When Connecting to an LDAP User Store

Procedure

1. Log on to SAP Cloud Platform cockpit. For more information, see Navigating to a Subaccount.

2. In the SAP Cloud Platform cockpit, choose Services in the navigation area Identity Authentication Add-On Enable in the detailed view of the service.

   This enables the extension service of SAP Cloud Platform Identity Authentication service named proxy and provided by an SAP Cloud Platform subaccount named sci.

   △ Caution

   If you don't see the Identity Authentication Add-On tile in the cockpit, you need to report an incident with a subject "Enable Corporate User Store Feature" on SAP Support Portal Home under the component BC-IAM-IDS. You have to provide information about your SAP Cloud Platform subaccount name and region.

3. In your subaccount on SAP Cloud Platform, register an OAuth client for the subscribed proxy application provided by the sci subaccount.
The procedure is described in the documentation of SAP Cloud Platform in the link below.

**i Note**

Since Identity Authentication will create the subscription to the proxy application, the Prerequisites section in the respective document is not relevant for the current scenario.

For the Authorization Grant field in the SAP Cloud Platform cockpit, choose Client Credentials from the dropdown list.

For more information about how to register an OAuth client, see Register an OAuth Client.

4. Install an SAP Cloud Platform Connector in your corporate network.

   For more information, see Installation.

5. Connect the Cloud Connector with your SAP Cloud Platform account.

   ○ If you haven’t used your Cloud Connector before, see Initial Configuration.
   ○ If you have used your Cloud Connector before, you can start the configuration from Set up Connection Parameters and HTTPS proxy.

6. Connect SAP Cloud Platform with your corporate user store.

   **i Note**

   You have to specify the SAP Cloud Platform settings. The Prerequisites section in the document describing the configuration is already configured for the proxy application, and you should proceed with the configuration steps. For more information, see Configure the User Store.

   The User Name field must be in the \(<service_user_name>@<domain>\) format.

   For the User Path and Group Path fields, specify the LDAP tree that contains the users and groups, respectively. For example, if the tree has the following structure:

   ```
   dc=examplcom,
   dc=com
   
   ou=People
   
   cn=John   cn=Donna
   ```

   The user and group paths should appear as in the table below:

<table>
<thead>
<tr>
<th>User Path</th>
<th>ou=People, dc=examplcom, dc=com</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Path</td>
<td>ou=People, dc=examplcom, dc=com</td>
</tr>
</tbody>
</table>

7. **Optional**: Change the default attributes or include additional attributes.
If you want to change the user attributes taken from Microsoft Active Directory, you can do it as part of the configuration of the SAP Cloud Platform Connector via changing the default user attribute mapping. You can also add the employeeNumber, division, department, and organization attributes that are defined in the SCIM Enterprise User Schema Extension.

SAP Cloud Platform Connector uses the SCIM protocol to transfer the data, so the Active Directory attributes are mapped first to the SCIM attributes. When the data is provisioned, the SCIM attributes are mapped to the user store attributes of Identity Authentication.

a. In your system go to /sapcc-<version>/config_master/com.sap.core.connectivity.protocol.scim/

b. On that level, create a new idstorage.cfg file based on the idstorage_extended_schema.cfg file which is given as an example in the folder.

c. Edit the newly created file. For more details, see the information below:

To change the default user attributes, or to add new user attributes you have to edit the whole file.

⚠️ Caution

This file overwrites the configurations you made in Configure the User Store.

In this section, provide the same information as when you specified the SAP Cloud Platform settings in the previous step.

```json
{"LDAPServers": [  
  {  
  "Host": "<The host name of the LDAP server to be contacted>",  
  "Port": "<The port where the LDAP service is running. If omitted then the default LDAP port will be used - 389 for plain connections and 636 for SSL connections>"  
  }  
  },  
  "UserPath": "<LDAP subtree containing the users. Example "DC=users,DC=organisation,DC=location">",  
  "GroupPath": "<LDAP subtree containing the groups. Example "DC=groups,DC=organisation,DC=location">",  
  "ServiceUser": {  
  "Name": "<The name of the user that will be used to establish communication with the LDAP. In case of Active Directory the user name should contains Domain suffix, e.g. "john@ACME.COM">",  
  "Password": "<Password of this user>"  
  }  
  },
```

If you want to use SSL, we recommend that you configure this section.

```json
"UseSSL": "<Possible values are "true" or "false". If true then the communication to LDAP will go over SSL>",  
"IdentityKeystorePath": "<File system path to the client identity keystore - must be set if the used LDAP server requires client certificate authentication>",  
"IdentityKeystorePassword": "<The password of the client identity keystore>",  
"TrustKeystorePath": "<File system path to the trusted CAs keystore - must be set if UseSSL is true>",  
"TrustKeystorePassword": "<The password of the trusted CAs keystore>",
```
In this section, define the mapping between the Active Directory user attributes and the SCIM user attributes that will be sent via the Cloud Connector to the user store of Identity Authentication, or add the additional attributes employeeNumber, division, department, and organization, defined in the SCIM Enterprise User Schema Extension.
"mappings": [  
  
  },  
  
  },  
  
  },  
  
  },  
  
  },  
  
  },  
  
  },  
  
  },  
  
  ],

SAP Cloud Platform Identity Authentication Service

SAP Cloud Platform Identity Authentication Service

PUBLIC

147
}
],
"MultiValuedAttributes": [
{
"SCIMAttribute": "emails",
"values": [
{
"primary": "true",
"mappings": [
{
"SCIMSubAttribute": "value",
"LDAPAttribute": {
"name": "mail"
}
}
]
}
]
},
{
"SCIMAttribute": "phoneNumbers",
"values": [
{
"type": "work",
"primary": "true",
"mappings": [
{
"SCIMSubAttribute": "value",
"LDAPAttribute": {
"name": "telephoneNumber"
}
}
]
},
{
"type": "fax",
"mappings": [
{
"SCIMSubAttribute": "value",
"LDAPAttribute": {
"name": "facsimileTelephoneNumber"
}
}
]
},
{
"type": "cell",
"mappings": [
{
"SCIMSubAttribute": "value",
"LDAPAttribute": {
"name": "mobile"
}
}
]
}
]
},
{
"SCIMAttribute": "addresses",
"values": [
{
"primary": "true",
"mappings": [
{
"SCIMSubAttribute": "streetAddress",
"LDAPAttribute": {
"name": "streetAddress"

148

PUBLIC

SAP Cloud Platform Identity Authentication Service
SAP Cloud Platform Identity Authentication Service


d. Save your changes.
This file overwrites the configurations you made in Configuring the User Store.

Next Steps

The following table shows the default mapping between the Active Directory user attributes and the SCIM attributes. It also shows the existing mapping between the SCIM attributes and the attributes in the user store of Identity Authentication.

Detailed Attribute Mapping Between Active Directory and SCIM, and between SCIM and the User Store of SAP Cloud Platform Identity Authentication Service

<table>
<thead>
<tr>
<th>Microsoft Active Directory Attributes</th>
<th>SCIM Attributes</th>
<th>SAP Cloud Platform Identity Authentication Service User Store Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>sAMAccountname</td>
<td>userName</td>
<td>loginName</td>
</tr>
<tr>
<td>givenName</td>
<td>givenName</td>
<td>firstName</td>
</tr>
<tr>
<td>sn</td>
<td>familyName</td>
<td>lastName</td>
</tr>
<tr>
<td>personalTitle</td>
<td>honorificPrefix</td>
<td>title</td>
</tr>
<tr>
<td>displayName</td>
<td>displayName</td>
<td>displayName</td>
</tr>
<tr>
<td>locale</td>
<td>locale</td>
<td>language</td>
</tr>
<tr>
<td>Microsoft Active Directory Attributes</td>
<td>SCIM Attributes</td>
<td>SAP Cloud Platform Identity Authentication Service User Store Attribute</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------------</td>
</tr>
<tr>
<td>timezone</td>
<td>timeZone</td>
<td>timeZone</td>
</tr>
<tr>
<td>employeeNumber</td>
<td>employeeNumber</td>
<td>personnelNumber</td>
</tr>
<tr>
<td>division</td>
<td>division</td>
<td>division</td>
</tr>
<tr>
<td>department</td>
<td>department</td>
<td>department</td>
</tr>
<tr>
<td>costCenter</td>
<td>costCenter</td>
<td>costCenter</td>
</tr>
<tr>
<td>company</td>
<td>organization</td>
<td>company</td>
</tr>
<tr>
<td>mail</td>
<td>emails.value</td>
<td>mail</td>
</tr>
<tr>
<td>telephoneNumber</td>
<td>phoneNumbers[work].value</td>
<td>telephone</td>
</tr>
<tr>
<td>facsimileTelephoneNumber</td>
<td>phoneNumbers[fax].value</td>
<td>fax</td>
</tr>
<tr>
<td>mobile</td>
<td>phoneNumbers[cell].value</td>
<td>mobile</td>
</tr>
<tr>
<td>streetAddress</td>
<td>addresses.streetAddress</td>
<td>street</td>
</tr>
<tr>
<td>l</td>
<td>Addresses.locality</td>
<td>city</td>
</tr>
<tr>
<td>st</td>
<td>Addresses.region</td>
<td>state</td>
</tr>
<tr>
<td>postalCode</td>
<td>Addresses.postalCode</td>
<td>zip</td>
</tr>
<tr>
<td>co</td>
<td>Addresses.country</td>
<td>country</td>
</tr>
</tbody>
</table>

**Note**

The attributes `employeeNumber`, `division`, `department`, `costCenter` in the *Microsoft Active Directory Attributes* column are given as examples. They can differ according to the specific LDAP properties containing these attributes.

Configure SAP Cloud Platform Identity Authentication Service [page 152]

### Configure SAP Cloud Platform When Connecting to an SAP NW AS Java User Store

**Prerequisites**

- You have an SAP NetWeaver 7.2 or higher Application Server for the Java system.
- You have installed and deployed federation software component archive (SCA) from SAP Single Sign-On (SSO) 2.0. For more information, see [Downloading and Installing the Federation Software](#).
Procedure

1. Log on to SAP Cloud Platform cockpit. For more information, see Navigating to a Subaccount.

2. In the SAP Cloud Platform cockpit, choose Services in the navigation area > Identity Authentication Add-On > Enable in the detailed view of the service.

   This will enable the extension service of SAP Cloud Platform Identity Authentication service named proxy and provided by an SAP Cloud Platform subaccount named sci.

   **Caution**
   
   If you don’t see the Identity Authentication Add-On tile in the cockpit, you need to report an incident with a subject ”Enable Corporate User Store Feature” on SAP Support Portal Home under the component BC-IAM-IDS. You have to provide information about your SAP Cloud Platform subaccount name and region.

3. In your subaccount on SAP Cloud Platform, register an OAuth client for the subscribed proxy application provided by the sci subaccount.

   The procedure is described in the documentation of SAP Cloud Platform in the link below.

   **Note**
   
   Since Identity Authentication will create the subscription to the proxy application, the Prerequisites section in the respective document is not relevant for the current scenario.

   For the Authorization Grant field in the SAP Cloud Platform cockpit, choose Client Credentials from the dropdown.

   For more information about how to register an OAuth client, see Register an OAuth Client.

4. Install an SAP Cloud Platform Connector in your corporate network.

   For more information, see Installation.

5. Connect the Cloud Connector with your SAP Cloud Platform account.

   ○ If you haven’t used your Cloud Connector before, see Initial Configuration.

   ○ If you have used your Cloud Connector before, you can start the configuration from Set up Connection Parameters and HTTPS proxy.

6. Connect SAP Cloud Platform with your corporate user store.

   a. In the configuration of SAP Cloud Platform Connector, configure the host mapping to the on-premise system. For more information, see Configure Access Control (HTTP). For the Limiting the Accessible Services for HTTP(S) section, be sure that the URL Path is /scim/v1, and Path and all Subpaths radio button is chosen for Access Policy.

   b. Create a destination to the on-premise system. In the SAP Cloud Platform cockpit, choose Services in the navigation area > Identity Authentication Add-On > Configure Identity Authentication Add-On > New Destination.

   **Note**
   
   When configuring the destination to the on-premise system, make sure of the following:

   ○ The Name is SAPCloudIdentityUserStore.
Next Steps

Configure SAP Cloud Platform Identity Authentication Service [page 152]

1.5.2.8.4 Configure SAP Cloud Platform Identity Authentication Service

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Under Applications and Resources, choose the Tenant Settings tile.

3. Choose the Corporate User Store list item.

   i Note
   You will not see this list item if the feature has not been enabled by an Identity Authentication operator.

4. Select your SAP Cloud Platform subaccount’s region, enter your SAP Cloud Platform subaccount technical name, and the OAuth client ID and secret.

   i Note
   The Client ID and Client Secret fields in the administration console for Identity Authentication have to match the ID and Secret registered on SAP Cloud Platform under the OAuth Settings tab for your subaccount.
The **Technical Name** field in the administration console for Identity Authentication has to match your SAP Cloud Platform subaccount **Technical Name**.

The **Data Center** field in the administration console for Identity Authentication has to match your SAP Cloud Platform region.

5. Save your configuration.

   If the operation is successful, you receive the message **Connection settings saved**.

**Results**

When the configuration is complete, the user can log in to the application with the on-premise credentials. The first logon requires **Login Name** and password. After successful authentication, a new user record is created in Identity Authentication with type **employee**.

### 1.5.2.9 Configure Kerberos Authentication

**Overview**

You configure Kerberos authentication for Identity Authentication to allow users to log on without a username and password when they are in the corporate network. Identity Authentication supports Kerberos with Simple and Protected GSS-API Negotiation Mechanism (SPNEGO).

Kerberos authentication with Identity Authentication requires the following systems:

- **Web client**
  The web client requests a protected resource of an application configured to use Identity Authentication as an identity provider. It authenticates against the Key Distribution Center (KDC). For example, users can use the web browser to access cloud applications using Identity Authentication.

- **Key Distribution Center (KDC)**
  It authenticates the user and grants a ticket that is used for the communication between the web client and Identity Authentication.

- **Identity Authentication**
  Identity Authentication accepts the ticket issued by the KDC and checks the authenticating user in its cloud user store.
The communication flow is as follows:

1. A user accesses a cloud application on his or her web browser (web client) in the corporate network, and the web client sends a request to Identity Authentication.
3. The Web client requests a Kerberos ticket from the Microsoft Active Directory (KDC).
4. The Microsoft Active Directory (KDC) responds with the ticket.
5. The Web client sends the ticket to Identity Authentication.
6. Identity Authentication validates the ticket, checks that the user exists in its cloud user store by the user’s logon name, and authenticates the user.

Related Information

Kerberos: The Network Authentication Protocol
1.5.2.9.1 Prerequisites

- You have configured the web browser (web client) to use Kerberos authentication. For more information about this procedure, see the corresponding browser (client) documentation.

  → Tip
  
  This setting is usually found under the Local Intranet tab or the Trusted Sites list in the browser. Search on the Internet or in your browser documentation for information about how Kerberos authentication is enabled.

- You have a tenant for SAP Cloud Platform Identity Authentication service.
- The trust with the service provider of Identity Authentication is configured. For more information, see Integration Scenarios [page 409].
- The users logging on with Kerberos authentication exist in the cloud user store with the required details. Each user has to have a logon name as a user attribute. This is specified under the loginName column in the imported CSV file. For details, see Related Information.

Related Information

Import or Update Users for a Specific Application [page 196]

1.5.2.9.2 Configure Key Distribution Center (KDC)

Context

This procedure is performed by the domain administrator. If you are not a domain administrator, skip to the next section.

Procedure

1. Create a service user in KDC (in Microsoft Active Directory for example).

   → Note
   
   A service user is associated with one tenant only.

2. Generate a keytab file and provide it to the tenant administrator.

   When you create the keytab file, the password you specify for the service user is used to generate a key. A setting on the service user also allows you to configure a key type to be derived and used for the encryption of the Kerberos ticket. You have to provide this keytab file as well as the key type to the tenant administrator so that he or she can configure Identity Authentication.
⚠️ Caution
The realm you specify to generate the keytab file has to be in capital letters.

💡 Example
You can derive the key by using your Java installation. To derive the key, proceed as follows:

1. In the command prompt, run the `ktab -help` command to see the list of available commands.

→ Tip
Go to your Java `bin` folder or set the Java path as an environment variable.

2. Enter `ktab -a <service user>@<realm> -k <path>/<keytab filename>.ktab` with `<realm>` in capital letters to create a new keytab file.
You are also prompted to enter the service user password that is used to derive the key.

3. Register a service principal name (SPN) associated with the service user for the host name used to access Identity Authentication. The SPN has to be unique.

💡 Example
The command line `setspn -A HTTP/<tenantID>.accounts.ondemand.com <service user>` registers an SPN for the `<tenantID>.accounts.ondemand.com` host associated with the service user.

⚠️ Caution
If you have one of the following combination of an operating system and web browser:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browser</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 10</td>
<td>Microsoft Internet Explorer 11</td>
</tr>
<tr>
<td>Microsoft Windows</td>
<td>Google Chrome</td>
</tr>
<tr>
<td>Microsoft Windows</td>
<td>Mozilla Firefox</td>
</tr>
</tbody>
</table>

you must ensure a registration of an SPN for the root host name of Identity Authentication.

The root host name is:

- `ap.accounts.ondemand.com.cloud.sap.akadns.net` - for tenants in Australia
- `accounts.ondemand.com.cloud.sap.akadns.net` - for tenants in EU
- `ru.accounts.ondemand.com.cloud.sap.akadns.net` - for tenants in Russia
- `us-east.accounts.ondemand.com.cloud.sap.akadns.net` - for tenants in USA
Example

The command line `setspn -A HTTP/accounts.ondemand.com.cloud.sap.akadns.net <service user>` registers an SPN for the root host `accounts.ondemand.com.cloud.sap.akadns.net` associated with the service user.

1.5.2.9.3 Configure SAP Cloud Platform Identity Authentication Service

Context

This procedure is performed by the tenant administrator.

Procedure

1. Extract the key from the keytab file provided by the domain administrator.

   Example

   You can extract the key by using your `Java` installation.

   1. In the command prompt, run the `ktab -help` command to see the list of available commands.

      → Tip

      Go to your Java `bin` folder or set the Java path as an environment variable.

   2. Enter `klist -e -f -k -K <path>\<keytab filename>.ktab` to list the derived keys corresponding to the key types.

   3. Copy the key according to the number of the provided key type: 23 corresponds to `RC4`, 17 corresponds to `AES128`, and 18 corresponds to `AES256`.

2. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   Note

   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

3. Under `Applications and Resources`, choose the `Tenant Settings` tile.

4. Choose the `SPNEGO` list item.

5. Enter the following information:

   ○ Realm

      The Kerberos realm (domain) which the SPN and service user reside in.
The realm (domain) has to be in capital letters.

- **Key type**
  The key type has to match the encryption type of the corresponding service user that contains the tenant as a service principal name. Identity Authentication supports the following key types: **RC4**, **AES128**, and **AES256**. For more information about these key types, see RFC 4757 and RFC 3962.

- **Key**
  The key derived with the password of the service user in the KDC.

- **IP white list**
  A comma-separated list of ranges of the web client’s IPs or proxies allowed for the Kerberos authentication. The IP white list has to contain ranges in Classless Inter-Domain Routing (CIDR) notation.

**Note**

By default the field is empty, which means any client IP is allowed.

**Example**

Enter `123.45.67.1/24, 189.101.112.1/16` to allow the web client to use any client IP starting with 123.45.67 or with 189.101.

6. Save your entries.

   If the operation is successful, you receive the message **SPNEGO settings saved**.

**Next Steps**

Enable Kerberos authentication for specific applications. For more information, see **Enable or Disable Kerberos Authentication for an Application** [page 78].

**1.5.2.10 Configure SAP Authentication 365 in Administration Console**

Configure SAP Authentication 365 to enable **Phone Verification via SMS** in the administration console.

**Prerequisites**

- You have an account in SAP Authentication 365.
- You are assigned the Manage Tenant Configuration role. For more information about how to assign administrator roles, see **Edit Administrator Authorizations** [page 241].
**Context**

SAP Authentication 365 service enables multichannel two-factor authentication (2FA), adding another layer of security to customers’ online accounts, beyond their login and password. The service enables you to configure tokens – such as one-time passwords (OTPs), personal identification numbers (PINs), and verification codes – that are tailored to businesses and particular use cases. For more information, see [SAP Authentication 365](#).

For the integration between Identity Authentication and SAP Authentication 365, you must make the following configuration steps in the administration console:

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
   
   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern. 
   
   **Tenant ID** is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the **tenant ID**.

2. Under **Applications and Resources**, choose the **Tenant Settings** tile.
3. Choose the **SAP Authentication 365 Configuration** list item.
4. Enter the required information.
5. Save your entries.

   If the operation is successful, you receive the message **SAP Authentication 365 saved**.

**1.5.2.11 Configure RADUIS Server Settings**

Configure Remote Authentication Dial-In User Service (RADIUS) server settings in the administration console for Identity Authentication.

**Prerequisites**

You have the **host**, **port**, and **secret** parameters, configured for the RADIUS server which will be used to authenticate users with RADIUS two-factor authentication. You can receive the parameters from the RADIUS server administrator.
Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Under *Applications and Resources*, choose the *Tenant Settings* tile.
3. Choose the *RSA SecurID Configuration* list item.
4. Fill in the information in the fields. All fields are required.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host</strong></td>
<td>Host address of the RADIUS server (used for user authentication).</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>The port number used by the RADIUS server for authentication requests.</td>
</tr>
<tr>
<td><strong>Secret</strong></td>
<td>A shared secret is used to encrypt the user password. This shared secret also must be defined in the RADIUS server. Paste the secret defined in the RADIUS server into this field.</td>
</tr>
</tbody>
</table>
   | **User Attribute** | Unique attribute for the user. Configure the supported attribute which the RADIUS server is configured to use for authentication. Possible values are:  
   ○ User ID  
   ○ E-Mail  
   ○ Login Name |
   | **PAP / CHAP**  | Authentication method for the RADIUS server. Possible values are:  
   ○ PAP  
   ○ CHAP  
   The default value is **PAP**. |

5. Save your entries.

   If the operation is successful, you receive the message *Configuration saved*.

   To delete the settings, remove the configuration.

   **Caution**
   Make sure to remove the *RSA SecurID Two-Factor Authentication* rule, when you delete the RADIUS server configuration. If the configuration is missing, the users cannot log on.
Next Steps

Configure an application to require RADUIS PIN code as a second factor apart from the password for user authentication. For more information, Configure Risk-Based Authentication [page 82].

1.5.2.12 Configure Mail Server for Application Processes

Configure mail server for the e-mails sent to the end-users in the different application processes.

Prerequisites

You are assigned the Manage Tenant Configuration role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].

Context

Identity Authentication uses own mail server for the e-mails sent to users for the different application processes. For example, when a user makes a registration for an application, he receives an activation e-mail from notification@sapnetworkmail.com.

For more information, about the e-mails sent for the different application processes, see Configuring E-Mail Templates [page 184].

Identity Authentication provides also the possibility to configure custom mail server for the application processes e-mails.

Remember

Once the tenant administrator configures the mail server, all e-mails will go through this configuration.

To return to the default settings, remove the configuration.

To configure the mail server, follow the procedure below:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

Note

The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
**Tenant ID** is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Under **Applications and Resources**, choose the **Tenant Settings** tile.
3. Choose the **Mail Server Configuration** list item.
4. Enter the required information in all the fields.
5. Save your entries.

If the operation is successful, you receive the message **Configuration saved**.

→ **Tip**

To return to the default settings, remove the configuration.

**Example**

**Testing Mail Server Configuration**

Access the profile page at https://<tenant ID>.accounts.ondemand.com/ from a new browser where you do not have an active session with Identity Authentication. Choose the **Forgot password?** link from the logon page to start the reset password process.

→ **Remember**

Only three reset password e-mails are allowed to be sent for 24 hour. If you have already reached the limit, Identity Authentication will not send you an e-mail. To check the number of reset password e-mails, access **administration console for** > **Users & Authorizations** > **User Management** > **your user** > **Authentication** > **Next to Password Reset** you can see the number of e-mails sent. If necessary, choose **Reset Counter** to be able to send more reset password e-mails.

If the reset password e-mail is sent successfully, and the configuration is correct, the e-mail that you receive should have as a sender the e-mail specified in the configuration.

If the configuration is not correct, no e-mail is sent.

**Related Information**

Configuring E-Mail Templates [page 184]

**1.5.2.13 Configure IdP-Initiated SSO**

**Overview**

In the IdP-initiated single sign-on (SSO), the authentication starts at the identity provider (IdP). The user is first authenticated at the identity provider, and after that he or she is allowed to access the protected resource at the application ((service provider (SP)).
1. The user accesses the identity provider via a link.
2. The identity provider requires credentials.
3. The user provides credentials, and he or she is authenticated.
4. The identity provider sends assertion about the user to the service provider.
5. The service provider validates the assertions and gives access rights to the user.
6. The identity provider redirects the user to the protected resource.

→ Remember

The service provider (SP) metadata that is used to configure the trust must contain the default assertion consumer service (ACS) endpoint that can process unsolicited SAML responses.

↓ Note

When SAP Cloud Platform acts as a service provider, the ACS endpoint should be the URL of the protected application resource. To point to the application protected URL, change the ACS endpoint on the identity provider side. For more information about how to change the ACS endpoint in SAP Cloud Platform Identity Authentication, see Configure Trust [page 55].

The link for IdP-initiated SSO follows the pattern: https://<tenant_ID>.accounts.ondemand.com/saml2/idp/sso?sp=<sp_name>[&RelayState=<sp_specific_value>&index=<index_number>]

↓ Note

The following table lists the URL parameters you can use for IdP-initiated SSO.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sp</td>
<td>Yes</td>
<td>Name of the SAML 2 service provider for which SSO is performed.</td>
</tr>
<tr>
<td>RelayState</td>
<td>No</td>
<td>Relay state forwarded to the service provider with the SAML response.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Mandatory</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>index</td>
<td><img src="#" alt="Note" /></td>
<td>You can choose by the index the correct ACS endpoint for unsolicited SAML response processing. Provide the index parameter when the default ACS endpoint which has been configured via the administration console cannot process unsolicited SAML responses. Otherwise the identity provider uses the default endpoint configured for the trusted service provider. A non-digit value or a value for an index entry that is not configured returns an error message.</td>
</tr>
</tbody>
</table>

**Example**

Richard Wilson, tenant administrator at Company A, would like to set up an IdP-initiated SSO process and has configured the default assertion consumer service (ACS) endpoint correctly at the cloud identity provider. Dona Moore, who is an employee at Company A, tries to access the identity provider, but because she does not have a valid session she is prompted to provide credentials. Once Dona has logged in at the IdP, a session is created for her. She is automatically redirected to her application (the default ACS URL as specified in the service provider (SP) metadata)).

1. User provides credentials; logs on.
2. Identity Authentication sends assertions.
3. Service provider validates assertions; gives access rights.
4. User accesses content.
Enable or Disable IdP-Initiated SSO

Prerequisites

You have specified the default assertion consumer service (ACS) endpoint in the configuration of a trusted service provider (SP) in the administration console for Identity Authentication. For more information, see Configure Trust [page 55].

Context

By default, IdP-Initiated SSO is enabled in Identity Authentication. The tenant administrator can disable the IdP-Initiated SSO process via the administration console for Identity Authentication.

⚠️ Caution

When IdP-Initiated SSO is disabled, users cannot access their profile page.

Use this procedure to disable or enable the IdP-Initiated SSO process.

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note

   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Tenant Settings tile.

3. Use the slider next to IdP-Initiated SSO to disable or enable it.

   If the operation is successful, you receive a confirmation message.
1.5.3 Configuring Password Policies

Passwords for the authentication of users are subject to certain rules. These rules are defined in the password policy. SAP Cloud Platform Identity Authentication service provides you with two predefined password policies, in addition to which you can create and configure a custom one.

You have the following options for a password policy:

- **Standard** (Predefined) Use this option to set special rules for changing, resetting, and locking a password.
  
  **Note**
  
  This is the default setting. It meets the minimum strength requirements.

- **Enterprise** (Predefined) Use this option to set enhanced password management features. It is stronger than the standard policy, but weaker than the custom one.

- **Custom** (Configurable) Use this option to set the strongest password management features for the password policy.

  **Remember**
  
  This option is only possible if you have configured a custom password policy in the administration console for Identity Authentication. For more information, see Configure Custom Password Policy [page 170].

### Password Policy Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Standard</th>
<th>Enterprise</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Content of password (configurable)</strong></td>
<td>● Minimum length of 8 characters;</td>
<td>● Minimum length of 8 characters;</td>
<td>● Minimum length of 8 characters;</td>
</tr>
<tr>
<td></td>
<td>● Maximum length of 255 characters;</td>
<td>● Maximum length of 255 characters;</td>
<td>● Maximum length of 255 characters;</td>
</tr>
<tr>
<td></td>
<td>● Characters from at least three of the following groups:</td>
<td>● Characters from at least three of the following groups:</td>
<td>● Characters from at least three of the following groups:</td>
</tr>
<tr>
<td></td>
<td>○ Lower-case Latin characters (a-z);</td>
<td>○ Lower-case Latin characters (a-z);</td>
<td>○ Lower-case Latin characters (a-z);</td>
</tr>
<tr>
<td></td>
<td>○ Upper-case Latin characters (A-Z);</td>
<td>○ Upper-case Latin characters (A-Z);</td>
<td>○ Upper-case Latin characters (A-Z);</td>
</tr>
<tr>
<td></td>
<td>○ Base 10 digits (0-9);</td>
<td>○ Base 10 digits (0-9);</td>
<td>○ Base 10 digits (0-9);</td>
</tr>
<tr>
<td></td>
<td>○ Non-alphabetic characters (@#$ %...);</td>
<td>○ Non-alphabetic characters (@#$ %...);</td>
<td>○ Non-alphabetic characters (@#$ %...);</td>
</tr>
<tr>
<td><strong>Session time limit</strong></td>
<td>Yes, 12 hours</td>
<td>Yes, 12 hours</td>
<td>Yes, 12 hours</td>
</tr>
</tbody>
</table>

Session time limit indicates when the current session expires.
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Standard</th>
<th>Enterprise</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>“Remember me” option</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Indicates whether the browser can store a cookie with the credentials.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forgot password deactivation period</td>
<td>Yes, 24 hours</td>
<td>Yes, 24 hours</td>
<td>Yes, 24 hours</td>
</tr>
<tr>
<td>Indicates the period during which users can initiate the number of forgot password e-mails specified by the forgot password counter.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forgot password counter</td>
<td>Yes, 3</td>
<td>Yes, 3</td>
<td>Yes, 3</td>
</tr>
<tr>
<td>Indicates how many times a user can initiate forgot password e-mails during the deactivation period. For example, a user can initiate up to 3 forgot password e-mails within 24 hours.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minimum password age</td>
<td>No</td>
<td>Yes, 24 hours</td>
<td>Yes, minimum 1 hour, maximum 48 hours</td>
</tr>
<tr>
<td>Shows the minimum lifetime of a password before it can be changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum failed logon attempts</td>
<td>Yes, 5</td>
<td>Yes, 5</td>
<td>Yes, minimum 1, maximum 5</td>
</tr>
<tr>
<td>Indicates how many logon attempts are allowed before the user password is locked.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password locked period</td>
<td>Yes, 1 hour</td>
<td>Yes, 1 hour</td>
<td>Yes, minimum 1 hour, maximum 24 hours</td>
</tr>
<tr>
<td>Indicates how long a password is locked for.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum password age</td>
<td>No</td>
<td>Yes, 6 months</td>
<td>Yes, minimum 1 month, maximum 6 months</td>
</tr>
<tr>
<td>Shows the maximum lifetime of a password before it has to be changed.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Password history</td>
<td>No</td>
<td>Yes, the last 5 passwords are retained.</td>
<td>Yes, minimum the last 5 passwords, and maximum the last 20 passwords are retained.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Standard</td>
<td>Enterprise</td>
<td>Custom</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------</td>
<td>------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Maximum unused period</td>
<td>No</td>
<td>Yes, 6 months</td>
<td>Yes, minimum 1 month, maximum 6 months</td>
</tr>
</tbody>
</table>

Indicates how long the system retains unused passwords for.

As a tenant administrator, you can do the following:

- **Set a Password Policy for an Application [page 168]**
  As a tenant administrator, you can set a password policy that matches your application logon requirements.

- **Configure Custom Password Policy [page 170]**
  Tenant administrators can create and configure a custom password policy for scenarios where SAP Cloud Platform Identity Authentication service is the authenticating authority.

- **Delete Custom Password Policy [page 172]**
  As a tenant administrator, you can delete the custom password policy that you have created in the administration console for SAP Cloud Platform Identity Authentication service.

### 1.5.3.1 Set a Password Policy for an Application

As a tenant administrator, you can set a password policy that matches your application logon requirements.

**Context**

You can choose from standard, enterprise, and custom password policies. The standard and enterprise password policies are predefined, and you cannot configure them. You can configure only the custom password policy. The strength of the policies grows from standard to custom. For more information about the password policies features, see Configuring Password Policies [page 166].

**Tip**

To see the configuration of the password policies in the tenant, go to the Password Policies tile icon next to the policy you want to view.

To set a password policy for an application, proceed as follows:

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
i Note
The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
   This operation opens a list of the applications.
3. Choose the application that you want to edit.

i Note
Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Authentication and Access tab.
5. Under POLICIES, choose Password Policy.
6. Select the radio button for the password policy.
7. Save your selection.
   Once the application has been updated, the system displays the message Application <name of application> updated.

i Note
When the user tries to log on to the application whose password policy has been updated, he or she is prompted to change the password if the current one does not meet the requirements in the updated password policy.

Task overview: Configuring Password Policies [page 166]

Related Information

Configure Custom Password Policy [page 170]
Delete Custom Password Policy [page 172]
Troubleshooting for Administrators [page 298]
Create a New Application [page 43]
Configure Custom Password Policy [page 170]
1.5.3.2 Configure Custom Password Policy

Tenant administrators can create and configure a custom password policy for scenarios where SAP Cloud Platform Identity Authentication service is the authenticating authority.

Context

Identity Authentication provides you with two predefined password policies, in addition to which you can create and configure a custom one. The custom password policy is by default stronger than the enterprise policy, which in turn is stronger than the standard policy.

→ Remember
You can only create one custom password policy. To change the configuration of the custom password policy or to create new one, delete the existing custom policy first, then create the new one. For more information, see Delete Custom Password Policy [page 172].

To create and configure a new custom password policy, follow the procedure:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   → Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Password Policies tile.
3. Choose the + Add Custom Policy button.

   ! Restriction
   You can only add one custom password policy. If you already have a custom password policy in your tenant, the + Add Custom Policy button is grayed out.

4. Fill in the required information in the fields.

   → Remember
   The fields accept rules that are stronger than the enterprise password policy.
### Configuration Options

<table>
<thead>
<tr>
<th>Configuration Options</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Password Policy Name</strong></td>
<td>The name of the password policy that appears in the administration console.</td>
</tr>
<tr>
<td><strong>Password Length</strong></td>
<td>The length can be between 8 and 255 characters. The default value is 8 characters.</td>
</tr>
<tr>
<td><strong>Password Lifetime</strong></td>
<td>The lifetime can be between 1 month and 6 months. The default value is 6 months.</td>
</tr>
<tr>
<td><strong>Maximum Duration of User Inactivity</strong></td>
<td>The maximum duration of user inactivity can be between 1 and 6 months. The default value is 6 months.</td>
</tr>
<tr>
<td><strong>Number of Last Used Passwords that Cannot Be Reused</strong></td>
<td>The minimum requirement is the last 5 passwords to be retained. The value cannot be more than 20.</td>
</tr>
<tr>
<td><strong>Number of Allowed Failed Logon Attempts</strong></td>
<td>The number of allowed failed logon attempts can be between 1 and 5. The default value is 5.</td>
</tr>
<tr>
<td><strong>Password Locked Period</strong></td>
<td>The period can be between 1 and 24 hours. The default value is 24 hours.</td>
</tr>
</tbody>
</table>

5. Save your changes.

Once the password policy has been created and configured, the system displays the message **Password policy <name of policy> created**.

The new custom password policy appears in the list of the password policies that you can use for the applications.

### Next Steps

To use the custom password policy for your application or applications, you should set it as a password policy for that application or applications. For more information, see Set a Password Policy for an Application [page 168].

**Task overview:** Configuring Password Policies [page 166]

### Related Information

- Set a Password Policy for an Application [page 168]
- Delete Custom Password Policy [page 172]
1.5.3.3 Delete Custom Password Policy

As a tenant administrator, you can delete the custom password policy that you have created in the administration console for SAP Cloud Platform Identity Authentication service.

Prerequisites

- You have created a custom password policy in the administration console for SAP Cloud Platform Identity Authentication service. For more information, see Configure Custom Password Policy [page 170].
- The custom password policy should not be set as a password policy for any of the applications in the tenant. For more information about how to set a standard or enterprise policy for an application, see Set a Password Policy for an Application [page 168].

Context

You can only have one custom password policy for your tenant. To change the configuration of the custom password policy, or to create a new one, delete the existing custom policy first.

To delete the custom password policy, proceed as follows:

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.
   
   i Note
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern. 
   
   **Tenant ID** is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the **tenant ID**.

2. Choose the Password Policies tile.

3. Press the next to the custom password policy.

   △ Caution
   
   You can only delete the password policy if it is not set as a password policy for any applications in the tenant.
Results

Once the password policy has been deleted, the system displays the message Password policy <name of policy> deleted.

Task overview: Configuring Password Policies [page 166]

Related Information

Set a Password Policy for an Application [page 168]
Configure Custom Password Policy [page 170]

1.5.4 Configuring Privacy Policies

Initially, administration console for SAP Cloud Platform Identity Authentication service displays a default privacy policy.

To set a new customized policy, first you must create one. Then you must configure the versions for each language, as you must upload a plain text file for each language version.

Every time you want to update the privacy policy document you have to create a new document and to add its language versions.

You can use the following languages:

- Arabic
- Azerbaijani
- Bulgarian
- Chinese
- Croatian
- Czech
- Dutch
- English
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Portuguese
The application's language is defined in the following order of importance:

- By the **locale** parameter in the URL used for accessing the application.

  **Note**
  
  If the SP is configured to support a specific language, only this language is used by the application.

- By the language of the application's browser

  **Note**
  
  The application takes the browser language only if the SP's language is not selected, and the **locale** parameter is not set in the URL. The default browser setting is *English*.

As a tenant administrator, you can do the following:

1. Create a Privacy Policy Document [page 174]
2. Add Language Versions of a Privacy Policy Document [page 175]
   
   To add a language version of a privacy policy document, you need to upload a plain text file containing the privacy policy text.
3. Define a Privacy Policy Document for an Application [page 176]
4. View a Privacy Policy Document [page 177]
   
   Tenant administrators can view privacy policy documents uploaded in the administration console for SAP Cloud Platform Identity Authentication service.

### 1.5.4.1 Create a Privacy Policy Document

**Context**

Provided you have the authorization, you can create and configure a new privacy policy. After you create a new privacy policy document, you have to add custom language versions of the document. To set the custom language versions, you need to upload text files for the respective languages.
**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   
   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the *Privacy Policy Documents* tile.

   This operation opens a list of the privacy policy documents.

3. Choose the *Add* button on the left-hand panel in order to add a new privacy policy document to the list.

4. Specify a name for the document.

   **i Note**
   
   The name can contain only Latin letters, numbers or the underscore character, or a combination of them.

5. Save your selection

   Once the document has been created, the system displays the message `Privacy policy document <name of document> created`.

**Task overview:** Configuring Privacy Policies [page 173]

**Next task:** Add Language Versions of a Privacy Policy Document [page 175]

### 1.5.4.2 Add Language Versions of a Privacy Policy Document

To add a language version of a privacy policy document, you need to upload a plain text file containing the privacy policy text.

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
**Tenant ID** is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the *Privacy Policy Documents* tile.

   This operation opens a list of the privacy policy documents.

3. To add a language version to a privacy policy document, choose that document from the list on the left.

   ▶ Tip
   
   Type the name of the document in the search field to filter the list items.

4. Choose the *Add* button in the details view.
   
   a. Select the language.
   
   b. Specify the plain text file for the language.

   ▪ Note
   
   Use a file with an extension .txt.

   c. Save your selection

   Once the file has been uploaded, the system displays the message "Privacy policy file uploaded."

Task overview: Configuring Privacy Policies [page 173]

Previous task: Create a Privacy Policy Document [page 174]

Next task: Define a Privacy Policy Document for an Application [page 176]

### 1.5.4.3 Define a Privacy Policy Document for an Application

**Context**

The privacy policy is displayed on the registration form, which form appears when the user chooses the *Register Now* link on the logon page. It is also shown to the user when the registration information has been upgraded. Initially, the application is set to use a default privacy policy on the registration and upgrade forms. To change this configuration, you have to select a custom privacy policy.

If you have the authorization, you can create a custom privacy policy document. This document is used once you have set it for the respective application.
Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The URL has the <code>https://&lt;tenant ID&gt;.accounts.ondemand.com/admin</code> pattern.</td>
</tr>
<tr>
<td><strong>Tenant ID</strong> is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the <strong>tenant ID</strong>.</td>
</tr>
</tbody>
</table>

2. Choose the *Applications* tile. This operation opens a list of the applications.
3. Choose the application that you want to edit.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.</td>
</tr>
<tr>
<td>If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].</td>
</tr>
</tbody>
</table>

4. Choose the *Authentication and Access* tab.
5. Under **POLICIES**, choose **Privacy Policy**.
6. Select the radio button for the Privacy Policy.
7. Save your selection.

**Task overview:** Configuring Privacy Policies [page 173]

**Previous task:** Add Language Versions of a Privacy Policy Document [page 175]

**Next task:** View a Privacy Policy Document [page 177]

1.5.4.4 View a Privacy Policy Document

Tenant administrators can view privacy policy documents uploaded in the administration console for SAP Cloud Platform Identity Authentication service.

**Context**

To view a terms of use document, follow the procedure below:
Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **Note**
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Privacy Policy Documents tile.
   This operation opens a list of the privacy policy documents.

3. To view a language version to a privacy policy document, choose that document from the list on the left.

   **Tip**
   Type the name of the document in the search field to filter the list items.

4. Choose the display icon next to the language version of the document you want to view.
   The file opens in a new tab.
   
   To view another privacy policy document, repeat the procedure.

Task overview: Configuring Privacy Policies [page 173]

Previous task: Define a Privacy Policy Document for an Application [page 176]

1.5.5 Configuring Terms of Use

Initially, administration console for SAP Cloud Platform Identity Authentication service displays default terms of use. To set custom terms of use, you need to create a new document and to add its language versions.

Every time you want to update the terms of use document you have to create a new document and to add its language versions.

For each language version, you have to upload a text file. You can define a terms of use document in the following languages:

- Arabic
- Azerbaijani
- Bulgarian
- Chinese
- Croatian
- Czech
- Dutch
- English
The application’s language is defined in the following order of importance:

- By the `locale` parameter in the URL used for accessing the application.

  **i Note**
  
  If the SP is configured to support a specific language, only this language is used by the application.

- By the language of the application’s browser

  **i Note**
  
  The application takes the browser language only if the SP’s language is not selected, and the `locale` parameter is not set in the URL. The default browser setting is *English*.

As a tenant administrator, you can do the following:

1. Create a New Terms of Use Document [page 180]
2. Add Language Versions of a Terms of Use Document [page 181]
   
   To add a language version of a terms of use document, you must upload a UTF-8 encoded plain text file containing the terms of use statement.
3. Define a Terms of Use Document for an Application [page 182]
4. View a Terms of Use Document [page 183]
   
   Tenant administrators can view terms of use documents uploaded in the administration console for SAP Cloud Platform Identity Authentication service.
1.5.5.1 Create a New Terms of Use Document

Context

Provided you have the authorization, you can create and configure a new terms of use document. After you create the document, you have to add custom language versions of the document. To set the custom language versions, you need to upload text files for the respective languages.

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **Note**  
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.  
   `Tenant ID` is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the `tenant ID`.

2. Choose the Terms of Use Documents tile.  
   This operation opens a list of the terms of use documents.

3. Choose the +Add button on the left-hand panel in order to add a new terms of use document to the list.

4. Specify a name for the document.

   **Note**  
   The name can contain only Latin letters, numbers or the underscore character, or a combination of them.

5. Save your selection

   Once the document has been created, the system displays the message `Terms of use document <name of document> created`.

Task overview: Configuring Terms of Use [page 178]

Next task: Add Language Versions of a Terms of Use Document [page 181]

Related Information

Troubleshooting for Administrators [page 298]
### 1.5.5.2 Add Language Versions of a Terms of Use Document

To add a language version of a terms of use document, you must upload a UTF-8 encoded plain text file containing the terms of use statement.

#### Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   
   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the *Terms of Use Documents* tile.

   This operation opens a list of the terms of use documents.

3. To add a language version to a terms of use document, choose that document from the list on the left.

   **→ Tip**
   
   Type the name of the document in the search field to filter the list items.

4. Choose the *Add* button in the details view.
   
   a. Select the language.
   
   b. Specify the plain text file for the language.

   **i Note**
   
   Use a file with an extension `.txt`.

   c. Save your selection

   Once the file has been uploaded, the system displays the message *Terms of use file uploaded*.

**Task overview:** Configuring Terms of Use [page 178]

**Previous task:** Create a New Terms of Use Document [page 180]

**Next task:** Define a Terms of Use Document for an Application [page 182]
Related Information

Troubleshooting for Administrators [page 298]

1.5.5.3 Define a Terms of Use Document for an Application

Context

The terms of use document is displayed on the registration form, which form appears when the user chooses the Register Now link on the logon page. It is also shown to the user when the registration information has been upgraded. By default, the application is set not to use a terms of use document on the registration and upgrade forms. To change this configuration, you have to update the None setting in the administration console.

If you have the authorization, you can create a custom terms of use document. This document is used once you have set it for the respective application.

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   i Note

   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.

   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Authentication and Access tab.

5. Under POLICIES, choose Terms of Use.

6. Select the radio button for the Terms of Use.

7. Save your selection.
1.5.5.4 View a Terms of Use Document

Tenant administrators can view terms of use documents uploaded in the administration console for SAP Cloud Platform Identity Authentication service.

Context

To view a terms of use document, follow the procedure below:

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   **i Note**
   - The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   - *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the *Terms of Use Documents* tile.
   - This operation opens a list of the terms of use documents.

3. To view a language version to a terms of use document, choose that document from the list on the left.

   **→ Tip**
   - Type the name of the document in the search field to filter the list items.
4. Choose the display icon next to the language version of the document you want to view.
The file opens in a new tab.
To view another terms of use document, repeat the procedure.

Task overview: Configuring Terms of Use [page 178]

Previous task: Define a Terms of Use Document for an Application [page 182]

1.5.6 Configuring E-Mail Templates

Tenant administrators can use the default or a custom e-mail template set for the application processes.

Overview

The e-mail template set is a semantic grouping of different e-mail templates. Each e-mail template from the set is used for the respective application process, such as self-registration, for example. When a user makes a registration for an application, Identity Authentication uses the e-mail template for self-registration from the template set to communicate with that user.

The administration console for Identity Authentication provides the possibility to use a default e-mail template set with English templates only. The default set is named Default.

You can also configure your own templates in a custom template set. There you can customize the texts and branding according to your needs.

You can define a set of e-mail templates with different language versions for the following processes:

- **Self-registration**
  This e-mail template is used when a user registers via the Registration page. The user then receives an e-mail with instructions about how to activate his or her account. The name of the e-mail template used for this process is Self-Registration.

- **On-behalf registration**
  This e-mail template is used when somebody else registers the user on his or her behalf. In this case, the registered user receives an e-mail with instructions about how to activate his or her account. The name of the e-mail template used for this process is On-Behalf Registration.

- **Invitation**
  This e-mail template is used when a user invites another user for registration. In this case, the invitee receives an e-mail with instructions about how to register. The name of the e-mail template used for this process is Invitation.

- **Forgot password**
  This e-mail template is used when a user wants to change his or her password by going through the Forgot Password page. In this case, the user receives an e-mail with instructions about how to change his or her password. The name of the e-mail template used for this process is Forgot Password.

- **Locked password**
This e-mail template is used when a user locks his or her password by exceeding the allowed number of logon attempts. In this case, the user receives an e-mail with instructions about how to log on. The name of the e-mail template used for this process is *Locked Password*.

- **Reset password**
  This e-mail template is used when a user has to reset his or her password. In this case, the user receives an e-mail with instructions about how to reset his or her password. The name of the e-mail template used for this process is *Reset Password*.

To activate a user registration or to reset a password, users choose an activation link in their e-mails. For these cases, you can use placeholders. For more information about which placeholders can be used, see *Edit or Add an E-Mail Template Set* [page 188].

You can also define which languages each e-mail template uses, and you can set custom versions for each language. You can set the following languages:

- Arabic
- Azerbaijani
- Bulgarian
- Chinese
- Croatian
- Czech
- Dutch
- English
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Portuguese
- Romanian
- Russian
- Serbian
- Slovak
- Slovenian
- Spanish
- Swedish
- Ukrainian
- Welsh

The language for the e-mail template sets is set according to the following order of priorities:

1. If the locale is set, the e-mails use the language set there, if there is a template in that language. If there is no template in that language, the e-mails use the English language template.

Setting the locale, sets an Identity Authentication cookie. This cookie is used for all the applications in this session that are configured to use Identity Authentication as identity provider.
The locale can be set in either of the following ways:

- The locale is communicated to Identity Authentication by adding a locale parameter to `SAP_IDS.js`.

  ```html
  ```

- The locale is communicated to Identity Authentication by a direct GET request.

  ```html
  ```

2. If the locale is not set, the e-mails use the language that the user’s browser is set to.
   - If the language is not in the list of supported languages, the e-mails use English instead.
   - If the language is in the list of supported languages, the e-mails use this language.

If you want to use a custom e-mail template you should create one if it does not exist. Add or edit the e-mail template set, if necessary, and then define that e-mail template set for the application. Optionally, you can view the uploaded e-mail templates.

1. **Create a New E-Mail Template Set** [page 186]
   Tenant administrators can create a new set of e-mail templates so that each template in the set can have a custom language version.

2. **Edit or Add an E-Mail Template Set** [page 188]
   Tenant administrators can configure language versions of each template in the template set. They can also set a custom template for each language, and change the name of each template set.

3. **Define an E-Mail Template Set for an Application** [page 192]
   Tenant administrators can define the e-mail template set that the application uses.

4. **View E-Mail Template Document** [page 194]
   Tenant administrators can view language e-mail templates in the template set uploaded in the administration console for SAP Cloud Platform Identity Authentication service.

### 1.5.6.1 Create a New E-Mail Template Set

Tenant administrators can create a new set of e-mail templates so that each template in the set can have a custom language version.

**Prerequisites**

You are assigned the Manage Tenant Configuration role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
Context

To create an e-mail template, follow the procedure below:

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern. Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the **E-Mail Template Sets** tile.

   This operation opens a list of the template sets.

3. Press the **+Add** button on the left-hand panel to add a new template set to the list.

4. Specify a name for the set.

5. Save your selection.

   Once template has been created, the system displays the message **Template set <name of set> created**.

Task overview: Configuring E-Mail Templates [page 184]

Next task: Edit or Add an E-Mail Template Set [page 188]

Related Information

Troubleshooting for Administrators [page 298]
1.5.6.2 Edit or Add an E-Mail Template Set

Tenant administrators can configure language versions of each template in the template set. They can also set a custom template for each language, and change the name of each template set.

Prerequisites

- You are assigned the Manage Tenant Configuration role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
- You have prepared the plain text and HTML template files that will be added in the e-mail template set. For that purpose, you need to open the template set for the respective application process from the links in the table below. After that, edit the texts according to your needs, and save a copy of your versions of the documents.
  If you want to use a custom template set in another language, first you need to open the template set for the respective application process from the links in the table below. After that edit the texts in the respective language, and again save a copy of your versions of the documents.

⚠ Caution

You should use only the placeholders used in the template documents. If you use other placeholders, even if they are in comments, e-mails for the respective process will not be sent.

When you edit texts in languages written in Right-To-Left (RTL) direction check that the placeholders are situated in the right place.

You can define an e-mail template set in the following languages:
- Arabic
- Azerbaijani
- Bulgarian
- Chinese
- Croatian
- Czech
- Dutch
- English
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Polish
- Portuguese
- Romanian
→ Remember

If you do not specify a version for a custom template of a specific process, users will receive the e-mail from the default template set for this process. If you do not set an e-mail template for the self-registration process for example, users will receive the default activation e-mail when they complete the registration.

If you do not specify a language version for a custom template of a specific process, users will receive the e-mail from the default template set for this process.

### E-Mail Templates

<table>
<thead>
<tr>
<th>Application Process Template</th>
<th>Usage</th>
<th>Template Set Links</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-Registration</td>
<td>This e-mail template is used after a user fills in the registration form. It should contain activation information.</td>
<td>○ HTML document&lt;br&gt;○ TXT document</td>
</tr>
<tr>
<td>On-Behalf Registration</td>
<td>This e-mail template is used after somebody else registers on-behalf of a user. It should contain registration information.</td>
<td>○ HTML document&lt;br&gt;○ TXT document</td>
</tr>
<tr>
<td>Invitation</td>
<td>This e-mail template is used when a user is invited to register. It should contain registration information.</td>
<td>○ HTML document&lt;br&gt;○ TXT document</td>
</tr>
<tr>
<td>Forgot Password</td>
<td>This e-mail template is used when a user creates a new password. It should contain password update information.</td>
<td>○ HTML document&lt;br&gt;○ TXT document</td>
</tr>
<tr>
<td>Locked-Password</td>
<td>This e-mail template is used after a user locks his or her password. It should contain information on unlocking the password.</td>
<td>○ HTML document&lt;br&gt;○ TXT document</td>
</tr>
<tr>
<td>Reset Password</td>
<td>This e-mail template is used when a user’s password has expired. It should contain password reset instructions.</td>
<td>○ HTML document&lt;br&gt;○ TXT document</td>
</tr>
</tbody>
</table>
Context

To edit or add an e-mail template, follow the procedure below:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the E-Mail Template Sets tile.
   This operation opens a list of the template sets.

3. Choose the list item of the template set you want to edit.

4. Optional: To change the name of the template set, choose it.

5. Select the tab signifying the process, which you want to add or change the template for.

6. Add another language version by choosing the +Add button or edit an existing language version by selecting the respective list item.
   a. Choose language from the dropdown.

   i Note
   The dropdown is grayed out when you are editing an existing language version.

   b. Specify the subject.
   This is the subject of the e-mail that the user receives for the respective process. You are allowed to include placeholders in the subject’s text.

   i Note
   The subject must contain at least one non-space character.

   c. Upload the plain text template file that you have prepared.
   The text file can contain placeholders and HTML tags. The following placeholders can be used: $user.sap_mailing_logo$, $user.company_logo$, $user.firstName$, $user.lastName$, $user.uid$, $
Example

Dear ${user.firstName} ${user.lastName},

An account has been created for you. To activate your account for ${user.sp_name}, click the link below. You will be taken to a page where you will also set a password for your account.

<a href="${user.activate_account_link}">${user.activate_account_link}</a>

If the link above is not displayed or does not work, copy and paste the link below to your browser’s address bar.

<a id="activation-link" href="${user.activate_account_link}">${user.activate_account_link}</a>

Best regards,

Your Project Manager

d. Upload the HTML template file that you have prepared.

The content of the HTML file must comply with the HTML markup requirements, and the file can contain placeholders.

Example

```html
<html>
<head>
<title>Activation Mail</title>
<meta ... />
</head>
<body ... >

<p>...>Dear ${user.firstName} ${user.lastName},</p>

<h1>...>An account has been created for you. To activate your account for ${user.sp_name}, click the link below. You will be taken to a page where you will also set a password for your account.</h1>

<a href="${user.activate_account_link}"...>Click here to activate your account</a>

<p>...>If the link above is not displayed or does not work, copy and paste the link below to the address bar of your browser.</p>

<a id="activation-link" href="${user.activate_account_link}"...>${user.activate_account_link}</a>

...>

<p>Best regards, <p/>

<p>Your Project Manager</p>

...>

</body>
</html>
```

7. Save your selection.

Once the e-mail template has been updated, the system displays the message E-mail template <name of template> updated.
Results

When you edit a previous version of a template in the template set, the changes are applied immediately. The e-mail that is sent contains the latest changes.

When you create a new template set, you must assign the new template set to the application. If you do not assign it, the application will use the currently assigned template. See Next Steps.

Task overview: Configuring E-Mail Templates [page 184]

Previous task: Create a New E-Mail Template Set [page 186]

Next task: Define an E-Mail Template Set for an Application [page 192]

Related Information

Troubleshooting for Administrators [page 298]

1.5.6.3 Define an E-Mail Template Set for an Application

Tenant administrators can define the e-mail template set that the application uses.

Context

Initially, the application uses a default template set with an English language version for all the templates in the set. This template set is named Default. If you want to use another e-mail template set, assign it to the respective application.

i Note

Both the HTML and TXT formats are included in the e-mails sent to a user. What the user sees, depends on the settings of his or her e-mail client.

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
i Note

The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

*Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the *Applications* tile.
   This operation opens a list of the applications.

3. Choose the application that you want to edit.

i Note

Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.

If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the *Branding and Layout* tab.
5. Under *E-MAIL CONFIGURATIONS*, choose *E-Mail Template Set*.
6. Select the radio button of the e-mail template set the application will use.
7. Save your selection.

   Once the application has been updated, the system displays the message Application <name of application> updated.

**Next Steps**

(Optional) Configure custom mail server. To use own mail server for the e-mails sent for the different application processes, you should configure your mail server in the administration console for Identity Authentication.

For more information, see Configure Mail Server for Application Processes [page 161].

**Task overview:** Configuring E-Mail Templates [page 184]

**Previous task:** Edit or Add an E-Mail Template Set [page 188]

**Next task:** View E-Mail Template Document [page 194]

**Related Information**

Troubleshooting for Administrators [page 298]
Create a New Application [page 43]
1.5.6.4 View E-Mail Template Document

Tenant administrators can view language e-mail templates in the template set uploaded in the administration console for SAP Cloud Platform Identity Authentication service.

Prerequisites

- You are assigned the Manage Tenant Configuration role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
- You have added the plain text and HTML template files in the e-mail template set. For more information, see Edit or Add an E-Mail Template Set [page 188].

**Note**
Both the TXT and HTML formats are included in the e-mails sent to a user. What the user sees, depends on the settings of his or her e-mail client.

Context

You can view both the TXT and HTML formats of the e-mails sent to a user.
To view an e-mail template, follow the procedure below:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **Note**
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   **Tenant ID** is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the E-Mail Template Sets tile.
   This operation opens a list of the template sets.
3. Choose the list item of the template set you want to view.
4. Select the tab signifying the process, whose template you want to view.
5. View the file:
   ○ To view the plain text file, choose the plain text file icon next to the respective language version.
To view the HTML file, choose the HTML file icon next to the respective language version. The file opens in a new tab.

To view another template, repeat the procedure.

Task overview: Configuring E-Mail Templates [page 184]

Previous task: Define an E-Mail Template Set for an Application [page 192]

1.5.7 User Management

Tenant administrators can manage user accounts via the administration console of SAP Cloud Platform Identity Authentication service, and via APIs.

The user management enables you to create, modify, and delete users and their attributes, and manage the user accounts in the user store of Identity Authentication.

i Note
For more information about the users that are authenticated with their corporate credentials from the corporate user store, see Corporate User Store [page 139].

→ Remember
To perform user management operations, you must be assigned an administrator role or roles that include the relevant authorizations for the operation. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].

With user management, you can perform the following activities:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Description</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create user</td>
<td>Create users via the Add User option in the administration console</td>
<td>Create a New User [page 202]</td>
</tr>
<tr>
<td></td>
<td>Create users via a CSV file import in the administration console</td>
<td>Import or Update Users for a Specific Application [page 196]</td>
</tr>
<tr>
<td></td>
<td>Create users programmatically via API</td>
<td>Create User Resource [page 348]</td>
</tr>
<tr>
<td>Search users</td>
<td>Search users in the administration console</td>
<td>Search Users [page 203]</td>
</tr>
<tr>
<td></td>
<td>Search users via API</td>
<td>Users Search [page 337]</td>
</tr>
</tbody>
</table>
### Activity | Description | Procedure
--- | --- | ---
List and edit user details | List a specific user and edit the information about that user via the administration console | List and Edit User Details [page 205]

| List and update user details via API | • User Resource [page 343]  
• Update User Resource [page 358] | Import or Update Users for a Specific Application [page 196]
Update user details via a CSV import | Manage user password via the administration console | • Unlock User Password [page 211]  
• Send Reset Password E-Mail [page 213]  
• Reset Counter for E-Mail Sending [page 214]  
• Set Initial Password [page 215]

Delete users | Delete users via the administration console | Delete Users [page 207]

| Delete users programmatically via API | Assign and unassign groups via the administration console | • Assign Groups to a User [page 220]  
• Unassign Users from Groups [page 221]

### 1.5.7.1 Import or Update Users for a Specific Application

As a tenant administrator, you can import new users or update existing ones for a specific application with a CSV file. You can also send activation e-mails to the users that have not received activation e-mails for that application so far.

#### Prerequisites

- You are assigned the Manage Users role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
- You have uploaded the service provider’s metadata or entered the information manually. For more information see, Configure Trust [page 55].

#### i Note

You need the metadata to configure the trust between the service provider and Identity Authentication, which is in the role of identity provider.
Context

By importing new users with a CSV file, you create user profiles without passwords in Identity Authentication. As a result, the users receive e-mails with instructions how to activate their accounts. After the users set their passwords, they can log on to the application for which they were imported. Based on the user access configuration of the application, the users can log on to other applications connected with the tenant in Identity Authentication.

In addition to the new user import, you can specify existing users in the imported CSV file. You thus define the users to be updated in Identity Authentication.

By specifying existing users in the imported CSV file you can also restrict the access to a specific application via the Private options. For more information, see Configure User Access to the Application [page 87].

i Note

The user import does not assign any special rights or roles to the created or updated users for the specific application.

The CSV file can contain only columns with the following attributes.

- status
- loginName
- mail
- firstName
- lastName
- language
- validTo
- validFrom
- spCustomAttribute1
- spCustomAttribute2
- spCustomAttribute3
- spCustomAttribute4
- spCustomAttribute5
- groups

Remember

If you include columns with other attributes, their values in the table are ignored.

The status, mail, and lastName columns are mandatory, and they must always have values.

The loginName, mail, firstName, and lastName columns must be with a string value of up to 64 characters.

The language column must be with a string value specified by a two-letter code defined in ISO 639-1. If you have defined an e-mail template set for the language that is set in the language column, the user receives the activation e-mail in that language.

The validFrom and validTo columns must be with a string value in the Zulu format yyyyMMddHHmmss'Z'.
The information in the `validFrom` and `validTo` columns can be processed by the service provider to limit user access. It would not affect the authentication of the user, though.

The names in the `mail` and `loginName` columns must be unique.

The `status` column defines whether the user is still active in the system and is able to work with any tenant applications. When a user is deleted, it is rendered inactive. The valid values here are `active` or `inactive`.

The groups in the `groups` column must be existing. You cannot add a user to a user group that is not existing. For more details how to list or create user groups, see Related Information.

⚠️ Caution

You cannot change the e-mail of an existing user.

**Examples**

**Example**

A tenant administrator decides to import three new users (Michael, Julie, Donna) and to update two others (John and Denise) that will use the company’s applications. Michael is a member of three groups, namely `Employees`, `Managers`, and `HR`. John and Denise were inactive users that now use tenant’s applications. The administrator would also like to update another user (Richard) who currently does not work for the company. To do this, the administrator uploads a CSV file with the following information:

<table>
<thead>
<tr>
<th>status</th>
<th>loginName</th>
<th>mail</th>
<th>firstName</th>
<th>lastName</th>
<th>language</th>
<th>validFrom</th>
<th>validTo</th>
<th>spCustomAttribute1</th>
<th>groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>EID000001</td>
<td><a href="mailto:michael.adams@example.com">michael.adams@example.com</a></td>
<td>Michael</td>
<td>Adams</td>
<td>en</td>
<td>20110901120000Z</td>
<td>20150901120000Z</td>
<td>Industry</td>
<td>Managers, Employees, HR</td>
</tr>
<tr>
<td>active</td>
<td>EID000002</td>
<td><a href="mailto:julie.armstrong@example.com">julie.armstrong@example.com</a></td>
<td>Julie</td>
<td>Armstrong</td>
<td>en</td>
<td>20110901120000Z</td>
<td>20150901120000Z</td>
<td>Department</td>
<td>Employees</td>
</tr>
<tr>
<td>active</td>
<td>EID000003</td>
<td><a href="mailto:donna.moore@example.com">donna.moore@example.com</a></td>
<td>Donna</td>
<td>Moore</td>
<td>de</td>
<td>20110901120000Z</td>
<td>20160901120000Z</td>
<td>Shift</td>
<td>HR</td>
</tr>
<tr>
<td>status</td>
<td>EID000 04</td>
<td>loginName</td>
<td>mail</td>
<td>firstName</td>
<td>lastName</td>
<td>language</td>
<td>validFrom</td>
<td>validTo</td>
<td>spCustomAttribute</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
<td>--------------------</td>
<td>------------------</td>
<td>-----------</td>
<td>-----------</td>
<td>----------</td>
<td>------------</td>
<td>-----------</td>
<td>-------------------</td>
</tr>
<tr>
<td>active</td>
<td><a href="mailto:john.miller@example.com">john.miller@example.com</a></td>
<td>John</td>
<td>Miller</td>
<td>en</td>
<td></td>
<td>201109011200 00Z</td>
<td>201809011200 00Z</td>
<td>Unit</td>
<td>IT</td>
</tr>
<tr>
<td>active</td>
<td>EID000 05</td>
<td><a href="mailto:denise.smith@example.com">denise.smith@example.com</a></td>
<td>Denise</td>
<td>Smith</td>
<td>en</td>
<td>201109011200 00Z</td>
<td>201409011200 00Z</td>
<td>Administrators</td>
<td></td>
</tr>
<tr>
<td>inactive</td>
<td>EID000 06</td>
<td><a href="mailto:richard.wilson@example.com">richard.wilson@example.com</a></td>
<td>Richard</td>
<td>Wilson</td>
<td>en</td>
<td>201109011200 00Z</td>
<td>201609011200 00Z</td>
<td>All</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

When there are more than one user groups that have to be added for a single user, the groups are received in the SAML 2.0 assertion under the following format:

```
<Attribute Name="groups">
</Attribute>
```

The users that have not received activation e-mails will receive such e-mails, and then can activate their accounts and log on.

**Example**

A sales company has employed two new people (Michael Adams and Julie Armstrong) in the HR department. The tenant administrator has to import these two new employees that will use the company’s applications. Michael and Julie are members of the groups Employees and HR. To do this, the administrator uploads a CSV file with the following information:
Six months later, Julie is promoted as HR Manager, while Michael moves to the Sales department. The tenant administrator has to update the profiles of Michael and Julie to represent the changes. Julie remains in the current groups and has to be included in the Managers group. Michael has to be removed from the HR group, and to be included in the Sales group. To do this, the administrator uploads a CSV file with the following information:

<table>
<thead>
<tr>
<th>status</th>
<th>mail</th>
<th>firstName</th>
<th>lastName</th>
<th>groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td><a href="mailto:michael.adams@example.com">michael.adams@example.com</a></td>
<td>Michael</td>
<td>Adams</td>
<td>Employees, HR</td>
</tr>
<tr>
<td>active</td>
<td><a href="mailto:julie.armstrong@example.com">julie.armstrong@example.com</a></td>
<td>Julie</td>
<td>Armstrong</td>
<td>Employees, HR</td>
</tr>
</tbody>
</table>

Remember

When tenant administrators must update a user via a CSV file, they must include the new information, and repeat the information that remains unchanged.

If you, as a tenant administrator, include only the new information, the information that is not repeated will be deleted.

In this example, the administrator imports Michael with the Employees group, and Julie with the Employees and HR groups in the new table.

To import users for an application into Identity Authentication, and to send activation e-mails, proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note

   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Import Users tile.

   This operation opens the Import Users page.

3. Choose the application that you want to edit.
4. Choose the **Browse...** button and specify the location of the CSV file.

**i Note**

Use a file smaller than 100 KB and with an extension .csv. If your file is 100 KB or larger, you have to import the user information in iterations with smaller size files.

5. Choose the **Import** button.

If the operation is successful, the system displays the message **Users imported or updated**.

6. Choose one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do nothing</td>
<td>The users are imported or updated for the selected application, but they will not receive activation e-mails. The activation e-mails will be sent when you choose <strong>Send E-Mails</strong>.</td>
</tr>
<tr>
<td>Repeat steps 1 to 5</td>
<td>The users are imported or updated for the selected application, but they will not receive activation e-mails. The activation e-mails will be sent when you choose <strong>Send E-Mails</strong>.</td>
</tr>
</tbody>
</table>

**Choose**

This will send activation e-mails to all users that are imported for the selected application, but have not received activation e-mails so far.

**i Note**

The **Send** button is inactive if **Home URL** or SAML 2.0 configuration of the application is missing. You can only import users, but you cannot send activation emails.

You need the **Home URL** configured for the specific application to be able to send the activation e-mails to the imported new users. For more information, see **Configure an Application’s Home URL** [page 50].

To access the application, the users have to activate their accounts by following the link they receive in the e-mails.

---

**Related Information**

- Troubleshooting for Administrators [page 298]
- Configure an Application’s Home URL [page 50]
- Configure User Access to the Application [page 87]
- List User Groups [page 218]
- Create a New User Group [page 217]
- Edit Administrator Authorizations [page 241]
- Export Existing Users of a Tenant of SAP Cloud Platform Identity Authentication Service [page 281]
1.5.7.2 Create a New User

As a tenant administrator, you can create a new user in the administration console for SAP Cloud Platform Identity Authentication service.

Prerequisites

You are assigned the Manage Users role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].

Context

The tenant administrator creates the new user with a minimum set of attributes and can set an initial password.

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   - **Note**: The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern. *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the User Management tile.

3. Press Add User.

4. Fill in the required fields in the dialog box.

   - **Note**: By default the User Type field is Employee. To change the default setting, choose user type from the drop-down list. The available user types are: Customer, Employee, Partner, and Public.

5. Select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send activation e-mail</td>
<td>The user receives an e-mail with instructions how to activate the user account.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Set password</td>
<td>The tenant administrator sets the password for the user.</td>
</tr>
<tr>
<td>i Note</td>
<td>The user is prompted to reset the password during the first authentication.</td>
</tr>
</tbody>
</table>

6. Save your entries.

### 1.5.7.3 Search Users

As a tenant administrator, you can search for a specific user or users in the administration console for SAP Cloud Platform Identity Authentication service.

#### Prerequisites

You are assigned the Manage Users role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].

#### Context

You can list all users in the tenant for Identity Authentication or filter your search by User ID, First Name, Last Name, E-Mail, or Login Name.

#### Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
   
   i Note
   
   The URL has the \https://<tenant ID>.accounts.ondemand.com/admin\ pattern.
   
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the User Management tile.
   
   The system displays the first 20 users in the tenant sorted by their user ID number.

3. Optional: You can choose one of the following:
Search Options

List All Users
Press More

This will expand the list by 20 users.

i Note
This option is available only if the users in the tenant are more than 20.

Simple Search

○ (default mode) Type your search criteria string in the search field and press the key

○ (when in Advanced Search mode) Press Simple Search; type your search criteria string in the search field, and press the Enter key

Once the search is completed, the system will list the users whose User ID, E-Mail, or Login Name match your search criteria string. In this case the system does not include the First Name and Last Name fields in the search.

If you are not satisfied with the search result, edit your search criteria and repeat the step again.

i Note
The search is case insensitive. The system searches for entries that begin with the typed string.

If you place asterix (*) in the beginning or in the middle of your search string the system will treat it as a regular character and will include it in the search. For example, if you type *on in the search field, the system will look for users whose first three letters in any of the three fields are *on. If you type on or on* in the search field, the system will look for users whose first two letters in any of the three fields are on.
Advanced Search
Press Advanced Search and type your search criteria strings in at least one of the search fields. The system checks the search fields simultaneously. Once the search is completed, it will list the users that match the search criteria from all the fields.

**i Note**
The search is case insensitive.
The system searches for entries that begin with the typed string.
If you place asterix (*) in the beginning or in the middle of your search string the system will treat it as a regular character and will include it in the search. For example, if you type *on in the First Name field, the system will look for users whose first three letters of the first name are *on. If you type on or on* in the First Name field, the system will look for users whose first two letters of the first name are on.

**Related Information**
Edit Administrator Authorizations [page 241]

### 1.5.7.4 List and Edit User Details

As a tenant administrator, you can view detailed information about the users in the administration console for SAP Cloud Platform Identity Authentication service. Optionally you can edit this information.

**Procedure**

1. Find the user whose details you want to view or edit.
   For more information about how to find a user in Identity Authentication, see Search Users [page 203].
2. Click the user to view his or her details.
   This operation opens the User Details view.
3. Optional: Choose the User Details tab.
   a. Expand the Personal Information, Employee Information, and Company Information sections if collapsed in the User Details tab.
   b. Press the icon next to the Personal Information, Employee Information, or Company Information sections.

   **i Note**
   To exit edit mode, press the icon.

   a. Edit the information in the relevant fields and save your changes.

   **i Note**
   Last Name, Display Name, and E-Mail fields are mandatory.

   E-Mail and Login Name can be used as unique identifiers. Be sure to enter unique values if you edit these two fields.

   If the check box below the E-Mail is selected, the e-mail of the user is verified. The tenant administrator can select it manually, to mark the e-mail as verified. For more information about how to require e-mail verification of the user, see, Enable E-Mail Verification [page 89].

   User ID, and Manager Display Name fields cannot be edited. They are filled automatically by the system.

   If you choose Customer, Employee, or Partner for User Type, the Company Relationship field is overwritten, and takes the same value as in the User Type field. If you choose Public for User Type, the Company Relationship can be filled with any of the options from the drop down list.

   If the operation is successful, the system displays the message User <user ID> updated.

4. Optional: Choose the Applications tab, to view details specific for the applications that the user has logged on, and the applications that the user was imported to via a CSV file import.

5. Optional: Choose the Legal tab to view audit information about the user, such as the policies accepted by him or her, the last log on, and password related information.
i Note

The tenant administrators can view a history of the signed Terms of Use and Privacy Policy documents of the users in the administration console for Identity Authentication. The information is in the format `<document name><document version><time stamp>.

The information about when the user has accepted a particular document is available for documents accepted after May 16, 2018.

6. Optional: Choose the Authentication tab to manage the two-factor authentication for the user. You have the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Additional Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Details</td>
<td>○ Unlock user password. For more information, see Unlock User Password [page 211].</td>
</tr>
<tr>
<td></td>
<td>○ Send reset password e-mail. For more information, see Send Reset Password E-Mail [page 213].</td>
</tr>
<tr>
<td></td>
<td>○ Reset counter for e-mail sending. For more information, see Reset Counter for E-Mail Sending [page 214].</td>
</tr>
<tr>
<td></td>
<td>○ Set initial password to the user. For more information, see Set Initial Password [page 215].</td>
</tr>
<tr>
<td>Two-Factor Authentication</td>
<td>If the user has enabled two factor authentication, you can do the following:</td>
</tr>
<tr>
<td></td>
<td>○ Deactivate the user devices. For more information, see Deactivate User Devices for TOTP Two-Factor Authentication [page 210].</td>
</tr>
<tr>
<td></td>
<td>○ Unlock User TOTP Passcode [page 210].</td>
</tr>
</tbody>
</table>

7. Optional: Choose the User Groups tab to manage the group assignments of the user.

You can see the user groups assigned to the user. You have two options:

○ Assign groups. For more information, see Assign Groups to a User [page 220].
○ Unassign one or more groups that are assigned to the user Unassign Users from Groups [page 221].

1.5.7.5 Delete Users

As a tenant administrator, you can delete users in the administration console for SAP Cloud Platform Identity Authentication service.

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

i Note

The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
2. Choose the User Management tile.
   The system displays the first 20 users in the tenant sorted by their user ID number.
3. Find the user that you want to delete.
   For more information about how to find a user in SAP Cloud Platform Identity Authentication service, see Search Users [page 203].
4. Select the checkbox next to the user or users that you want to delete.
   You are not allowed to delete your own user profile.
5. Press Delete Users.
6. Confirm the operation.

1.5.7.6 Deactivate Users

As a tenant administrator, you can deactivate users in the administration console for SAP Cloud Platform Identity Authentication service

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the User Management tile.
   The system displays the first 20 users in the tenant sorted by their user ID number.
3. Find the user that you want to deactivate.
   For more information about how to deactivate a user in SAP Cloud Platform Identity Authentication service, see Search Users [page 203].
4. Select the user that you want to deactivate.
   This operation opens the User Details view.
5. **Optional:** Choose the *User Details* tab.
   a. Expand the *Personal Information*

   b. Press the icon next to the *Personal Information* section.

   c. Select *Inactive* from the dropdown next to the *Status* field.

6. Save your changes.

   If the operation is successful, the system displays the message *User <user ID> updated.*

**Results**

When a user with status *Inactive* tries to log on to an application the following message appears: *Sorry, we could not authenticate you. Try again.*

---

**Note**

To active a user again, set the *Status* to *Active.*
1.5.7.7 Deactivate User Devices for TOTP Two-Factor Authentication

This document shows you how to deactivate the mobile devices used by a user to generate passcodes for access to applications requiring time-based one-time (TOTP) as two-factor authentication. You deactivate the user mobile devices from the administration console for SAP Cloud Platform Identity Authentication service.

Context

You deactivate all user’s mobile devices that generate passcodes if a single device has been lost or stolen. You cannot deactivate a single device.

i Note

If you deactivate the mobile devices, the user will no longer be able to log on to applications that require passcodes. To be able to access them again the user has to activate a new mobile device on the user profile page. For more information, see the Related Information.

To deactivate the mobile devices that generate passcodes, proceed as follows:

Procedure

1. Find the user whose device you want to deactivate.
   For more information about how to find a user in Identity Authentication, see Search Users [page 203].
2. Select the user whose device you want to deactivate.
4. Use the slider next to Status to deactivate two-factor authentication.

1.5.7.8 Unlock User TOTP Passcode

You can unlock a user passcode when the user must log on to the application before the automatic unlock time of 60 minutes has passed.

Context

The user locks his or her passcode after submitting five incorrect passcodes when trying to log on to an application that requires time-based one-time (TOTP) two-factor authentication. The passcode is unlocked automatically after 60 minutes.
When the user locks his or her TOTP passcode, he or she will not be able to log on only to applications that require TOTP passcodes. The applications that do not require two-factor authentication will be accessible only with the user password.

To unlock the user TOTP passcode manually, proceed as follows:

**Procedure**

1. Find the user whose TOTP passcode you want to unlock.
   
   For more information about how to find a user in SAP Cloud Platform Identity Authentication service, see [Search Users](#) [page 203].
2. Select the user that you want to unlock.

   **Note**
   
   You can only unlock locked user TOTP passcodes.
3. Choose the **Authentication** tab.
4. Choose **Two-Factor Authentication**.
5. Press **Unlock** under **Passcode Status**.

   The system displays the message: Account <name of user> unlocked.

**1.5.7.9 Unlock User Password**

You can unlock a user password when the user must log on to the application before the automatic unlock time of 60 minutes has passed.

**Context**

The user locks his or her password after submitting five incorrect passwords when trying to log on to the account. The user receives a notification e-mail that the password log on to the account has been disabled for 60 minutes. After 60 minutes, the user again can log on with his or her password, or choose the link provided in the e-mail to set a new password.

The tenant administrator can unlock the logon to the user account via the administration console.
To unlock the user password manually, proceed as follows:

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   
   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the **User Management** tile.

   The system displays the first 20 users in the tenant sorted by their user ID number.

3. Choose the user whose password you want to unlock.

   For more information about how to find a user in SAP Cloud Platform Identity Authentication service, see [Search Users](#).

4. Choose **Password Details** under the **Authentication** tab.

5. Choose **Unlock**.

   **Remember**
   
   You can only unlock locked user passwords.

**Results**

The password is unlocked. The user can now access his or her account after providing the correct credentials.

**Related Information**

[Send Reset Password E-Mail](#)
1.5.7.10 Send Reset Password E-Mail

You can trigger the sending of an e-mail to the user with reset password information.

Context

Tenant administrator can trigger the sending of an e-mail to the user with reset password information. When the user follows the link provided in the e-mail, the reset password screen appears and the user is prompted to set a new password.

Note

Tenant administrator can send to the user only three reset password e-mails per 24 hours. If the administrator must send more than three e-mails, he or she must reset the counter for e-mail sending first. For more information, see Reset Counter for E-Mail Sending [page 214].

Tip

(For SAML 2.0 Applications) To log out the user from all active session, when a new password is set, configure the SOAP endpoint. For more information, see Configure SAML 2.0 Service Provider [page 55].

To send a reset password e-mail, proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

Note

The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern. Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the User Management tile.

The system displays the first 20 users in the tenant sorted by their user ID number.

3. Choose the user whose password needs to be reset.

For more information about how to find a user in SAP Cloud Platform Identity Authentication service, see Search Users [page 203].

Remember

The maximum number or reset password e-mails that can be sent is three. If you need to send more e-mails, first reset the password counter. For more information, see Reset Counter for E-Mail Sending [page 214].
4. Choose **Password Details** under the **Authentication** tab.

5. Press **Send E-Mail**.

**Results**

The user receives an e-mail with information how to reset his or her password. After resetting the password, he or she is able to log on to the account.

1.5.7.11 **Reset Counter for E-Mail Sending**

You can reset the counter for e-mail sending with reset password information.

**Context**

By default, the tenant administrator can send via the administration console up to three reset password e-mails per 24 hours. If three e-mails are sent, but it is necessary to send a new e-mail, the tenant administrator must first reset the counter for e-mail sending.

To reset the counter for e-mail sending, proceed as follows:

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   
   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the **User Management** tile.

   The system displays the first 20 users in the tenant sorted by their user ID number.

3. Choose the user whose e-mail counter needs to be reset.

   For more information about how to find a user in SAP Cloud Platform Identity Authentication service, see **Search Users** [page 203].

4. Choose **Password Details** under the **Authentication** tab.

5. Press **Reset Counter**.
Results

The counter for the Password Reset option is reset to zero.

Related Information

Send Reset Password E-Mail [page 213]

1.5.7.12 Set Initial Password

You can set initial password for a user that has already activated his or her account.

Context

Tenant administrator can set an initial password for a user that has already activated the account. When the user logs on with the new password, he or she is prompted to change the password with a new one.

→ Tip
(For SAML 2.0 Applications) To log out the user from all active session, when a new password is set, configure the SOAP endpoint. For more information, see Configure SAML 2.0 Service Provider [page 55].

To set an initial password, proceed as follows:

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   → Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the User Management tile.

   The system displays the first 20 users in the tenant sorted by their user ID number.

3. Choose the user who needs an initial password.

   For more information about how to find a user in SAP Cloud Platform Identity Authentication service, see Search Users [page 203].
4. Choose **Password Details** under the **Authentication** tab.
5. Press **Set Initial**.

**Results**

The user logs on to the application with the new password set by the tenant administrator. He or she is prompted to change the password with a new one. After changing the password, the user is able to log on to the application.

### 1.5.8 User Groups

Tenant administrators can create user groups, and assign and unassign groups to users via the administration console for SAP Cloud Platform Identity Authentication service.

A user group is a collection of users. Groups serve to create sets of users who have something in common. For example, users who work in the same department or users who have similar tasks in a company.

<table>
<thead>
<tr>
<th>To learn about</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>How to list the user groups in the tenant</td>
<td>List User Groups [page 218]</td>
</tr>
<tr>
<td>How to list users in a user group</td>
<td>List Users in User Groups [page 219]</td>
</tr>
<tr>
<td>Create a new user group</td>
<td>Create a New User Group [page 217]</td>
</tr>
<tr>
<td>Add a user to a user group via CSV file</td>
<td>Import or Update Users for a Specific Application [page 196]</td>
</tr>
<tr>
<td>Assign groups to a user via the administration console for Identity Authentication</td>
<td>Assign Groups to a User [page 220]</td>
</tr>
<tr>
<td>Unassign groups via the administration console for SAP Cloud Platform Identity Authentication service</td>
<td>Unassign Users from Groups [page 221]</td>
</tr>
<tr>
<td>Delete groups via the administration console for SAP Cloud Platform Identity Authentication service.</td>
<td>Delete User Groups [page 222]</td>
</tr>
</tbody>
</table>
1.5.8.1 Create a New User Group

As a tenant administrator you can create new user groups in the tenant via the administration console for SAP Cloud Platform Identity Authentication service.

Prerequisites

You are assigned the Manage Groups role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].

Context

To create a new user group, proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   ![Note]
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the User Groups tile.

   This operation opens a list of the user groups in the tenant.

3. Press the + Add button at the bottom of the page.

4. Fill in the required fields.

   ![Caution]
   
   The name field can contain lower-case Latin characters (a-z), upper-case Latin characters (A-Z), base 10 digits (0-9), hyphens, and underscores.

5. Save your entries.
1.5.8.2 List User Groups

As a tenant administrator, you can list and view information about the user groups in a tenant in the administration console for Identity Authentication.

Prerequisites

- You are assigned the Manage Groups role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
- You have created user groups in your tenant. For more details how to create user groups, see Create a New User Group [page 217].

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The URL has the https://&lt;tenant ID&gt;.accounts.ondemand.com/admin pattern.</td>
</tr>
<tr>
<td>Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.</td>
</tr>
</tbody>
</table>

2. Choose the User Groups tile.
   This operation opens a list of the user groups in the tenant.
3. Optional: Type a Name or Display name of a group in the search field to filter the list items.
4. Optional: Choose a group from the list on the left to view its details.

Related Information

Create a New User Group [page 217]
Edit Administrator Authorizations [page 241]
1.5.8.3 List Users in User Groups

As a tenant administrator, you can list and view information about the users in a user group in a tenant in the administration console for Identity Authentication.

Prerequisites

- You are assigned the Manage Groups role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
- You have created at least one user group in the tenant. For more details about how to create user groups, see Related Information.
- You have assigned at least one user to the selected user group. For more details about how to assign groups to a user, see Related Information.

Context

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.
   
   i Note
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the User Groups tile.
   
   This operation opens a list of the user groups in the tenant.

3. Optional: Type the Name or Display name of a group in the search field in order to filter the list items.

4. Choose a group from the list on the left.
   
   This will open the User Groups Details view.

5. Choose the Users tab.

Related Information

Create a New User Group [page 217]
1.5.8.4 Assign Groups to a User

As a tenant administrator, you can assign one or more groups created for a specific tenant to a user via the administration console for Identity Authentication.

Prerequisites

- You have created user groups in your tenant. For more details how to create user groups, see Related Information.
- You are assigned the Manage Users role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   Note
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the User Management tile.

   The system displays the first 20 users in the tenant sorted by their user ID number.

3. Choose the user that you want to assign to a group or groups.

4. Choose the User Groups tab.

5. Press the Assign Groups button at the bottom of the page.

6. In the dialog box, select the group or groups that you want to assign to the user.

7. Save your changes.

Next Steps

Configure the attributes that are sent to the application in the assertion. For more information, see Configure the User Attributes Sent to the Application [page 64]
1.5.8.5 Unassign Users from Groups

As a tenant administrator, you can unassign one or more groups that are assigned to a user via the administration console for Identity Authentication.

Prerequisites

- You have created user groups in your tenant. For more details how to create user groups, see Related Information.
- You have assigned groups to the user. For more details how to assign a group or groups to a user, see Related Information.

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
   - **Note**
     - The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
     - Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the User Management tile.

3. Choose the user whose group assignments you want to edit.


5. Select the group or groups that you want to unassign.

6. Press the Unassign Groups button at the bottom of the page.

7. Confirm your changes.
1.5.8.6 Delete User Groups

As a tenant administrator, you can delete one or more user groups in a tenant of SAP Cloud Platform Identity Authentication service.

Prerequisites

You are assigned the Manage Groups role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].

Context

The Delete User Groups operation removes user groups and unassigns all users from them.

To delete one or more groups choose one of the following options:

Delete Multiple Groups

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
   
   **Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern. `Tenant ID` is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the User Groups tile. This operation opens a list of the user groups in the tenant.

3. Choose the icon in the left-hand panel to enter Delete Groups mode. This operation activates the Delete Groups mode.

4. Select the user group or groups that you want to delete.

5. Press the Delete button.
6. Confirm the operation in the pop-up dialog.
   If the operation is successful, the system displays the message `<number> groups deleted`.

## Delete Single Group

### Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
   
   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the *User Groups* tile.
   This operation opens a list of the user groups in the tenant.
3. Select the user group that you want to delete.
4. Press the *Delete* button.
5. Confirm the operation in the pop-up dialog.
   If the operation is successful, the system displays the message `1 group deleted`.

### 1.5.9 User Provisioning

As a tenant administrator, you can configure target systems for user provisioning and provision users to these target systems.

- **Configure SAP Jam Target Systems for User Provisioning** [page 224]
  Tenant administrators can configure SAP Jam target systems for user provisioning via the administration console for SAP Cloud Platform Identity Authentication service.

- **Configure Identity Provisioning Target Systems for User Provisioning** [page 226]
  Tenant administrators can configure Identity Provisioning target systems for user provisioning via the administration console for SAP Cloud Platform Identity Authentication service.

- **Provision Users to Target Systems** [page 228]
  Tenant administrators can provision users of SAP Cloud Platform Identity Authentication service to SAP Jam and Identity Provisioning targets systems.

- **Delete Target System** [page 235]
  As a tenant administrator, you can delete one or more target systems in a tenant of SAP Cloud Platform Identity Authentication service.
1.5.9.1 Configure SAP Jam Target Systems for User Provisioning

Tenant administrators can configure SAP Jam target systems for user provisioning via the administration console for SAP Cloud Platform Identity Authentication service.

Prerequisites

You are assigned the Manage Users role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].

Note

Currently, Identity Authentication supports user provisioning to SAP Jam and SAP Cloud Platform Identity Provisioning service instances.

Remember

Use the Identity Authentication user provisioning feature for up to 500 users. If you want to provision more than 500 user, use SAP Cloud Platform Identity Provisioning service. For more information, see SAP Cloud Platform Identity Provisioning Service

Context

To configure an SAP Jam target system, proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   Note

   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the User Provisioning tile.

   This operation opens a list of the target systems.

3. Press the +Add button on the left-hand panel to add a new target system to the list.
4. Make the corresponding entries in the Target Configurations and Authentication Configurations fields for the target system you want to add.

All fields are obligatory.

➤ Remember
Choose SAP Jam from the drop-down.

5. Save your changes.

If the operation is successful, the system displays the message System <name of system> configuration updated.

6. (Optional) To check the SAP Jam Target System configuration press the Test Connection button.

If the operation is successful, the system displays the message Connection to the selected target system was established successfully.

Note
To change the configuration, select the target system, press Edit, fill in the fields with the new entries, and save your changes.

Next Steps

Provision Users to Target Systems [page 228]

Task overview: User Provisioning [page 223]

Related Information

Configure Identity Provisioning Target Systems for User Provisioning [page 226]
Provision Users to Target Systems [page 228]
Delete Target System [page 235]
User Provisioning [page 223]
1.5.9.2 Configure Identity Provisioning Target Systems for User Provisioning

Tenant administrators can configure Identity Provisioning target systems for user provisioning via the administration console for SAP Cloud Platform Identity Authentication service.

Prerequisites

- You are assigned the Manage Users role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
- You have added a source system in the Identity Provisioning UI with name SAP Cloud Platform Identity Authentication. For more information, see Add System.
- You have registered an OAuth client in the platform cockpit. For more information, see Register an OAuth Client.

**Note**
For Subscription, choose <provider_subaccount>/ips.
For Authorization Grant, choose Client Credentials.

Context

In this scenario you configure SAP Cloud Platform Identity Provisioning service as a target system in Identity Authentication, and Identity Authentication as a source system in Identity Provisioning. As a result Identity Authentication provisions users to Identity Provisioning, which in its turn provisions these users to the targets systems, configured for Identity Authentication.
To configure an Identity Provisioning target system, proceed as follows:

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern. 

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the *User Provisioning* tile.

   This operation opens a list of the target systems.

3. Press the *Add* button on the left-hand panel to add a new target system to the list.

4. Make the corresponding entries in the *Target Configurations* and *Authentication Configurations* fields for the target system you want to add.

   All fields are obligatory.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Display Name</em></td>
<td>Put a name for the target system you are creating.</td>
<td></td>
</tr>
<tr>
<td><em>Type</em></td>
<td>Choose <em>Identity Provisioning</em> from the dropdown.</td>
<td></td>
</tr>
<tr>
<td><em>SCIM URL</em></td>
<td>The SCIM URL should be in the following pattern:</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>https://ips-&lt;subaccount&gt;.&lt;domain&gt;/ips/api/v1/</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>systems/&lt;id of the Identity Authentication source system&gt;/entities/user</code></td>
<td></td>
</tr>
</tbody>
</table>

   For example: `https://ips-abcd1234.hana.ondemand.com/ips/api/v1/systems/12ab12345-1234-alb2-12ab-12a34bcde678d/entities/user`

   **Tip**

   You can copy the basic part of the URL from the cockpit. Under your subaccount, go to

   - [Applications] > [Subscriptions] > [Subscribed HTML5 Applications] > [the Identity Provisioning Service]

   The Application URL is the basic part of the URL.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OAuth URL</td>
<td>In the Cockpit, choose the Security &gt; OAuth section, and go to the Branding tab. Copy the Token Endpoint link and paste it in the OAuth URL field in the administration console for Identity Authentication.</td>
</tr>
<tr>
<td>Client ID</td>
<td>Use the ID of your registered OAuth client.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>Use the Secret of your registered OAuth client.</td>
</tr>
</tbody>
</table>

5. Save your changes.

If the operation is successful, the system displays the message System <name of system> configuration updated.

Task overview: User Provisioning [page 223]

Related Information

Configure SAP Jam Target Systems for User Provisioning [page 224]
Provision Users to Target Systems [page 228]
Delete Target System [page 235]
User Provisioning [page 223]

1.5.9.3 Provision Users to Target Systems

Tenant administrators can provision users of SAP Cloud Platform Identity Authentication service to SAP Jam and Identity Provisioning targets systems.

Prerequisites

- You are assigned the Manage Users role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
- You have configured a target system in the administration console for Identity Authentication. For more details about how to configure target systems, see Configure SAP Jam Target Systems for User
i Note

Currently, Identity Provisioning supports user provisioning to instances of:

- SAP Jam

Remember

Use the Identity Authentication user provisioning feature for provisioning of up to 500 users. If you want to provision more than 500 users, use SAP Cloud Platform Identity Provisioning service. For more information, see SAP Cloud Platform Identity Provisioning Service.

- SAP Cloud Platform Identity Provisioning service

Context

Identity Authentication supports the following scenarios for user provisioning to target systems:

- Provision all users to selected target systems - In this scenario, all users in the user store of Identity Authentication are provisioned to a specific target system. The tenant administrator chooses the target system that all users will be provisioned to.
- Provision selected users to all target systems - In this scenario, the tenant administrator provisions particular users to all target systems that are configured. The administrator chooses which users to provision.
- Provision users from corporate user store - In this scenario, the users who are stored in a corporate user store are provisioned during authentication.
- Provision users at user creation and update - In this scenario, all newly created or updated users are automatically provisioned to all target systems.

Remember

The users that are in the user store of Identity Authentication are provisioned to the SAP Jam target system with a certain set of attributes. The table below shows the attributes taken from Identity Authentication and their mapping to the SAP Jam target system.

<table>
<thead>
<tr>
<th>SAP Cloud Platform Identity Authentication Service Attribute</th>
<th>SAP Jam Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Schema</td>
<td></td>
</tr>
<tr>
<td>firstName</td>
<td>name.givenName</td>
</tr>
<tr>
<td>lastName</td>
<td>name.familyName</td>
</tr>
<tr>
<td>uid</td>
<td>userName</td>
</tr>
<tr>
<td>SAP Cloud Platform Identity Authentication Service Attribute</td>
<td>SAP Jam Attribute</td>
</tr>
<tr>
<td>-------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>title</td>
<td>jobFunction</td>
</tr>
<tr>
<td>userType</td>
<td>type</td>
</tr>
<tr>
<td>mail</td>
<td>emails.value</td>
</tr>
<tr>
<td>status</td>
<td>active</td>
</tr>
<tr>
<td>telephone</td>
<td>phoneNumbers[work].value</td>
</tr>
<tr>
<td>street</td>
<td>addresses[home].streetAddress</td>
</tr>
<tr>
<td>city</td>
<td>addresses[home].locality</td>
</tr>
<tr>
<td>zip</td>
<td>addresses[home].postalCode</td>
</tr>
<tr>
<td>country</td>
<td>addresses[home].country</td>
</tr>
<tr>
<td>companyStreet</td>
<td>addresses[work].streetAddress</td>
</tr>
<tr>
<td>companyCity</td>
<td>addresses[work].locality</td>
</tr>
<tr>
<td>companyZip</td>
<td>addresses[work].postalCode</td>
</tr>
<tr>
<td>companyCountry</td>
<td>addresses[work].country</td>
</tr>
<tr>
<td>locale</td>
<td>locale</td>
</tr>
</tbody>
</table>

**Note**

- **active** is true only when **status** in SAP Cloud Platform Identity Authentication service is equal to active. In the other case **active** is false.

**Caution**

Do not send **locale** if **language** or **country** user attribute is missing.

**Enterprise User Schema Extension**
If Identity Authentication is used as proxy to delegate the authentication to a corporate identity provider, the users that are authenticated by the corporate identity provider will not be provisioned during authentication.

When you delete a user, he or she is automatically deprovisioned from the configured target systems.

To provision users, choose one of the options below and follow the corresponding procedure.

**Task overview:** User Provisioning [page 223]

**Related Information**

Configure SAP Jam Target Systems for User Provisioning [page 224]
Configure Identity Provisioning Target Systems for User Provisioning [page 226]
Delete Target System [page 235]

**Provision All Users to a Selected Target System**

**Context**

The tenant administrator can select the target systems that all users will be provisioned to.

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
2. Choose the User Provisioning tile.
   This operation opens a list of the target systems.
3. Choose the list item of the target system that you want to provision the users to.
   ! Note
   If you do not have a configured target system in your list, you can add one. For more details, see Configure SAP Jam Target Systems for User Provisioning [page 224].
   If the operation is successful, the system displays the message <number of users> provisioned.

**Provision Selected Users to All Target Systems**

**Context**

The tenant administrator can choose which of the users to be provisioned to the configured target systems.

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
   ! Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.
2. Choose the User Management tile.
   The system displays the first 20 users in the tenant sorted by their user ID number.
3. Optional: You can choose one of the following:
Search Options

List All Users

Press More

This will expand the list by 20 users.

**i Note**

This option is available only if the users in the tenant are more than 20.

**Simple Search**

- (default mode) Type your search criteria string in the search field and press the key
- (when in Advanced Search mode) Press Simple Search, type your search criteria string in the search field, and press the Enter key

Once the search is completed, the system will list the users whose User ID, E-Mail, or Login Name match your search criteria string. In this case the system does not include the First Name and Last Name fields in the search.

If you are not satisfied with the search result, edit your search criteria and repeat the step again.

**i Note**

The search is case insensitive. The system searches for entries that begin with the typed string.

If you place asterix (*) in the beginning or in the middle of your search string the system will treat it as a regular character and will include it in the search. For example, if you type *on in the search field, the system will look for users whose first three letters in any of the three fields are *on. If you type on or on* in the search field, the system will look for users whose first two letters in any of the three fields are on.
Advanced Search

Press Advanced Search and type your search criteria strings in at least one of the search fields.

The system checks the search fields simultaneously. Once the search is completed, it will list the users that match the search criteria from all the fields.

**Note**
The search is case insensitive. The system searches for entries that begin with the typed string.

If you place asterix (*) in the beginning or in the middle of your search string the system will treat it as a regular character and will include it in the search. For example, if you type *on in the First Name field, the system will look for users whose first three letters of the first name are *on. If you type on or on* in the First Name field, the system will look for users whose first two letters of the first name are on.

4. Select the checkbox next to the user or users that you want to provision.
5. Press Provision Users.
6. Confirm the operation.

If the operation is successful, the system displays the message `<number of users> provisioned`.

**Provision Users from Corporate User Store**

A user is automatically provisioned after he or she has been authenticated.

For more information about how to configure Identity Authentication to use a corporate user store in addition to its own user store, see Configure Connection to a Corporate User Store [page 143].

**Provision Users at User Create and User Update**

All newly created and updated users are automatically provisioned to the target systems configured in the administration console for Identity Authentication. The users that use the self-registration service will be automatically provisioned to the target systems too.

For more information about user creation or user update, see Related Information
1.5.9.4 Delete Target System

As a tenant administrator, you can delete one or more target systems in a tenant of SAP Cloud Platform Identity Authentication service.

Prerequisites

You are assigned the Manage Users role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].

Task overview: User Provisioning [page 223]

Delete Multiple Target Systems

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the User Provisioning tile.
   This operation opens a list of the target systems.

3. Choose the icon in the left-hand panel.
   This operation activates the Delete Target Systems mode.

4. Select the target system or systems that you want to delete.
5. Choose the Delete button.
6. Confirm the operation in the pop-up dialog.
   Once the target system or systems have been deleted, the system displays the message <number> target systems deleted.

Delete Single Target System

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the User Provisioning tile.
   This operation opens a list of the target systems.

3. Select the target system that you want to delete.
4. Choose the Delete button in the right-hand panel to delete the selected target system.
5. Confirm the operation in the pop-up dialog.
   Once the application has been deleted, the system displays the message 1 target system deleted.

Related Information

User Provisioning [page 223]
1.5.10 Managing Administrators

This section describes how, as a tenant administrator, you can list all administrators in the administration console for SAP Cloud Platform Identity Authentication Service, add new administrators, and edit the administrator authorizations.

Related Information

List Administrators [page 237]
Add Administrators [page 238]
Edit Administrator Authorizations [page 241]

1.5.10.1 List Administrators

As a tenant administrator, you can list the administrators and their authorizations in the administration console for SAP Cloud Platform Identity Authentication service

Context

To list all administrators, proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern. Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Administrators tile.

   This operation opens a list of all administrators in alphabetical order.

   The list also includes the SAP Cloud Platform system, which by default has authorizations to set up the trust with Identity Authentication.
3. Choose the name from the list item to view the profile details, such as user ID and e-mail, and the authorizations assigned to the administrator.

→ Tip
Type the name of the administrator in the search field to filter the list items.

Related Information

Identity Authentication Tenant as an Application Identity Provider
Edit Administrator Authorizations [page 241]

1.5.10.2 Add Administrators

As a tenant administrator, you can add new administrators in the administration console for SAP Cloud Platform Identity Authentication service

Prerequisites

To add new tenant administrators, you must be assigned the Manage Tenant Configuration role.

Context

You can add both a person and a system in the administration console for Identity Authentication to act as administrators. The system can receive the same roles and can perform the same actions as the human administrator.

1.5.10.2.1 Add User as Administrator

Context

To add a person as a new tenant administrator, proceed as follows:
Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   **Note**
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   
   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the *Administrators* tile.

   This operation opens a list of all administrators in alphabetical order.

   **Note**
   The list also includes the SAP Cloud Platform system, which by default has authorizations to set up the trust with Identity Authentication.

3. Press the *+Add* button on the left-hand panel to add a new administrator to the list.

4. Choose *Add User*.

5. Make the appropriate entries in the *Email*, *First Name*, and *Last Name* fields for the user you want to add as an administrator.

   The *First Name*, and *Last Name* fields will be prefilled automatically for users that already exist in system.

6. Assign the required administrator roles for the user.

   To be a tenant administrator, a user must be assigned at least one of the following roles.

   **Administrator Roles**

<table>
<thead>
<tr>
<th>Authorization</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Applications</td>
<td>This role gives the tenant administrator permission to configure the applications via the administration console.</td>
</tr>
<tr>
<td>Manage Corporate Identity Providers</td>
<td>This role gives the tenant administrator permission to configure the identity providers via the administration console.</td>
</tr>
<tr>
<td>Manage Users</td>
<td>This role gives the tenant administrator permission to manage, import, and export users via the administration console.</td>
</tr>
<tr>
<td>Manage Groups</td>
<td>This role gives the tenant administrator permission to create, edit, and delete user groups via the administration console.</td>
</tr>
<tr>
<td>Manage Tenant Configuration</td>
<td>This role gives the tenant administrator permission to manage tenant configuration and authorization assignment to users.</td>
</tr>
</tbody>
</table>

   By default, all administrator roles are assigned.

7. Save your changes.
1.5.10.2.2 Add System as Administrator

Context

To add a system as a new tenant administrator, proceed as follows:

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.
   
   i Note
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Administrators tile.
   
   This operation opens a list of all administrators in alphabetical order.
   
   i Note
   
   The list also includes the SAP Cloud Platform system, which by default has authorizations to set up the trust with Identity Authentication.

3. Press the +Add button on the left hand panel in order to add a new administrator to the list.
4. Choose Add System:
5. Enter the name of the system under Name.
6. Assign the required administrator roles for the system.
   
   To be a tenant administrator, a user must be assigned at least one of the following roles.

<table>
<thead>
<tr>
<th>Administrator Roles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Applications</td>
<td>This role gives the tenant administrator permission to configure the applications via the administration console.</td>
</tr>
<tr>
<td>Manage Corporate Identity Providers</td>
<td>This role gives the tenant administrator permission to configure the identity providers via the administration console.</td>
</tr>
<tr>
<td>Manage Users</td>
<td>This role gives the tenant administrator permission to manage, import and export users via the administration console.</td>
</tr>
<tr>
<td>Manage Groups</td>
<td>This role gives the tenant administrator permission to create, edit and delete user groups via the administration console.</td>
</tr>
<tr>
<td>Authorization</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Manage Tenant</td>
<td>Configuration This role gives the tenant administrator permission to</td>
</tr>
<tr>
<td></td>
<td>manage tenant configuration and authorization assignment to users.</td>
</tr>
</tbody>
</table>

All administrator roles are assigned by default.

7. Configure the method for authentication when the system is used. You can choose from the following two options:
   - Certificate
   - Password

   **Note**
   User ID and password are used for basic authentication when Identity Authentication is used. The user ID is generated automatically when you set the password for the first time.

8. Save your entries.

### 1.5.10.3 Edit Administrator Authorizations

As a tenant administrator, you can edit both your own authorizations and other administrators' authorizations in the administration console for SAP Cloud Platform Identity Authentication service.

#### Prerequisites

To edit tenant administrators' authorizations, you must be assigned the Manage Tenant Configuration role.

#### Context

To edit an administrator's authorizations, proceed as follows:

#### Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   **Note**
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Administrators tile.

This operation opens a list of all administrators in alphabetical order.

i Note
The list also includes the SAP Cloud Platform system, which by default has authorizations to set up the trust with Identity Authentication.

3. Choose the administrator name whose authorizations you want to edit.

Tip
Type the name of the administrator in the search field to filter the list items.

4. Edit the administrator authorizations as required.

i Note
To be a tenant administrator, a user must be assigned one or more of the following roles:

<table>
<thead>
<tr>
<th>Administrator Roles</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Applications</td>
<td>This role gives the tenant administrator permission to configure the applications via the administration console.</td>
</tr>
<tr>
<td>Manage Corporate Identity Providers</td>
<td>This role gives the tenant administrator permission to configure the identity providers via the administration console.</td>
</tr>
<tr>
<td>Manage Users</td>
<td>This role gives the tenant administrator permission to manage, import, and export users via the administration console.</td>
</tr>
<tr>
<td>Manage Groups</td>
<td>This role gives the tenant administrator permission to create, edit, and delete user groups via the administration console.</td>
</tr>
<tr>
<td>Manage Tenant Configuration</td>
<td>This role gives the tenant administrator permission to manage tenant configuration and authorization assignment to users.</td>
</tr>
</tbody>
</table>

If you remove all authorizations, the user will no longer be a tenant administrator, and the name will be removed from the list on the left.

You cannot remove the Manage Tenant Configuration role from your own user.

5. Save your changes.

If the operation is successful, the system displays the message Tenant administrator <name of tenant administrator> updated.
Related Information

Identity Authentication Tenant as an Application Identity Provider

1.5.11 Corporate Identity Providers

Initially, Identity Authentication is set as the default identity provider for the applications. This section describes the scenarios in which Identity Authentication acts as a proxy to delegate the authentication to a corporate identity provider.

Identity Provider Proxy Overview

An identity provider can function as a proxy for another identity provider. An identity provider proxy enables you to create structures of trust relationships that ultimately simplify the management of your service providers.

A proxy relationship involves the following participants:

- **Corporate Identity Provider**
  The authenticating identity provider trusts the service provider of the identity provider proxy.

- **Identity Provider Proxy**
  The identity provider proxy is both an identity provider and a service provider. The service provider of the identity provider proxy trusts the authenticating identity provider.

- **Application**
  A service provider hosts a service that users want to access. This service provider trusts the identity provider of the identity provider proxy.

There is no direct trust relationship between the authenticating identity provider and the service provider that the user is trying to access.

Use Identity Authentication as Proxy

<table>
<thead>
<tr>
<th>To learn about</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>How Identity Authentication can use a SAML 2.0 identity provider as an external authenticating authority. Identity Authentication acts as a proxy.</td>
<td>Configure Trust with Corporate Identity Provider [page 256]</td>
</tr>
<tr>
<td>How to choose a type for the corporate identity provider</td>
<td>Choose Identity Provider Type [page 260]</td>
</tr>
<tr>
<td>How to delete corporate identity providers</td>
<td>Delete Corporate Identity Providers [page 261]</td>
</tr>
</tbody>
</table>
To learn about | See
---|---
How to configure the *Identity Federation* option | Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 266]
How to configure your systems for IdP-Initiated SSO with a corporate identity provider | Configure IdP-Initiated SSO with Corporate Identity Providers [page 244]
How to redirect the user to specific URL after logout | Service Provider Initiated Logout with Corporate Identity Providers [page 254]

## 1.5.11.1 Configure IdP-Initiated SSO with Corporate Identity Providers

This document shows you how to configure identity provider (IdP) initiated single sign-on (SSO) with corporate identity providers.

This use case is suitable for customers and partners who need to provide access to a cloud application for their employees via their corporate identity providers. In this scenario, the authentication starts at the corporate identity provider (IdP), with Identity Authentication being in the role of an identity provider proxy. As such, Identity Authentication will act as an SAML 2.0 identity provider to the service provider, and as an SAML 2.0 service provider to the corporate identity provider or providers. Once a user is authenticated at the corporate identity provider, successive authentication requests from the service provider, which use the same corporate identity provider will not be forwarded to it while the session at Identity Authentication is active. Identity Authentication will issue assertions based on the user data received during the first authentication.
This scenario also supports authentication with more than one corporate identity provider.
Configuration Steps

For this scenario, the configurations are made by users with different roles in different systems.

### Configuration and Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>System to be configured</th>
<th>What has to be configured</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application administrator</td>
<td>Consumer application</td>
<td>Trust</td>
<td>1. Configure the Application [page 247]</td>
</tr>
</tbody>
</table>

**Legend**
- Cloud
- On Premise
## Prerequisites

The IDP-Initiated SSO option in the tenant of Identity Authentication must be enabled.

**i Note**

IDP-Initiated SSO is enabled by default in Identity Authentication. For more information about how the tenant administrator can enable or disable this option, see Configure IdP-Initiated SSO [page 162].

### 1.5.11.11 1. Configure the Application

**Context**

The following configuration is made by the administrator of the application.

As an administrator of the application, you have to configure SAP Cloud Platform Identity Authentication service as a trusted identity provider for the application.

**i Note**

To do this, you will need the SAML 2.0 metadata of Identity Authentication. To receive the metadata, contact the tenant administrator of Identity Authentication.
Next Steps

Send the metadata of the service provider to the administrator of Identity Authentication. This is required for setting up the trust on the Identity Authentication provider side.

1.5.11.1.2 2. Configure SAP Cloud Platform Identity Authentication Service

Context

In the scenario where Identity Authentication acts as an identity provider proxy, it is in the role of an identity provider for the application, and a service provider for the corporate identity provider. You should configure trusts with the service provider and the corporate identity provider.

The following configuration is made by the tenant administrator of Identity Authentication.

Procedure

1. Configure trust with the service provider via the administration console. For more information, see Configure SAML 2.0 Service Provider [page 55].

   For this procedure, you will need the metadata from the service provider. If you do not have this, contact the administrator of the application.

   The service provider metadata that is used to configure the trust must contain the default assertion consumer service (ACS) endpoint that can process unsolicited SAML responses. With SAP Cloud Platform, the endpoint is the URL of the application’s protected page.

   → Remember

   If your scenario includes the enabling of the Trust All Corporate Identity Providers option in the administration console, the service provider metadata that is used to configure the trust must contain also the assertion consumer (ACS) endpoint with the URL of the application’s protected page and the index.

   → Sample Code

   <ns3:AssertionConsumerService index="1" isDefault="false"
   Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
   Location="https://<application URL>/protected.jsp" />


2. Configure a trust with the corporate identity provider. For more information, see Configure Trust with Corporate Identity Provider [page 256].

For this procedure, you will need the metadata from the corporate identity provider. If you do not have this, contact the administrator of the corporate identity provider.

3. Select identity provider. You have the following options:
   ○ If your scenario includes more than one corporate identity provider, enable the Trust All Corporate Identity Providers feature in the administration console. For more information, see Enable IdP-Initiated SSO from All Corporate Identity Providers [page 127].
   ○ If your scenario includes only one corporate identity provider, set the configured identity provider as the authenticating identity provider for the application. For more information, see Choose Default Identity Provider for an Application [page 112].

**Next Steps**

1. Send the Entity ID of the service provider to the administrator of the corporate identity provider. The administrator needs this information for the consumer assertion endpoint configuration.

   → **Tip**
   
   The Entity ID of the service provider is in the administration console in Applications > <application_name> > Trust > SAML 2.0 Configuration > Name.

   → **Remember**
   
   If your scenario includes the enabling of the Trust All Corporate Identity Providers option in the administration console, send also the index of the ACS endpoint of the application’s protected page. The administrator needs this information for the consumer assertion endpoint configuration.

2. Send the metadata of the tenant of Identity Authentication to the administrator of the service provider and the administrator of the corporate identity provider. They need the metadata for the trust configurations of the systems. For more information about how to download the tenant metadata, see Tenant SAML 2.0 Configuration [page 130].

**1.5.11.1.3 3. Configure the Corporate Identity Provider**

**Context**

The following configuration is made by the administrator of the corporate identity provider.
**Procedure**

1. Register SAP Cloud Platform Identity Authentication service as a service provider.

   **i Note**
   To do this, you will need the SAML 2.0 metadata of Identity Authentication. If you do not have this, contact the tenant administrator of Identity Authentication.

   **Tip**
   For more information about how to register Identity Authentication as a service provider, consult the corporate identity provider documentation. If the corporate identity provider is also a tenant of Identity Authentication, see Configure Trust [page 55].

2. Add the `sp=<sp_name>` parameter, and the index of the application’s assertion consumer service (ACS) endpoint URL, if provided. Replace the `sp_name` with the Entity ID of the service provider. This parameter is needed for Identity Authentication to know which service provider to redirect the user to after successful authentication.

   **Tip**
   The ACS endpoint URL should have the following format: `https://<the current ACS endpoint URL>?sp=<sp_name>&index=<index_number>`. Request the Entity ID of the service provider, and the index of the application’s protected page from the tenant administrator of Identity Authentication.
   The index is required.

**Results**

Once the trust is configured, the user can access the application via the link sent by the corporate identity provider administrator. For more information about how to configure the link for the IdP-initiated SSO scenario, consult the corporate identity provider documentation.

**Tip**

If your corporate identity provider is Identity Authentication, the link for IdP-Initiated SSO follows the pattern: `https://<tenant_ID>.accounts.ondemand.com/saml2/idp/sso?sp=<sp_name>&[&RelayState=<sp_specific_value>&index=<index_number>].` In this use case, replace the `sp_name` with the Entity ID of the tenant of Identity Authentication acting as the service provider. The `RelayState` is not mandatory and can be skipped. If your scenario includes only one corporate identity provider, the `index` parameter is not mandatory and also can be skipped. If your scenario includes more than one corporate identity provider, and the *Trust All Corporate Identity Providers* feature in the administration console is enabled, the `index` is used to determine the ACS endpoint which could process unsolicited SAML responses. For more information about the configuration, see Configure IdP-Initiated SSO [page 162].
Next Steps

Send the metadata of the corporate identity provider to the administrator of Identity Authentication. This will be needed for setting up the trust.

1.5.11.1.4 4. Optional: Configure Additional Settings in SAP Cloud Platform Identity Authentication Service

Context

The following configurations are made by the tenant administrator of SAP Cloud Platform Identity Authentication service.

Follow the procedures in this document if you want to:

- Restrict Access to Users in Identity Authentication User Store
- Restrict Access to Users in Certain User Groups
- Send Specific Assertion and Name ID Attributes to the Application

Restrict Access to Users in SAP Cloud Platform Identity Authentication Service User Store

Context

This configuration allows you to restrict access to the application to users who are in the Identity Authentication user store. Users who are not in the user store of Identity Authentication will not be able to access the application.

Procedure

1. Import the users that you will grant access to the application to via a CSV file import.
   For more information about how to import users in Identity Authentication, see Import or Update Users for a Specific Application [page 196].
2. Switch on the identity federation option in the administration console. For more information, see Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 266].
   This option allows the application to check if the users authenticated by the corporate identity provider exist in the user store of Identity Authentication.
Results

Only users that are in the user store of Identity Authentication will be able to access the application. If a user is not part of the user store of Identity Authentication, this user receives the following message: *Sorry, but you are currently not authorized for access.*

The settings in the application configuration for assertion attributes and name ID attribute will be used for issuing the assertion. For more information, see Configure the User Attributes Sent to the Application [page 64] and Configure the Name ID Attribute Sent to the Application [page 67].

Restrict Access to Users in Certain User Groups

Context

This configuration allows you to restrict the access to the application only to users who belong to certain user groups. This option is suitable for scenarios with more than one corporate identity providers. The tenant administrator assigns different groups to different identity providers and users, and can thus specify that certain users come from specific identity providers by assigning the same groups to them. Identity Authentication can thus check if the users are authenticated by the identity provider that they belong to.

Procedure

1. Make sure that the required user groups are created in the administration console of Identity Authentication. For more information, see Create a New User Group [page 217].
2. Import the users that you will grant access to the application via a CSV file import.

⚠️ Caution

The groups in the Groups column in your CSV file must match the groups that you created via the administration console.

For more information about how to import users in Identity Authentication, see Import or Update Users for a Specific Application [page 196].
3. Switch on the identity federation option in the administration console, and assign user groups to the corporate identity provider. For more information, see Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 266].

Results

Only the members of these groups will be authorized to access applications after successful authentication. If a user is not part of the groups, this user receives the following message: *Sorry, but you are currently not authorized for access.*
Send Specific Assertion and Name ID Attributes to the Application

Context

When the identity federation feature is disabled, Identity Authentication sends to the application the same attributes it has received from the corporate identity provider.

When the identity federation feature is enabled, Identity Authentication checks if a user with the respective unique identifier, written in the NameID attribute in the assertion coming from the corporate identity provider, exists in the user store of Identity Authentication. The following options exist:

- If the user exists, Identity Authentication issues a new assertion with Name ID and assertion attributes, configured for the application.
- If the user does not exist in the user store of Identity Authentication this user receives the following message: Sorry, but you are currently not authorized for access.

This configuration can be used if you want the application to receive assertions and name ID attributes that are different from those sent by the corporate identity provider.

If you want the application to receive assertions and name ID attributes that are different from those sent by the corporate identity provider, do the following: Configure the User Attributes Sent to the Application [page 64] and Configure the Name ID Attribute Sent to the Application [page 67].

Procedure

1. Switch on the identity federation option in the administration console. For more information, see Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 266].
2. Configure the user attributes and Name ID attribute sent to the application. For more information, see:
   - Configure the User Attributes Sent to the Application [page 64]
   - Configure the Name ID Attribute Sent to the Application [page 67]

Results

The application will receive in the assertion the attributes and name ID attribute that you have configured in Identity Authentication. They will be different from those that the corporate identity provider sent to Identity Authentication.
1.5.11.2 Service Provider Initiated Logout with Corporate Identity Providers

This document provides information about the service provider initiated logout with corporate identity providers.

In this scenario, SAP Cloud Platform Identity Authentication service has to be configured as an identity provider proxy. The corporate identity provider acts as an authenticating IdP to the application.

The logout procedure is triggered by the user at the service provider and results in a logout request sent to the identity provider proxy. Consequently, the identity provider proxy processes the request and destroys any local session information about the user. The identity provider proxy then checks whether there are other service providers in the single sign-on (SSO) session and sends logout requests to all of them. In return, the service providers send logout responses to the identity provider proxy informing it that the logout process is successful. Finally, the identity provider proxy sends a logout response to the original requesting service provider or the service provider of the application.

As an additional option, the tenant administrator of Identity Authentication can configure a URL which is sent in the SAML 2.0 Logout Response as an extension. The URL can be used to redirect the users after logging out of the application. The URL is specific for each corporate identity provider with which Identity Authentication has established a trust. For more information about this option, see Configure Logout URL [page 255].

Corporate Identity Provider Logout Flow

When Identity Authentication acts as a proxy to delegate authentication to an external corporate identity provider, and the user who is logged on to one or more applications chooses the Log Out link in one of the applications, the following flow is in force:

1. The user triggers a logout from the application.
2. Identity Authentication checks if the user is logged on to other applications. If yes, Identity Authentication sends logout requests to the applications, and terminates the sessions.
3. Identity Authentication sends logout requests to the corporate identity provider or corporate identity providers, if there are more than one.
4. The user is logged out of the corporate identity providers.
5. The user is logged out of Identity Authentication.
6. A logout response is sent to the initiating application.
7. (Optional) If the Redirect URL option is configured in the administration console for Identity Authentication, the URL is sent as an extension in the SAML 2.0 Logout Response. This option can be used by the application to redirect the user to the destination from the link configured for the specific corporate identity provider.

**i Note**

This step is valid only if the application supports the redirect of the user, as for example SAP SuccessFactors HCM Suite.
1.5.11.2.1 Configure Logout URL

As a tenant administrator, you can specify a link which is sent as an extension in the SAML 2.0 Logout Response. The link can be used by the application to redirect the user after successfully logging out of the application when Identity Authentication acts as an identity provider proxy.

Prerequisites

Identity Authentication must be configured to act as an identity provider proxy to delegate the authentication to a corporate identity provider. For more information, see Configure Trust with Corporate Identity Provider [page 256].

Context

When the user logs out of an application via a service provider initiated logout he or she can be redirected to a specific URL. This configuration can be applied to scenarios with one or more corporate identity providers. You configure a specific redirect URL in the administration console for Identity Authentication for each corporate identity provider.

1. Triggers Logout from the application.
2. Sends SAML Logout Request.
5. Sends SAML Logout Response with redirect URL.
6. Application redirects the user to the configured URL.

To configure the logout URL, follow the procedure:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.
2. Choose the **Corporate Identity Providers** tile.

3. Select the corporate identity provider that you want to configure.
   - If you do not have an identity provider in your list, choose the **Add** button to create one, and proceed with the configuration.
   - If you have an identity provider in your list, choose the one that you want to edit.

   **Tip**
   Type the name of the identity provider in the search field to filter the list items.

4. Choose **Logout Redirect URL**.
5. Type the redirect URL in the provided field.
6. Save your changes.

**Results**

Once the user has logged out of the application, Identity Authentication sends the logout URL in the SAML 2.0 Response as an extension to the application. The logout URL can be used by the application to redirect the user to the URL configured for the corporate identity provider in the administration console for Identity Authentication.

### 1.5.11.3 Configure Trust with Corporate Identity Provider

This document is intended to help you configure trust with a corporate identity provider in the administration console for SAP Cloud Platform Identity Authentication service. In this scenario Identity Authentication acts as a proxy to delegate the authentication to the corporate identity provider.

**Prerequisites**

- You are assigned the **Manage Corporate Identity Providers** role. For more information about how to assign administrator roles, see [Edit Administrator Authorizations](page 241).
- You have registered Identity Authentication as service provider at the corporate identity provider. For more information, see the documentation provided by the corporate identity provider.

**Note**

If you want to use IdP-initiated single sign-on (SSO) from your corporate identity provider, you have to add the parameter `sp=<sp_name>` to the assertion consumer service (ACS) endpoint configured on your corporate identity provider side for Identity Authentication.

**Example**

https://<the current ACS endpoint URL>?sp=<sp_name>
sp is the name of the SAML 2 service provider for which SSO is performed.

To see how to download the SAML 2.0 metadata of Identity Authentication read Tenant SAML 2.0 Configuration [page 130].

- You have downloaded the corporate identity provider metadata. For more information, see the documentation provided by the corporate identity provider.

**Context**

Identity Authentication can use a SAML 2.0 identity provider as an external authenticating authority. Identity Authentication thus acts as a proxy to delegate authentication to the external corporate identity provider. The requests for authentication sent by a service provider will be forwarded to the corporate identity provider.

As an identity provider proxy, Identity Authentication will act as an SAML 2.0 identity provider to the service provider, and as an SAML 2.0 service provider to the corporate identity provider. Once a user is authenticated at the corporate identity provider, successive authentication requests from service providers, which use the same corporate identity provider will not be forwarded to it as long as the session at Identity Authentication is active. Identity Authentication will issue assertions based on the user data received during the first authentication.

To use Identity Authentication as a proxy to delegate authentication to an external corporate identity provider you have to configure trust with that corporate identity provider. To configure a trusted corporate identity provider, proceed as follows:

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the **Corporate Identity Providers** tile.
3. Select the corporate identity provider that you want to configure.
   - If you do not have an identity provider in your list, choose the *Add* button to create one, and proceed with the configuration.
   - If you have an identity provider in your list, choose the one that you want to edit.

   **Tip**
   
   Type the name of the identity provider in the search field to filter the list items.
4. Under **SAML 2.0**, choose **SAML 2.0 Configuration**.

5. Upload the corporate identity provider metadata XML file or manually enter the communication settings negotiated between Identity Authentication and the identity provider.

   **Note**

   Use a file with an extension `.xml`.

   When the identity provider metadata is uploaded, the fields are populated automatically with the parsed data from the XML file. The minimum configuration is to complete the **Name** field, add at least one single sign-on endpoint, and provide a signing certificate.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata File</td>
<td>The metadata XML file of the identity provider.</td>
</tr>
<tr>
<td>Name</td>
<td>The entity ID of the identity provider.</td>
</tr>
<tr>
<td>Single Sign-On Endpoint URL</td>
<td>The URL of the identity provider's single sign-on endpoint that receives authentication requests.</td>
</tr>
<tr>
<td>Single Logout Endpoint URL</td>
<td>The URL of the identity provider's single logout endpoint that receives logout messages.</td>
</tr>
<tr>
<td>Binding</td>
<td>The SAML-specified HTTP binding used by the identity provider showing how the various SAML protocol messages can be carried over underlying transport protocols.</td>
</tr>
<tr>
<td>Signing Certificate</td>
<td>A base64-encoded certificate used by the identity provider to digitally sign SAML protocol messages sent to Identity Authentication.</td>
</tr>
</tbody>
</table>

6. Save your selection.

   Once the identity provider has been updated, the system displays the message **Identity provider <name of identity provider> updated**.

**Next Steps**

- Select the configured identity provider as the authenticating identity provider for the application. For more information, see **Choose Default Identity Provider for an Application** [page 112].
- (Optional) Configure the Name ID Format Sent to the Corporate IdP [page 259]

**Related Information**

- [SAML 2.0](#)
- [Edit Administrator Authorizations](#)
- [Configure IdP-Initiated SSO](#)
1.5.11.4 (Optional) Configure the Name ID Format Sent to the Corporate IdP

Context

When SAP Cloud Platform Identity Authentication service uses a SAML 2.0 identity provider (IdP) as an external authenticating authority it acts as a proxy to delegate authentication to that external corporate identity provider. As an identity provider proxy, Identity Authentication acts as a SAML 2.0 identity provider to the service provider, and as a SAML 2.0 service provider to the corporate identity provider. The requests for authentication sent by the service provider are forwarded by Identity Authentication to the corporate identity provider. In this scenario, the tenant administrator can configure the name ID format that is sent to the corporate identity provider. The name ID format is used in the `Format` attribute of the `NameID` element that Identity Authentication sends to the corporate identity provider with the SAML assertion.

→ Remember

To use Identity Authentication as a proxy to delegate authentication to an external corporate identity provider you have to configure trust with that corporate identity provider. For more information, see Configure Trust with Corporate Identity Provider [page 256].

To set the name ID format to be sent to the corporate identity provider, proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note

   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Corporate Identity Providers tile.

3. Select the corporate identity provider that you want to configure.
   ○ If you do not have an identity provider in your list, choose the Add button to create one, and proceed with the configuration.
   ○ If you have an identity provider in your list, choose the one that you want to edit.

   → Tip

   Type the name of the identity provider in the search field to filter the list items.

4. Under SAML 2.0, choose Name ID Format.
5. Select the name ID format from the following:
   - **None** - Name ID format is not sent. Corporate identity provider decides which attribute to use.
   - **Default** - The name ID format received from the application is sent.
   - **Unspecified** - The name ID format `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified` is always sent.
   - **E-Mail** - The name ID format `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress` is always sent.

6. Save your selection.
   Once the identity provider has been updated, the system displays the message **Identity provider <name of identity provider> updated**.

**Related Information**

Configure Trust with Corporate Identity Provider [page 256]
Choose Identity Provider Type [page 260]

### 1.5.11.5 Choose Identity Provider Type

This topic shows you how to choose a type for the corporate identity provider.

**Prerequisites**

You are assigned the **Manage Corporate Identity Providers** role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **Note**

   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the **Corporate Identity Providers** tile.
3. Select the corporate identity provider that you want to configure.
If you do not have an identity provider in your list, choose the Add button to create one, and proceed with the configuration.

If you have an identity provider in your list, choose the one that you want to edit.

Tip
Type the name of the identity provider in the search field to filter the list items.

4. Choose Identity Provider Type.
5. Select the radio button for the type of the identity provider.

You can choose one of the following options:
- SAML 2.0 Compliant
- SAP Single Sign-On
- Microsoft ADFS / Azure AD

6. Save your selection.

Once the identity provider has been updated, the system displays the message Identity provider <name of identity provider> updated.

Related Information

Corporate Identity Providers [page 243]
Edit Administrator Authorizations [page 241]

1.5.11.6 Delete Corporate Identity Providers

As a tenant administrator, you can delete one or more corporate identity providers in a tenant of SAP Cloud Platform Identity Authentication service.

Prerequisites

- You are assigned the Manage Corporate Identity Providers role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
- You have at least one corporate identity provider that you want to delete.
- The identity provider you want to delete must not be used by an application. For more information about how to choose an identity provider for an application, see Authenticating Identity Provider for an Application [page 111].
Context

A Delete Identity Providers operation removes the identity providers and all of their configurations from the tenant of Identity Authentication.

Note

If you want to delete an identity provider that is in use for conditional authentication, or is set as a default identity provider for an application, edit the rules, or change the default identity provider for the application. For more information see Authenticating Identity Provider for an Application [page 111].

To delete one or more identity providers, not used not used by applications in the tenant, choose one of the following options:

Delete Multiple Corporate Identity Providers

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   Note
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Corporate Identity Providers tile.

3. Choose the icon in the left-hand panel.

   This operation activates the Delete Identity Providers mode.

4. Select the identity provider or identity providers that you want to delete.

5. Choose the Delete button.

6. Confirm the operation in the pop-up dialog.

   The system deletes only the identity providers that are not used by applications.

   Once the identity provider or identity providers have been deleted, the system displays the message <number> identity providers deleted.
Delete Single Corporate Identity Provider

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the **Corporate Identity Providers** tile.

3. Select the identity provider that you want to delete.

   **Tip**

   Type the name of the identity provider in the search field to filter the list items.

4. Choose the **Delete** button in the right-hand panel to delete the selected corporate identity provider.

5. Confirm the operation in the pop-up dialog.

   The system deletes only the identity provider that is not used by applications.

   Once the identity provider has been deleted, the system displays the message **Identity provider deleted**.

Related Information

- [Edit Administrator Authorizations] [page 241]
- [Choose Default Identity Provider for an Application] [page 112]

1.5.11.7 Forward All SSO Requests to Corporate IdP

SAP Cloud Platform Identity Authentication can be configured to forward all single sign-on (SSO) requests to the corporate identity provider.

Prerequisites

- You are assigned the **Manage Corporate Identity Providers** role. For more information about how to assign administrator roles, see [Edit Administrator Authorizations] [page 241].
You have configured Identity Authentication to use a corporate identity provider as an external authenticating authority. For more information, see Configure Trust with Corporate Identity Provider [page 256].

You have selected the configured identity provider as the authenticating identity provider for your applications. For more information, see Choose Default Identity Provider for an Application [page 112].

Context

The *Forward All SSO Requests to Corporate IdP* option allows the corporate identity provider (IdP) to process all single sign-on (SSO) requests when Identity Authentication acts as a proxy.

**Forward All SSO Requests to Corporate IdP Disabled**

By default, the *Forward All SSO Requests to Corporate IdP* option is disabled. In this case Identity Authentication reuses the active session of the user.

```
1. User tries to access Application 1.
2. Application 1 sends authentication request to Identity Authentication.
3. Identity Authentication acts as proxy; forwards the request to corporate IdP.
4. Corporate IdP logs on the user.
5. Corporate IdP returns authentication response to Identity Authentication.
1* User tries to access Application 2.
2* Application 2 sends authentication request to Identity Authentication.
3* The user has an active session. Identity Authentication reuses the session and returns the authentication response to Application 2.
```

**Forward All SSO Requests to Corporate IdP Enabled**

When *Forward All SSO Requests to Corporate IdP* option is enabled, Identity Authentication sends new authentication request for each application.

```
1. User tries to access Application 1.
2. Application 1 sends authentication request to Identity Authentication.
3. Identity Authentication acts as proxy; forwards the request to corporate IdP.
4. Corporate IdP logs on the user.
5. Corporate IdP returns authentication response to Identity Authentication.
1* User tries to access Application 2.
2* Application 2 sends authentication request to Identity Authentication.
3* The user has an active session. Identity Authentication reuses the session and returns the authentication response to Application 2.
```
1. User tries to access Application 1.

2. Application 1 sends authentication request to Identity Authentication.

3. Identity Authentication acts as proxy; forwards the request to corporate IdP.

4. Corporate IdP logs on the user.

5. Corporate IdP returns authentication response to Identity Authentication.


* User tries to access Application 2.

* Application 2 sends authentication request to Identity Authentication.

* Identity Authentication acts as proxy; it forwards the request to corporate IdP, though the user has an active session.

* Corporate IdP logs on the user.

* Corporate IdP returns new authentication response to Identity Authentication.

* Identity Authentication returns new authentication response to Application 2.

To enable the Forward All SSO Requests to Corporate IdP, follow the procedure below:

**Procedure**

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   **i Note**

   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Corporate Identity Providers tile.

3. Select the corporate identity provider that you want to configure for Forward All SSO Requests to Corporate IdP.

   ○ If you do not have an identity provider in your list, click the Add button to create one, and proceed with the configuration.
If you have an identity provider in your list, choose the one that you want to configure.

4. Use the slider next to Forward All SSO Requests to Corporate IdP to enable or disable it.

If the operation is successful, the system displays the message Identity provider <name of identity provider> updated.

1.5.11.8 Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service

Tenant administrators can configure identity federation with SAP Cloud Platform Identity Authentication service user store.

Prerequisites

- You are assigned the Manage Corporate Identity Providers role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 241].
- You have configured Identity Authentication to use a corporate identity provider as an external authenticating authority. For more information, see Configure Trust with Corporate Identity Provider [page 256].
- You have selected the configured identity provider as the authenticating identity provider for your application. For more information, see Choose Default Identity Provider for an Application [page 112].
- You have imported the users, authenticated by the corporate identity provider, in Identity Authentication. For more information about how to import users, see Import or Update Users for a Specific Application [page 196].

Context

The Identity Federation option allows the application to check if the users authenticated by the corporate identity provider exist in the Identity Authentication user store.

In the default setting, the Identity Federation option is disabled.

Remember

In scenarios when the application is using for authentication a corporate identity provider, and the Identity Federation option is disabled, the user attributes, the name ID attributes, and the default attributes configurations in the administration console for Identity Authentication are not relevant. In such scenarios, Identity Authentication sends to the application the same attributes it has received from the corporate identity provider. For more information about the corporate identity provider scenario, see Corporate Identity Providers [page 243].

If Identity Federation is enabled, only the users that are imported in Identity Authentication are able to access the application. For more information about how to enable or disable Identity Federation with Identity...
Authentication, see the **Enable Identity Federation with Identity Authentication User Store** section in this topic.

If the **Identity Federation** option is enabled, the corporate identity provider will use the SAML attribute configuration set for the service provider. To change the configuration, follow the procedure described in **Configure the Name ID Attribute Sent to the Application** [page 67].

As a next step, when **Identity Federation** is enabled, you can assign a group or groups to the corporate identity provider. Only users that are members of the assigned group can access the application. For more information about how to assign or unassign user groups to corporate identity providers, see the **Assign User Groups to Corporate Identity Providers** section in this topic.

---

**Enable Identity Federation with SAP Cloud Platform Identity Authentication Service User Store**

**Procedure**

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   **i Note**

   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

   The **Tenant ID** is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the **tenant ID**.

2. Choose the **Corporate Identity Providers** tile.

3. Select the corporate identity provider that you want to configure for **Identity Federation**.
   - If you do not have an identity provider in your list, click the **Add** button to create one, and proceed with the configuration.
   - If you have an identity provider in your list, choose the one that you want to configure.

4. Use the slider next to **Identity Federation** to enable or disable it.

   If the operation is successful, the system displays the message **Identity provider <name of identity provider> updated.**

---

**Assign User Groups to Corporate Identity Providers**

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
2. Choose the **Corporate Identity Providers** tile.
3. Select the corporate identity provider that you want to configure.
   - If you do not have an identity provider in your list, choose the **Add** button to create one, and proceed with the configuration.
   - If you have an identity provider in your list, choose the one that you want to edit.

   **Tip**
   Type the name of the identity provider in the search field to filter the list items.

4. Choose **Identity Federation**.
   You will see a list of the user groups assigned to this corporate identity provider. If no groups are assigned, the list will be empty.
5. Choose the **Assign Groups** button.
6. Select the groups that you want to assign to this corporate identity provider.
   The list does not include the groups that are already assigned to the corporate identity provider.
   If you do not have any user groups in your list, you can create one. For more details about how to create user groups and assign the group to a user, see Related Information.
7. Save your changes.

   If the operation is successful, the system displays the message **Identity provider <name of identity provider> updated**.

   **i Note**
   To unassign user groups, select the groups you want to unassign, choose the **Unassign Groups** button, and confirm the operation in the dialog.

   Users that belong only to the unassigned groups will not be able to access the application any more.

### Related Information

- [Create a New User Group](#)
- [Assign Groups to a User](#)

### 1.5.12 Social Identity Providers

Configure Social Identity Providers [page 269]
By configuring a social provider, users can log on to applications with their social media credentials by liking their accounts in Identity Authentication to the social media account.

Remove Social Identity Providers Configuration [page 272]

You can remove the configurations of the social providers in the administration of SAP Cloud Platform Identity Authentication service.

1.5.12.1 Configure Social Identity Providers

By configuring a social provider, users can log on to applications with their social media credentials by liking their accounts in Identity Authentication to the social media account.

Context

Identity Authentication uses the OAuth protocol for social sign-on via one of the following predefined social providers:

- Twitter
- Facebook
- LinkedIn
- Google

Once a user has allowed Identity Authentication to link his or her account with the social provider accounts, the user can log on to applications via the social providers.

To configure social identity provider for the tenant, you have to register new applications on the corresponding social network sites. For more details, see Related Information.

**i Note**

You need to type `<https://<tenant ID>.accounts.ondemand.com/ui/oauth/googleCallback>` in the **Authorized redirect URIs** field when you create your client ID in Google Developers Console. For more information about the redirect URIs for your OAuth 2.0 credentials, see Set a redirect URI.

**i Note**

You need to type `<https://<tenant ID>.accounts.ondemand.com/ui/oauth/oauthCallback>` in the **Valid OAuth redirect URIs** field in the Settings section of Facebook Login in the App Dashboard. For more information about Facebook Valid OAuth redirect URIs, see Enable Strict Mode.

**i Note**

You need to type `<https://<tenant ID>.accounts.ondemand.com/ui/oauth/oauthCallback>` in the **Callback URLs** field in the Create an application section of Twitter Application Management page. For more information about Twitter Callback URL, see Callback URL.
To perform the social identity provider configuration in the administration console for Identity Authentication, you have to provide the following data:

**Required Google Settings**

<table>
<thead>
<tr>
<th>Authentication Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google’s client ID</td>
<td>The Google OAuth 2.0 credential after you set a project in the Google Developers Console.</td>
</tr>
<tr>
<td>Google’s client secret</td>
<td>The Google OAuth 2.0 credential after you set a project in the Google Developers Console.</td>
</tr>
</tbody>
</table>

**Required Facebook Settings**

<table>
<thead>
<tr>
<th>Authentication Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook’s application ID</td>
<td>The ID generated after you add an application on Facebook.</td>
</tr>
<tr>
<td>Facebook’s application secret</td>
<td>The secret generated after you add an application on Facebook.</td>
</tr>
</tbody>
</table>

**Required LinkedIn Settings**

<table>
<thead>
<tr>
<th>Authentication Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinkedIn’s Client ID (API key)</td>
<td>The key generated by LinkedIn to identify a user application and for API calls.</td>
</tr>
<tr>
<td>LinkedIn’s Client Secret (API secret)</td>
<td>The secret generated by LinkedIn to identify a user application and for API calls.</td>
</tr>
</tbody>
</table>

**Required Twitter Settings**

<table>
<thead>
<tr>
<th>Authentication Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Twitter’s consumer key</td>
<td>The key generated by Twitter to identify which user application is making the request.</td>
</tr>
<tr>
<td>Twitter’s consumer secret</td>
<td>The secret generated by Twitter to identify which user application is making the request.</td>
</tr>
</tbody>
</table>

**Procedure**

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern. *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*. 
2. Choose the **Social Identity Providers** tile.
   
   This operation opens a list of the social providers.

3. Choose the list item of the social provider that you want to configure.


5. Enter the generated authentication attributes from the social provider.

   **i Note**
   
   Check for leading or trailing spaces in the authentication attributes fields, and delete them. Sign-on through the social identity provider will not work if there are blank spaces before or after the strings in the fields.

6. Save your configuration.

   If the operation is successful, you will receive the following message: `<Social Provider Name> updated`. The slider next to the social provider is switched to **ON**.

   **i Note**
   
   If you do not want to use any of the social providers for logon you can drag the slider next to the social provider to **OFF**. The configuration for this social provider will be preserved, but the social provider will not appear on the logon pages of the applications in the tenant. If you want to remove the configuration for a given social provider, see Related Information for more details.

**Next Steps**

The above configurations are valid for the whole tenant. They will take effect for a specific application if you enable the **Social Sign-On** option via the administration console. For more information about how to enable social sign on for a specific application, see Enable or Disable Social Sign-On for an Application [page 76].

**Task overview:** Social Identity Providers [page 268]

**Related Information**

- Remove Social Identity Providers Configuration [page 272]
- Obtain OAuth 2.0 credentials
- Verify your site ownership
- Facebook Login
- Authentication with OAuth 2.0
- Authorizing a request
- Enable or Disable Social Sign-On for an Application [page 76]
- Remove Social Identity Providers Configuration [page 272]
1.5.12.2 Remove Social Identity Providers Configuration

You can remove the configurations of the social providers in the administration of SAP Cloud Platform Identity Authentication service.

Prerequisites

You have a configured social provider in the administration console for Identity Authentication

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern. Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Social Identity Providers tile.
   This operation opens a list of the social providers.
3. Choose the list item of the social provider whose configuration you want to remove.
5. Choose the Remove Configuration button.
6. Confirm your choice.

Results

The configuration for the selected social provider will be removed. The social provider will not appear on the logon pages of the applications in the tenant.

Task overview: Social Identity Providers [page 268]
1.5.13 Monitoring and Reporting

View Usage Statistics [page 273]
You can view statistical information for a tenant in the administration console for SAP Cloud Platform Identity Authentication service.

Access Audit Logs [page 274]
You can access the audit logs for changes in the personal data, successful, and failed authentications, in SAP Cloud Platform Identity Authentication service.

Export Change Logs with a History of Administration Operations [page 277]
You can download a CSV file with a history of the operations performed by administrators in the administration console for SAP Cloud Platform Identity Authentication service.

1.5.13.1 View Usage Statistics

You can view statistical information for a tenant in the administration console for SAP Cloud Platform Identity Authentication service.

Context

The Reporting view displays a chart of statistical information with the number of the user logon requests per month in the tenant.

A logon request is a single authentication request managed via Identity Authentication. Identity Authentication counts only one logon request per user per day. Logon requests are independent of the authentication mechanism and user type.

The statistical information begins with the month when the first logon request is registered, and continues to the current month.

Note

If you need statistics for the period before August 2015 you can report an incident on SAP Support Portal Home with a component BC-IAM-IDS.

Currently the statistics do not include the logon requests when Identity Authentication acts as a proxy to delegate authentication to an external corporate identity provider.
**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the *Reporting* tile.

**1.5.13.2 Access Audit Logs**

You can access the audit logs for changes in the personal data, successful, and failed authentications, in SAP Cloud Platform Identity Authentication service.

**Context**

To view the audit logs you should generate Client ID and Client Secret for audit logs in the administration console for Identity Authentication first. After that you should obtain an access token, and then call the audit log retrieval API to access the data.

To access the audit logs, follow the procedures below:

**1. Generate Client Credentials for Audit Logs**

**Context**

The Client ID and Client Secret for the current tenant are generated in the administration console for Identity Authentication.

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **Note**
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Logs tile.
This operation opens the Logs page.

3. Under Generate Client Credentials for Audit Logs choose the Generate button.
A dialog box with the generated Client ID and Client Secret appears.

→ Remember
Make sure that you copy the Client Secret from the dialog box. When you choose OK, the dialog box closes, and you cannot retrieve the Client Secret from the system anymore.

Results

The generated Client ID can be seen under Generate Client Credentials for Audit Logs in the Logs page.

→ Tip
To delete the client credentials, choose the icon next to the generated Client ID. This deletes the Client ID and Client Secret from the system.

2. Obtain an Access Token

Context

Use the Client ID and Client Secret generated for the current tenant in the administration console for Identity Authentication to obtain an access token. For more information about how to obtain the access token see 2. Get an OAuth Access Token in Using Platform APIs.

→ Tip
The URL for the POST request looks like this: https://api.<SAP Cloud Platform host>/oauth2/apitoken/v1?grant_type=client_credentials

Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

For tenants in Europe, you should use eu1.hana.ondemand.com for the SAP Cloud Platform host in the request.

For tenants in United States (US East), you should use us3.hana.ondemand.com for the SAP Cloud Platform host in the request.
3. Call the Audit Log Retrieval API

Context

To access the audit logs you should call the audit log retrieval API. You need the Client ID and Client Secret for the current tenant, generated in the administration console for Identity Authentication, and the access token. For more information, see Audit Log Retrieval API Usage.

You can filter the audit logs by time and/or categories. The categories that you can filter are:

- audit.authentication - audit logs related to authentication (failed, successful, type)
- audit.data-change - audit logs related to changes in personal data

Remember

The URI for the GET request looks like this: https://api.<SAP Cloud Platform host>/auditlog/v1/accounts/<Tenant ID>/AuditLogRecordsIds?$filter=(Time ge '2018-05-17T13.00.00' and Time le '2018-05-18T05.00.00')and Category eq '<category>'

Use that URI in the examples in Audit Log Retrieval API Usage.

Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

For tenants in Europe, you should use eu1.hana.ondemand.com for the SAP Cloud Platform host in the request.

For tenants in United States (US East), you should use us3.hana.ondemand.com for the SAP Cloud Platform host in the request.

For tenants in Russia (Moscow), you should use ru1.hana.ondemand.com for the SAP Cloud Platform host in the request.

For tenants in Australia (Sydney), you should use ap1.hana.ondemand.com for the SAP Cloud Platform host in the request.

For more information, see Region Availability [page 8] and Regions.
1.5.13.3 Export Change Logs with a History of Administration Operations

You can download a CSV file with a history of the operations performed by administrators in the administration console for SAP Cloud Platform Identity Authentication service.

**Context**

The exported change logs are saved in a CSV file and contain information about `CREATE`, `UPDATE`, or `DELETE` operations performed by administrators.

The change log entries are not deleted from the system. Each record should contain the following data:

- **Date**
  The date when the resource was created, updated, or deleted.
- **Administrator's ID**
  The ID of the user or the system that made the change.
- **Administrator's Name**
  The name of the user or the system that made the change.
- **Resource Type**
  This indicates which type of resource was created, updated, or deleted, for example service provider.
- **Resource ID**
  An identifier for the resource.
- **Resource Name**
  The name of the resource that was created, updated, or deleted.
- **Action**
  - `CREATE`  
    The log shows the value of the attribute when the resource was created.
  - `UPDATE`  
    The log shows the changed value of the attribute when the resource was updated.
  - `DELETE`  
    The log shows which resource was deleted.
- **Attribute**
  The attribute of the resource that was created or updated with the relevant operation.
- **Value**
  The new value of the attribute.

**Note**
There are attributes whose values cannot be displayed in the logs. In such cases the value fields are left blank.

**Example**

The table shows change logs for the following operations:

1. A tenant administrator, Donna Moore, creates a Company A application.
2. The tenant administrator uploads service provider metadata for the SAML 2.0 trust.
3. The tenant administrator creates custom Company A terms of use by uploading a plain text file.
4. The tenant administrator creates a custom Company A privacy policy by uploading a plain text file.
5. The tenant administrator allows user self-registration for an application of the configured service provider as she uses the default e-mail template for the self-registration process.
6. The tenant administrator configures a branding style for the application.
7. The tenant administrator sets SAP Community Password Policy v.1.1 for the application.
8. The tenant administrator sets Company A Terms of Use for the application.
9. The tenant administrator sets Company A Privacy Policy for the application.

Sample Change Logs Data

<table>
<thead>
<tr>
<th>Date</th>
<th>Administrator’s ID</th>
<th>Administrator’s Name</th>
<th>Resource Type</th>
<th>Resource ID</th>
<th>Resource Name</th>
<th>Action</th>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>16-05-2014</td>
<td>P12345</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e 4b0f3cb1 a01700</td>
<td>sp.example.com</td>
<td>UPDATE</td>
<td>Privacy Policy</td>
<td>Company A Privacy Policy</td>
</tr>
<tr>
<td>16-05-2014</td>
<td>P12345</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e 4b0f3cb1 a01700</td>
<td>sp.example.com</td>
<td>UPDATE</td>
<td>Terms of Use</td>
<td>Company A Terms of Use</td>
</tr>
<tr>
<td>16-05-2014</td>
<td>P12345</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e 4b0f3cb1 a01700</td>
<td>sp.example.com</td>
<td>UPDATE</td>
<td>Password Policy</td>
<td><a href="https://accounts.sap.com/policy/passwords/sap/web/1.1">https://accounts.sap.com/policy/passwords/sap/web/1.1</a></td>
</tr>
<tr>
<td>16-05-2014</td>
<td>P12345</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e 4b0f3cb1 a01700</td>
<td>sp.example.com</td>
<td>UPDATE</td>
<td>Branding Style</td>
<td>Text Color=#ffffff, Background Top Color=#E3 E3E3, Border Color=#7B 9EB3, show_header=false, Background Bottom Color=#E3 E3E3</td>
</tr>
<tr>
<td>16-05-2014</td>
<td>P12345</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e 4b0f3cb1 a01700</td>
<td>sp.example.com</td>
<td>UPDATE</td>
<td>Branding Type</td>
<td>Custom Theme</td>
</tr>
<tr>
<td>16-05-2014</td>
<td>P12345</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e 4b0f3cb1 a01700</td>
<td>sp.example.com</td>
<td>UPDATE</td>
<td>Self-Registration</td>
<td>Allowed</td>
</tr>
<tr>
<td>Date</td>
<td>Administrator's ID</td>
<td>Administrator's Name</td>
<td>Resource Type</td>
<td>Resource ID</td>
<td>Resource Name</td>
<td>Action</td>
<td>Attribute</td>
<td>Value</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------</td>
<td>----------------------</td>
<td>---------------</td>
<td>----------------------</td>
<td>----------------------------------------</td>
<td>-------------</td>
<td>-----------</td>
<td>------------------------</td>
</tr>
<tr>
<td>16-05-2014</td>
<td>P12345</td>
<td>Donna Moore</td>
<td>Terms of Use Document</td>
<td>53da05f9e 4b0732235 f24b8a</td>
<td>English Version of Company A Terms of Use</td>
<td>CREATE</td>
<td>Display Name Company A Privacy Policy</td>
<td></td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P12345</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e 4b0f3c8a1 01f700</td>
<td>Company A Service Provider</td>
<td>UPDATE</td>
<td>SAML 2.0 Provider Name company_a_service_provider</td>
<td></td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P12345</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e 4b0f3c8a1 01f700</td>
<td>Company A Service Provider</td>
<td>UPDATE</td>
<td>Authentication Authority company_a_tenant_id</td>
<td></td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P12345</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e 4b0f3c8a1 01f700</td>
<td>Company A Service Provider</td>
<td>UPDATE</td>
<td>Assertion Consumer Service Endpoint service_provider_acs_endpoint, HTTP-POST</td>
<td></td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P12345</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e 4b0f3c8a1 01f700</td>
<td>Company A Service Provider</td>
<td>UPDATE</td>
<td>Single Logout Endpoint service_provider_slo_endpoint, HTTP-POST</td>
<td></td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P12345</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e 4b0f3c8a1 01f700</td>
<td>Company A Service Provider</td>
<td>UPDATE</td>
<td>Single Logout Endpoint service_provider_slo_endpoint, HTTP-Redirect</td>
<td></td>
</tr>
<tr>
<td>Date</td>
<td>Adminstrator’s ID</td>
<td>Adminstrator’s Name</td>
<td>Resource Type</td>
<td>Resource ID</td>
<td>Action</td>
<td>Attribute</td>
<td>Value</td>
<td></td>
</tr>
<tr>
<td>------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>----------------</td>
<td>----------------------------</td>
<td>------------</td>
<td>-----------</td>
<td>-----------------</td>
<td></td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>CREATE</td>
<td>Name ID</td>
<td>User ID</td>
<td></td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>CREATE</td>
<td>Default Name ID Format</td>
<td>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</td>
<td></td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>CREATE</td>
<td>Self-Registration</td>
<td>Inherit</td>
<td></td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>CREATE</td>
<td>Certificate</td>
<td>CN=sp.example.com</td>
<td></td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>CREATE</td>
<td>Assertion Consumer Service Endpoint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>CREATE</td>
<td>Single Log-out Endpoint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>CREATE</td>
<td>User Attribute</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>CREATE</td>
<td>Constant Attribute</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
To download a CSV file with change logs information, proceed as follows:

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **i Note**
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Logs tile.

   This operation opens the Logs page.

3. Under Export Change Logs choose the Export button.

**Results**

You have downloaded a CSV file containing history of operations for the tenant administration, and for the configurations of identity providers and service providers.

**Related Information**

[Troubleshooting for Administrators](page 298)

**1.5.14 Export Existing Users of a Tenant of SAP Cloud Platform Identity Authentication Service**

**Prerequisites**

You are assigned the Manage Users role. For more information about how to assign administrator roles, see [Edit Administrator Authorizations](page 241).
You can download a CSV file containing information of up to 10,000 tenant users in SAP Cloud Platform Identity Authentication service including the tenant administrators. The CSV file contains the following columns: \textit{status}, \textit{loginName}, \textit{mail}, \textit{firstName}, and \textit{lastName}. If the status of a user is inactive, he or she cannot perform any operations on the tenant.

\begin{tabular}{lccccc}
\textbf{status} & \textbf{loginName} & \textbf{mail} & \textbf{firstName} & \textbf{lastName} \\
\hline
active & EID00001 & michael.adams@example.com & Michael & Adams \\
active & EID00002 & julie.armstrong@example.com & Julie & Armstrong \\
active & EID00003 & donna.moore@example.com & Donna & Moore \\
active & EID00004 & john.miller@example.com & John & Miller \\
active & EID00005 & denise.smith@example.com & Denise & Smith \\
inactive & EID00006 & richard.wilson@example.com & Richard & Wilson \\
\end{tabular}

All users but one can log on to tenant applications. Richard Wilson cannot log on because his user is not active.

To export tenant users from Identity Authentication, proceed as follows:

\textbf{Procedure}

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   \textit{i Note}

   The URL has the \texttt{https://<tenant ID>.accounts.ondemand.com/admin} pattern.

   \textit{Tenant ID} is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the \textit{tenant ID}.

2. Choose the \textit{Export Users} tile.

   This operation opens the \textit{Export Users} page.

3. Choose the \textit{Export} button.
1.5.15 SAML 2.0

The Security Assertion Markup Language (SAML) version 2.0 is a standard for the communication of assertions about principals, typically users. The assertion can include the means by which a subject was authenticated, attributes associated with the subject, and an authorization decision for a given resource.

The two main components of a SAML 2.0 landscape are an identity provider and a service provider. The service provider is a system entity that provide a set of Web applications with a common session management, identity management, and trust management. The identity provider is a system entity that manages identity information for principals and provides authentication services to other trusted service providers. In other words, the service providers outsource the job of authenticating the user to the identity provider. The identity provider maintains the list of service providers where the user is logged in and passes on logout requests to those service providers.

1.5.16 OpenID Connect

You can use SAP Cloud Platform Identity Authentication service to authenticate users in OpenID Connect protected applications.

OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol. Clients can verify the identity of the end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner. For more information about the OpenID Connect specification, see OpenID Connect Core 1.0.

The OpenID Connect implementation of Identity Authentication supports the authorization code flow and resource owner credential flow. For more information, see 3.1. Authentication using the Authorization Code Flow, and 1.3.3. Resource Owner Password Credentials.
Based on your scenario, choose one of the supported flows to see how to authorize access to your application:

- Using Authorization Code Flow [page 284]
- Using Resource Owner Credential Flow [page 292]

### 1.5.16.1 Using Authorization Code Flow

To authenticate using the authorization code flow, follow the procedures below. Tasks 1 and 2 are configuration on SAP Cloud Platform Identity Authentication service side. Tasks 3 and 4 are configurations, done on the client (relying party) side.

1. **Create OpenID Connect Application for Authentication Code Flow [page 285]**
   Create a new OpenID Connect application for authentication code flow.

2. **Configure OpenID Connect Application for Authorization Code Flow [page 286]**
   This document is intended to help you configure an OpenID Connect application in the administration console for SAP Cloud Platform Identity Authentication service for the authorization code flow.

3. **Configure the Client To Call Identity Authentication Authorize Endpoint [page 288]**
   The authorize endpoint is used for authentication and returns authorization code.

4. **Configure the Client To Call Identity Authentication Token Endpoint for Authorization Code Flow [page 290]**
   The token endpoint is used to get the user’s access token, and returns an id token in the form of a JSON Web Token (JWT).

**Related Information**

OpenID Connect [page 283]
1.5.16.1.1 Create OpenID Connect Application for Authentication Code Flow

Create a new OpenID Connect application for authentication code flow.

Context

To create a new OpenID Connect application follow the procedure below:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

3. Choose the +Add button on the left-hand panel to add a new application to the list.

   i Note
   The display name of the application is displayed on the logon and registration pages.

   Once the application has been created, the system displays the message Application <name of application> created.

   The newly created application appears on the list with the applications on the left. It is selected and you can set its type to OpenID Connect.

4. Choose Trust > SINGLE SIGN-ON > Type

   △ Caution
   Make sure that the application you want to configure as OpenID connect is selected on the left.

5. Select OpenID Connect.

6. Save your selection.

   The system displays the message Application <name of application> updated.

   i Note
   (Optional) If necessary, configure additional settings for the application. For more information about the supported configurations for the OpenID Connect applications, see the following links:

Next task: Configure OpenID Connect Application for Authorization Code Flow [page 286]

Related Information

OpenID Connect [page 283]

1.5.16.1.2 Configure OpenID Connect Application for Authorization Code Flow

This document is intended to help you configure an OpenID Connect application in the administration console for SAP Cloud Platform Identity Authentication service for the authorization code flow.

Prerequisites

You have an OpenID Connect application in the administration console for Identity Authentication. For more information, see Create OpenID Connect Application [page 45].
Context

The trust is configured by entering the information manually. You can enter manually the name of the client (relying party), and its redirect URIs.

i Note

The steps are one and the same, both for the authorization code flow and the resource owner credential flow.

To configure an OpenID Connect trusted application in the administration console for SAP Cloud Platform Identity Authentication service proceed as follows:

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   i Note
   
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.

   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.

5. Under SINGLE SIGN-ON, choose OpenID Connect Configuration.

6. Manually enter the communication settings negotiated between Identity Authentication and the client.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The issuer in the OpenID Provider metadata.</td>
</tr>
<tr>
<td>Redirect URI</td>
<td>The redirection URI to which the response will be sent. You can add up to five redirect URIs.</td>
</tr>
</tbody>
</table>

7. Save your selection. Once the application has been changed, the system displays the message Application <name of application> updated.
Remember

Configure trust on the client side. See the client documentation for more information about how to configure the trust. For more information how to view the OpenID Connect settings of Identity Authentication, see Tenant OpenID Connect Configuration [page 132].

Next Steps

- Configure HTTP basic authentication for the application. For more information about the configuration, see Configure Credentials for HTTP Basic Authentication [page 79].


Previous task: Create OpenID Connect Application for Authentication Code Flow [page 285]

Next: Configure the Client To Call Identity Authentication Authorize Endpoint [page 288]

Related Information

OpenID Connect [page 283]

1.5.16.1.3 Configure the Client To Call Identity Authentication Authorize Endpoint

The authorize endpoint is used for authentication and returns authorization code.

This document explains how to call the authorize endpoint and what are the authorize request parameters supported by Identity Authentication.

Request

URI: https://<tenant ID>.accounts.ondemand.com/oauth2/authorize

HTTP Method: GET
Request Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Data Type</th>
<th>Additional Information</th>
<th>Parameter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>redirect_uri</td>
<td>Yes</td>
<td>string</td>
<td>One of the valid URIs configured for the application. You can configure up to five URIs. For more information, see Configure OpenID Connect Application [page 59].</td>
<td>Path</td>
</tr>
<tr>
<td>response_type</td>
<td>Yes</td>
<td>string</td>
<td>The supported value is code</td>
<td>Path</td>
</tr>
<tr>
<td>scope</td>
<td>Yes</td>
<td>string</td>
<td>The supported value is openid</td>
<td>Path</td>
</tr>
<tr>
<td>client_id</td>
<td>Yes</td>
<td>string</td>
<td>The user ID configured for basic authentication for the application. For more information, see Configure Credentials for HTTP Basic Authentication [page 79].</td>
<td>Path</td>
</tr>
<tr>
<td>state</td>
<td>Yes</td>
<td>string</td>
<td>Free text</td>
<td>Path</td>
</tr>
</tbody>
</table>

Request Example


Response

Response Headers

<table>
<thead>
<tr>
<th>Header</th>
<th>Description</th>
<th>i Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>code</td>
<td>The code is generated by Identity Authentication and is returned in the URL as a parameter. It must be used when making a call to the token endpoint.</td>
<td>The parameter can be used within two minutes after it is generated and returned in the URL. It can be used only once.</td>
</tr>
</tbody>
</table>

Response Status and Error Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
</table>
| 302     | Found        | Successful operation. Additionally provides a URL in the header field Location. | i Note
|         |              | The URL contains code necessary for the token endpoint.                     |
### Response Example

| Location: | https://www.example.com/?code=4454554df477w01s34540672dc462e6f0&state=state |

**Parent topic:** Using Authorization Code Flow [page 284]

**Previous task:** Configure OpenID Connect Application for Authorization Code Flow [page 286]

**Next:** Configure the Client To Call Identity Authentication Token Endpoint for Authorization Code Flow [page 290]

### Related Information

OpenID Connect [page 283]

### 1.5.16.1.4 Configure the Client To Call Identity Authentication Token Endpoint for Authorization Code Flow

The token endpoint is used to get the user’s access token, and returns an id token in the form of a JSON Web Token (JWT).

This document explains how to call the token endpoint and what are the parameters supported by Identity Authentication.

#### Request

**URI:** https://<tenant ID>.accounts.ondemand.com/oauth2/token

**HTTP Method:** POST

**Request Headers**

<table>
<thead>
<tr>
<th>Header</th>
<th>Required</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td>application/x-www-form-urlencoded</td>
</tr>
</tbody>
</table>
### Request Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Data Type</th>
<th>Description</th>
<th>Parameter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>grant_type</td>
<td>Yes</td>
<td>string</td>
<td>authorization_code</td>
<td>Request body</td>
</tr>
<tr>
<td>code</td>
<td>Yes</td>
<td>string</td>
<td>The code generated by Identity Authentication in the authorize endpoint. It is returned with the request to the authorize endpoint.</td>
<td>Request body</td>
</tr>
<tr>
<td>redirect_uri</td>
<td>Yes</td>
<td>string</td>
<td>The same URL that has been sent with the authorization request. For more information, see Configure OpenID Connect Application [page 59].</td>
<td>Request body</td>
</tr>
<tr>
<td>client_id</td>
<td>Yes</td>
<td>string</td>
<td>The user ID configured for basic authentication for the application. For more information, see Configure Credentials for HTTP Basic Authentication [page 79].</td>
<td>Request body</td>
</tr>
</tbody>
</table>

**Note**

The `code` parameter can be used within two minutes after it is generated and returned in the URL. It can be used only once.

### Request Example

```
grant_type=authorization_code&client_id=T123456&code=768fsd1206we951236729134fa4a247ee&redirect_uri=https://www.example.com
```

### Response

### Response Status and Error Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>Successful operation.</td>
<td>Returns access_token and id_token.</td>
</tr>
</tbody>
</table>

**Note**

The `id_token` is generated by Identity Authentication. It is in the form of a JWT (JSON Web Token) and contains information about the user.

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>400 Bad Request</td>
<td>Missing or wrong parameter.</td>
</tr>
</tbody>
</table>
To get access using the resource owner credential flow, follow the procedures below. Tasks 1 and 2 are configuration on SAP Cloud Platform Identity Authentication service side. Task 3 is configuration, done on the client (relying party) side.

1. **Create OpenID Connect Application for Resource Owner Credential Flow** [page 293]
   You can create a new OpenID Connect application.

2. **Configure OpenID Connect Application for Resource Owner Credential Flow** [page 294]
   This document is intended to help you configure an OpenID Connect application in the administration console for SAP Cloud Platform Identity Authentication service for the resource owner credential flow.

3. **Configure the Client To Call Identity Authentication Token Endpoint for Resource Owner Credential Flow** [page 296]
   The token endpoint is used to get the user’s access token, and returns an id token in the form of a JSON Web Token (JWT).

**Related Information**

OpenID Connect [page 283]
1.5.16.2.1 Create OpenID Connect Application for Resource Owner Credential Flow

You can create a new OpenID Connect application.

Context

To create a new OpenID Connect application you have to add a new application to the list of applications in SAP Cloud Platform Identity Authentication service, and then set the type of application to OpenID Connect.

To create a new OpenID Connect application, choose your scenario and follow the procedure there.

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
   
<table>
<thead>
<tr>
<th>i Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The URL has the <code>https://&lt;tenant ID&gt;.accounts.ondemand.com/admin</code> pattern.</td>
</tr>
<tr>
<td>Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.</td>
</tr>
</tbody>
</table>

2. Choose the Applications tile.
3. Choose the +Add button on the left-hand panel to add a new application to the list.
   
<table>
<thead>
<tr>
<th>i Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>The display name of the application is displayed on the logon and registration pages.</td>
</tr>
</tbody>
</table>

   Once the application has been created, the system displays the message Application `<name of application>` created.

   The newly created application appears on the list with the applications on the left. It is selected and you can set its type to OpenID Connect.

4. Choose Trust > SINGLE SIGN-ON > Type
   
<table>
<thead>
<tr>
<th>△ Caution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make sure that the application you want to configure as OpenID connect is selected on the left.</td>
</tr>
</tbody>
</table>

5. Select OpenID Connect.
6. Save your selection.
   
   The system displays the message Application `<name of application>` updated.
i Note
(Optional) If necessary, configure additional settings for the application. For more information about the supported configurations for the OpenID Connect applications, see the following links:
- Configure the User Attributes Sent to the Application [page 64]
- Configure the Default Attributes Sent to the Application [page 71]
- Configure Credentials for HTTP Basic Authentication [page 79]
- Configure a Certificate for API Authentication [page 80]
- Configure Risk-Based Authentication [page 82]
- Configure User Access to the Application [page 87]
- Enable E-Mail Verification [page 89]
- Configuring Password Policies [page 166]

Task overview: Using Resource Owner Credential Flow [page 292]

Next task: Configure OpenID Connect Application for Resource Owner Credential Flow [page 294]

Related Information

OpenID Connect [page 283]

1.5.16.2.2 Configure OpenID Connect Application for Resource Owner Credential Flow

This document is intended to help you configure an OpenID Connect application in the administration console for SAP Cloud Platform Identity Authentication service for the resource owner credential flow.

Prerequisites

You have an OpenID Connect application in the administration console for Identity Authentication. For more information, see Create OpenID Connect Application [page 45].

Context

The trust is configured by entering the information manually. You can enter manually the name of the client (relying party), and its redirect URIs.
To configure an OpenID Connect trusted application in the administration console for SAP Cloud Platform Identity Authentication service proceed as follows:

**Procedure**

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
   
   **Note**
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   
   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the Applications tile.
   
   This operation opens a list of the applications.

3. Choose the application that you want to edit.
   
   **Note**
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
   
   If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.

5. Under **SINGLE SIGN-ON**, choose **OpenID Connect Configuration**.

6. Manually enter the communication settings negotiated between Identity Authentication and the client.

   **Setting** | **Description**
   --- | ---
   **Name** | The issuer in the OpenID Provider metadata.
   **Redirect URI** | The redirection URI to which the response will be sent. You can add up to five redirect URIs.
   
   **Note**
   The *Redirect URI* configuration is not mandatory for the Resource Owner Credential Flow and can be skipped.

7. Save your selection. Once the application has been changed, the system displays the message `Application <name of application> updated`. 
→ Remember

Configure trust on the client side. See the client documentation for more information about how to configure the trust. For more information how to view the OpenID Connect settings of Identity Authentication, see Tenant OpenID Connect Configuration [page 132].

Next Steps

- Configure HTTP basic authentication for the application. For more information about the configuration, see Configure Credentials for HTTP Basic Authentication [page 79].

Task overview: Using Resource Owner Credential Flow [page 292]

Previous task: Create OpenID Connect Application for Resource Owner Credential Flow [page 293]

Next: Configure the Client To Call Identity Authentication Token Endpoint for Resource Owner Credential Flow [page 296]

Related Information

OpenID Connect [page 283]

1.5.16.2.3 Configure the Client To Call Identity Authentication Token Endpoint for Resource Owner Credential Flow

The token endpoint is used to get the user’s access token, and returns an id token in the form of a JSON Web Token (JWT).

This document explains how to call the token endpoint and what are the parameters supported by Identity Authentication.

Request

URI: https://<tenant ID>.accounts.ondemand.com/oauth2/token

HTTP Method: POST
**Request Headers**

<table>
<thead>
<tr>
<th>Header</th>
<th>Required</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td>application/x-www-form-urlencoded</td>
</tr>
<tr>
<td>Basic Authentication</td>
<td>Yes</td>
<td>User ID and a password to authenticate the client (relying party). For more information, see Configure Credentials for HTTP Basic Authentication [page 79].</td>
</tr>
</tbody>
</table>

**Request Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Data Type</th>
<th>Additional Information</th>
<th>Parameter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>grant_type</td>
<td>Yes</td>
<td>string</td>
<td>The supported value is password</td>
<td>Request body</td>
</tr>
<tr>
<td>username</td>
<td>Yes</td>
<td>string</td>
<td>The user identifier.</td>
<td>Request body</td>
</tr>
<tr>
<td>password</td>
<td>Yes</td>
<td>string</td>
<td>The user password.</td>
<td>Request body</td>
</tr>
<tr>
<td>otpcode</td>
<td>No</td>
<td>string</td>
<td>The one-time password (OTP) generated by the user’s registered device.</td>
<td>Request body</td>
</tr>
</tbody>
</table>

**Request Example**

grant_type=password&username=<user identifier>&password=<user password>

**Response**

**Response Status and Error Codes**

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>Successful operation.</td>
<td>Returns access_token and id_token.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>i Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The id_token is generated by Identity Authentication. It is in the form of a JWT (JSON Web Token) and contains information about the user.</td>
</tr>
<tr>
<td>400 Bad Request</td>
<td>Missing or wrong parameter.</td>
<td>Returns an information about the error.</td>
</tr>
</tbody>
</table>
## 1.5.17 Troubleshooting for Administrators

This section is intended to help administrators deal with error messages in the administration console for SAP Cloud Platform Identity Authentication service.

### Solutions to Error Messages

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>This field is required</td>
<td>This field is empty.</td>
<td>You must enter at least one non-space character.</td>
</tr>
</tbody>
</table>
| Internal error; contact system administrator | Unexpected error occurred. | • Try again.  
• Check the browser logs.  
• Contact an operator of Identity Authentication. |
<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
</table>
| The provided file is of wrong type; specify a different file | You have specified a wrong file format. | You should use the following files:  
  - For service provider metadata, use XML.  
  - For privacy policy and terms of use documents, use plain text files.  
  - For certificate for API authentication, use base64-encoded certificate. |
| The imported CSV file contains entries with a duplicate email <email address>. The values under mail column must be unique. | You have provided a CSV file with a mail column that has the same e-mail entries. | Correct the file so that the mail column contains unique values. |
| The imported CSV file contains entries with a duplicate login name <login name>. The values under loginName column must be unique. | You have provided a CSV file with a loginName column that has the same entries. | Correct the file so that the loginName column contains unique values. |
| First <number> users are imported. User import has been interrupted due to an invalid entity. ... | The first <number> users in the CSV file are already imported for the tenant. The next user was not imported because the CSV file contains an incorrect data for that user. | Delete the first <number> users from the CSV file, correct the invalid row, and re-import the updated file. |
| First <number> users are imported. User import has been interrupted due to multiple users in the database with the same email address <email address>. The email address must be unique for each user. | The first <number> users in the CSV file are already imported for the tenant. The next user was not imported because its e-mail matches with the e-mail of other users. |  
  - Correct the user data, delete the first <number> users from the CSV file, and re-import the updated file.  
  - Contact an operator of Identity Authentication to check if your emails exist in the database. |
<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>First &lt;number&gt; users are imported. User import has been interrupted for user with email address &lt;email address&gt;.&lt;br&gt;...</td>
<td>The first &lt;number&gt; users in the CSV file are already imported for the tenant. The next user was not imported because its data in the CSV file conflicts with the data in the database.</td>
<td>- Correct the e-mail for the logon name under the mail column, delete the first &lt;number&gt; users from the CSV file, and re-import the updated file.</td>
</tr>
<tr>
<td>Your e-mail activation link is invalid. The link that the user has followed has expired or has already been used.</td>
<td>- The user should visit the application choose Log On follow Forgot Password link. This will trigger the Forgot Password process and the user will receive an e-mail to reset his or her password. - Delete the user and create it again. - Valid for the User Import scenario. If the user was imported via a CSV file, check if you have sent the activation e-mails. For more information, see Import or Update Users for a Specific Application [page 196].</td>
<td></td>
</tr>
</tbody>
</table>

### Related Information

Get Support [page 432]
1.6 User Guide

This user guide describes the scenarios in the SAP Cloud Platform Identity Authentication service from a user’s perspective. It is aimed at consumers, partners, and employees.

For the scenarios, users can use services to maintain or update their user profiles and to log on to applications. For configuration of certain profile services, users access the profile page at https://<tenant ID>.accounts.ondemand.com/.

**i Note**

*Tenant ID* is an automatically generated ID by the system. For more information about the *Tenant ID*, contact your system administrator.

Users can use the following sign-on services:

- Basic authentication
  Users can log on to applications by providing basic credentials, such as user name and password.
- Single Sign-On authentication
  Users can access cloud applications via SAML 2.0 or OpenID Connect based single sign-on (SSO).
- Two-Factor authentication
  If the application requires two-factor authentication, users should provide a passcode generated by a mobile device as an addition to the basic authentication. For more information, see [Two-Factor Authentication](page 303).

Users can use the following self-services:

**On the Logon Page**

- Self-registration
  If this option is activated by an administrator, a user can register when he or she accesses the application’s logon page. When the user clicks on the *Register Now* link, a registration form appears, where he or she needs to provide some personal data. The user also has to accept the organization’s terms of use and privacy policy. Once the user has submitted the form, he or she receives an e-mail explaining how to activate the account. Successful activation of the user account completes the registration, thus allowing the user to log on to the application.

  **i Note**

  If the user has not received the activation e-mail, he or she can do the following:
  - Check the *Deleted*, *Junk*, or other folders in his or her mail box.
  - Follow the *Forgot Password* link in the logon page of the application. If the registration was successful, this will trigger the *Forgot Password* process, and the user will receive an e-mail with instructions how to reset the password.
  - Choose the *Register Now* link, and fill in the registration form again.
  - Contact the system administrator of the application.

- Forgot password
  A user can change his or her password when he or she accesses the application’s logon page. When the user clicks on the *Forgot password?* link, the user triggers the forgot password process.

- Social sign-on
If this feature is enabled by an administrator, users can link their Identity Authentication accounts with social network accounts. That way they can authenticate through a social provider by choosing the social network button on the logon page. They can also unlink their accounts on the profile page.

**On the Profile Page**

→ **Tip**

Users can access the profile page at https://<tenant ID>.accounts.ondemand.com/.

- **Changing profile data**

Users can change their profile information on the profile page. This includes Personal Information, Company Information, and Contact Preferences.

  → **Note**

  The *E-mail* and *Login Name* fields cannot be edited on the profile page. These fields can be edited by the tenant administrator via the administration console for Identity Authentication.

  If your telephone is verified, the *Phone* cannot be edited on the profile page. This field can be edited by the tenant administrator via the administration console for Identity Authentication.

- **Viewing profile data**

  ○ Users can open a printable overview of all the data on file for them by clicking the *View* button in the *My Data* section.

    → **Note**

    The data includes the *Terms of Use* and *Privacy Policy* documents signed by the user. The documents can be seen by clicking on their names. They open in a new tab.

  ○ Users can download an overview of all the data for them on a JSON file by clicking the *Download* button in the *My Data* section.

- **Changing user passwords**

Users can change their passwords on the profile page.

By clicking the *Change Password* button, users trigger the change password process. That way, they are asked to provide the current and the new passwords. Users also must comply with the password requirements.

  → **Note**

  Users must familiarize themselves with the password policy for logging on to the respective application. If no password policy is set for the application, users are able to modify their passwords with any characters of their choosing.

- **Unlinking social sign-on**

Users can unlink their accounts on the profile page.

**Related Information**

[Scenarios](page 33)

[Two-Factor Authentication](page 303)
1.6.1 Two-Factor Authentication

This document provides information about activation and deactivation, performed on the user profile page, of a mobile device to generate passcodes for time-based one-time (TOTP) two-factor authentication.

With two-factor authentication, you are required to provide a TOTP password, also called a passcode, in addition to your primary credentials. Passcodes are time-based and are valid for one logon attempt only, thus providing additional security to the common static passwords. Passcodes are generated by an authenticator application. The authenticator is a mobile application that you install on your mobile devices. The configurations in this guide are for the SAP Authenticator application. You can also use other third-party authenticators such as Google Authenticator or Microsoft Authenticator. For more information about how to install and configure authenticators other than SAP Authenticator see their documentation.

Activate a Device for TOTP Two-Factor Authentication [page 303]
   To log on to applications that require time-based one-time password (TOTP) as two-factor authentication, you have to activate a mobile device that will generate TOTP passcodes.

Deactivate Devices Configured for TOTP Two-Factor Authentication [page 305]
   This document shows you how to deactivate your mobile devices that you use to generate time-based one-time (TOTP) passcodes for access to applications requiring two-factor authentication.

1.6.1.1 Activate a Device for TOTP Two-Factor Authentication

To log on to applications that require time-based one-time password (TOTP) as two-factor authentication, you have to activate a mobile device that will generate TOTP passcodes.

Prerequisites

- You have installed a QR code scanner and an SAP Authenticator application on your mobile device.

   i Note
   You can also use other third-party authenticators such as Google Authenticator or Microsoft Authenticator. For more information about how to install and configure authenticators other than SAP Authenticator see their documentation.

   i Note
   SAP Authenticator runs on both iOS and Android mobile operating systems.
Context

Some applications require two-factor authentication as an additional security to the common static passwords. They will ask you to provide your password and a passcode, generated by a mobile device.

**i Note**

Passcodes are only necessary for applications that require two-factor authentication. You do not need to activate a device for applications that only require passwords for authentication.

To activate a mobile device that will generate passcodes, proceed as follows:

Procedure


   **i Note**

   *Tenant ID* is an automatically generated ID by the system. For more information about the *Tenant ID*, contact your system administrator.

2. Press *Activate* under *Two-Factor Authentication*. This operation expands the *Two-Factor Authentication* section.

3. Call [Edit] [New Account] in SAP Authenticator, and do one of the following on your mobile device:
   - Scan the QR code.
   - Enter the secret key manually

   **i Note**

   The QR code and the secret key are available in the *Two-Factor Authentication* section of the profile page.

4. Tap *Done* on your mobile device.

5. Enter the passcode generated by the SAP Authenticator application in the space provided on the profile page.

6. Press *Activate*.

Results

Now you can log on to applications that require passcode as an additional security for authentication.

Task overview: Two-Factor Authentication [page 303]
1.6.1.2 Deactivate Devices Configured for TOTP Two-Factor Authentication

This document shows you how to deactivate your mobile devices that you use to generate time-based one-time (TOTP) passcodes for access to applications requiring two-factor authentication.

Context

You can deactivate the mobile devices with authenticator if you do not want to use them any more to generate passcodes.

Note

If you deactivate your mobile devices, you will not be able to log on to applications that require passcodes any more. To be able to access the applications again, you have to activate again a device on the user profile page. For more information, see the Related Information.

If your mobile device has been lost or stolen, or you cannot provide a valid passcode, contact your system administrator.

To deactivate your mobile devices that generate passcodes, proceed as follows:

Procedure


   i Note
   
   Tenant ID is an automatically generated ID by the system. For more information about the Tenant ID, contact your system administrator.

3. Enter the passcode generated by the authenticator application in the provided space on the profile page.
4. Press Deactivate.

Task overview: Two-Factor Authentication [page 303]
1.6.2 Social Authentication

Log on with a Social Provider Account

You can log on to applications that use SAP Cloud Platform Identity Authentication service via your accounts in Twitter, Facebook, LinkedIn, or Google.

Prerequisites

The applications must be configured to allow logon via social networks.

Context

Using the social network authentication, you link your Identity Authentication account with your social network account or accounts. After the initial setup, when you link the accounts, you can log on to the applications with your social network credentials.

Identity Authentication has access to the following data from the social providers:

<table>
<thead>
<tr>
<th>Social Identity Provider</th>
<th>Data Used by SAP Cloud Platform Identity Authentication Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>• ID of your user - used to link your Facebook account with your Identity Authentication account</td>
</tr>
<tr>
<td></td>
<td>• your display name - used to prefill the registration form in case of non-existing user</td>
</tr>
<tr>
<td>Google</td>
<td>• ID of your user - used to link your Google account with your Identity Authentication account</td>
</tr>
<tr>
<td></td>
<td>• your display name, first name, and last name - used to prefill the registration form in case of non-existing user</td>
</tr>
<tr>
<td>LinkedIn</td>
<td>• ID of your user - used to link your LinkedIn account with your Identity Authentication account</td>
</tr>
<tr>
<td></td>
<td>• your first name and last name - used to prefill the registration form in case of non-existing user</td>
</tr>
</tbody>
</table>
Social Identity Provider | Data Used by SAP Cloud Platform Identity Authentication Service
---|---
Twitter | - ID of your user - used to link your Twitter account with your Identity Authentication account  
- your display name - used to prefill the registration form in case of non-existing user  
- your logon name

This data is used for the initial linking of your Identity Authentication account with the social network account. Later, if you update the personal information in your social account, the updated information will not be copied by Identity Authentication.

To link your Identity Authentication account with a social network account, proceed as follows:

**Procedure**

1. Access the application’s logon page.
2. Choose the icon of the social network provider you want to log on with.

   **i Note**
   
   Which social networks are displayed on the page depends on the application.

3. Sign in to your social network account.
4. Choose one of the following options:
   1. Link your Identity Authentication account with your social network account.
   2. Create a new Identity Authentication account that will be linked with your social network account.

   **i Note**
   
   This option appears only for applications that allow user registration.

**Results**

Once you allow Identity Authentication to link your account with the social providers’ accounts, you can log on to the applications via the social providers.
Unlink a Social Provider Account

You can unlink your social provider account via the profile page.

Context

To remove your social network logon information from your Identity Authentication account, proceed as follows:

Procedure

   
   Note
   
   Tenant ID is an automatically generated ID by the system. For more information about the Tenant ID, contact your system administrator.

3. Press Unlink to remove your social network logon information from your account.

   If the operation is successful, the system displays the message Profile updated.

1.6.3 Use the Remember Me Option

With the Remember me functionality enabled, you can log on to an application without the need to provide your credentials every time you access it.

Context

If you enable the Remember me functionality, the application saves a cookie in the browser on your local computer. It automatically logs you on next time you access the application from the same browser on your local computer. Once enabled, the Remember me functionality is valid for 3 months unless you log out from the application.

Note

If the application requires two-factor authentication, you must provide a valid one-time password (passcode) generated by a mobile device every time you access the application. For more details about how to use two-factor authentication on your mobile device, see Related Information.
Procedure

1. Access the application that you want to log on to with Remember me.
2. Provide your credentials and select the Remember me checkbox.
3. Optional: Provide a passcode if required.

Results

Next time you access the application, you will be logged on automatically. If the application requires two-factor authentication, you need to provide a valid passcode, generated by a mobile device.

**i Note**

If you want to disable Remember me for an application log out from the application, and do not select the checkbox next time you log on.

Related Information

Two-Factor Authentication [page 303]

1.6.4 Access Applications with Single Sign-On on Mobile Devices

You can access trusted applications that require two-factor authentication via your mobile devices using single sign-on (SSO).

Prerequisites

- The application requires passcode as additional protection.
- You have a mobile device.
- You have installed and configured an SAP Authenticator on your mobile device. For more details see, One-Time Password Authentication User Guide. SAP Authenticator runs on both iOS and Android mobile operating systems.
- You have activated your mobile device for two-factor authentication. For more details about how to activate a device for two-factor authentication, see Activate a Device for TOTP Two-Factor Authentication [page 303].
Context

This feature allows you to access applications via your mobile device without the need to type manually your username, password, and passcode. The first time you access the application, you will be prompted to provide your credentials. If you have enabled the Remember me functionality, you will be logged on next time based on the cookie saved in the browser. For more details about the Remember me functionality, see Related Information.

Procedure

1. Launch SAP Authenticator on your mobile device.
2. Add the application in the SAP Authenticator.
   
   To add the application, you need to scan a QR code or type the application’s link manually. Your administrator should provide you with the QR code or the application’s link. The link follows the following pattern:

   \[ https://<tenant_ID>.accounts.ondemand.com/saml2/idp/sso?sp=<sp_name>\&RelayState=<sp_specific_value>\&index=<index_number>\&j_username=[username]\&j_otpcode=[passcode] \]

   Note

   Tenant ID is an automatically generated ID by the system. For more information about the Tenant ID, contact your system administrator.

3. Log on to the application via SAP Authenticator.
4. Select the Remember me checkbox.
5. Provide your credentials.

Results

You are now logged on to the application. Next time you try to log on to this application via SAP Authenticator, you will not have to provide your credentials and a passcode. The system will log you on automatically.

Related Information

Two-Factor Authentication [page 303]
Use the Remember Me Option [page 308]
### 1.6.5 Change Password

You can change your current password via your profile page.

#### Context

Your password grants you access to any platform connected to SAP Cloud Platform Identity Authentication service. You can change your password by triggering the change password process. To change your current password, you need to provide the current and the new passwords to the system. You also must comply with the password requirements.

> **Tip**
>
> If you don’t know your current password, follow the *Forgot Password* link in the logon page of the application. This will trigger the *Forgot Password* process, and you will receive an e-mail with instructions how to reset your password.

To change your current password, follow the procedure below:

#### Procedure


    > **Note**
    > *Tenant ID* is an automatically generated ID by the system. For more information about the *Tenant ID*, contact your system administrator.

2. Press *Change Password* button in the *Password* section.
3. Provide your current and new password.
4. Save your changes.

#### Results

If the operation is successful, can log on with your new password.

> **Remember**
>
> Your password can only be changed once every 24 hours.
1.6.6 Troubleshooting for Users

This section aims to help end users to deal with error messages when using applications for logon, registration, invitation, password update, and account activation.

Error Codes

Solutions to Error Messages

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication failed; try again</td>
<td>You have entered the wrong credentials; Your account is not activated.</td>
<td>Try again; Open your e-mail and activate your account; Register on the logon page; Contact your administrator.</td>
</tr>
<tr>
<td>Account is locked; select the link in the e-mail that has been sent to unlock your account;</td>
<td>You are not allowed to log on to your account.</td>
<td>Check the e-mail you received from SAP Cloud Platform Identity Authentication service with instructions about how to unlock your account; Contact your administrator.</td>
</tr>
<tr>
<td>An error occurred; try again</td>
<td>An unexpected error occurred.</td>
<td>Try again; Contact your administrator.</td>
</tr>
<tr>
<td>Insufficient password complexity; check password requirements</td>
<td>Your password does not comply with the application’s password policy.</td>
<td>Familiarize yourself with the password policy for the application.</td>
</tr>
<tr>
<td>Cannot verify your password; try again</td>
<td>The old password for the password update is invalid.</td>
<td>Enter your correct current password.</td>
</tr>
<tr>
<td>The password has already been changed in the last 24 hours</td>
<td>According to the application’s policy, you are not allowed to change the password right now.</td>
<td>Familiarize yourself with the application’s policy for changing the password; Try again later.</td>
</tr>
<tr>
<td>Your e-mail activation link is invalid.</td>
<td>The e-mail activation link that you have received is expired or already used by you.</td>
<td><img src="image" alt="Visit the application choose Log On follow Forgot Password link" /> Contact your administrator.</td>
</tr>
</tbody>
</table>

Related Information

Get Support [page 432]
1.7 Developer Guide

The developer guide is aimed mainly at organization developers who can implement configurations in addition to the ones in the administration console of Identity Authentication. Developers can use REST API services to configure various authentication and registration mechanisms for their applications. The applications that administrators configure use different application services for all user-related processes.

Application Services

The application services are used by the cloud services and cloud applications to interact with Identity Authentication with regard to user records in the tenant.

The following APIs are offered to cloud applications:

- An API to register users
  For more information, see User Registration [page 320]
- An API to invite users
  For more information, see Invitation REST API [page 317]
- Identity Authentication implementation of the System for Cross-domain Identity Management (SCIM) REST API protocol.
  For more information, see SCIM REST API [page 334].
- An API to change the predefined texts and messages for end-user screens available per tenant in the Identity Authentication.
  For more information, see Change Tenant Texts REST API [page 382].
- An API to change the predefined master data texts.
  For more information, see Change Master Data Texts REST API [page 388].

Related Information

Troubleshooting for Developers [page 399]
Configure a Certificate for API Authentication [page 80]

1.7.1 API Authentication

Developers can choose the type of authentication when API methods of SAP Cloud Platform Identity Authentication service are used.

The certificate to be used for authentication by the REST APIs of Identity Authentication must be requested from the SAP Support Portal.
1.7.1.1  Configure Credentials for HTTP Basic Authentication

This document describes how developers set basic authentication when API methods of SAP Cloud Platform Identity Authentication service are used.

Context

You can use a user ID and a password to authenticate when REST API calls to the tenant of Identity Authentication are used. The system automatically generates a user ID when the password is set for the first time.

Note

The password must meet the following conditions:
- Minimum length of 8 characters
- Characters from at least three of the following groups:
  - Lower-case Latin characters (a-z)
  - Upper-case Latin characters (A-Z)
  - Base 10 digits (0-9)
  - Non-alphabetic characters (!@#$%...)

The password is locked for 60 min after 5 failed logon attempts with wrong value.

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   Note
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.

   `Tenant ID` is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the `tenant ID`.

2. Choose the Applications tile.

   This operation opens a list of the applications.

3. Choose the application that you want to edit.

   Note
   
   Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.
If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.
5. Under API AUTHENTICATION, choose HTTP Basic Authentication.
6. Enter your new password in the fields.

**Note**
If you are setting the password for API authentication for the first time, these fields are empty.

7. Save your entries.

Once the password has been saved, the system displays a message informing you of this.

### 1.7.1.2 Configure a Certificate for API Authentication

This document describes how developers configure the certificate used for authentication when API methods of SAP Cloud Platform Identity Authentication service are used.

**Prerequisites**

You have requested a client certificate from the SAP Support Portal.

**Context**

For the configuration, you have to provide the base64-encoded certificate as a file or plain text.

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   **Note**
   The URL has the \https://<tenant ID>.accounts.ondemand.com/admin\ pattern.

   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the Applications tile.

   This operation opens a list of the applications.
3. Choose the application that you want to edit.

Note

Type the name of the application in the search field to filter the list items, or choose the application from the list on the left.

If you do not have a created application in your list, you can create one. For more information, see Create a New Application [page 43].

4. Choose the Trust tab.


6. Upload or enter the base64-encoded certificate.

Note

For the upload, you have to use .cer or .crt files.

7. Save your entries.

Once the certificate has been uploaded, the system displays the message Certificate for API authentication updated.

Related Information

Create a New Application [page 43]
Invitation REST API [page 317]
User Management REST API [page 319]

1.7.2 API Documentation

This document contains references to the API Documentation of SAP Cloud Platform Identity Authentication service.

REST APIs

Invitation REST API [page 317]
User Management REST API [page 319]
Password Service REST API [page 329]
Forgot Password REST API [page 331]
SCIM REST API [page 334]
Change Tenant Texts REST API [page 382]
1.7.2.1 Invitation REST API

The invitation service allows you to implement a request for user invitations. The invitees then receive an e-mail containing information about how to register.

Prerequisites

- You need to set up the authentication type to access the API. For more information about this configuration, see API Authentication [page 79]

Resources

To configure the invitation service, you use a POST request with the following URI: `https://<tenant ID>.accounts.ondemand.com/cps/invite/`.

Representation

You have to use a JSON representation of the invitation request by specifying `application/json` content type. All declared parameters in the request must also be JSON encoded.

Parameters

<table>
<thead>
<tr>
<th>Required Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inviteeEmail</td>
<td>The e-mail of the invitee</td>
</tr>
</tbody>
</table>

**i Note**

Only `inviteeEmail` or `inviteeUserId` should be used, not both.
Required Parameter | Description
--- | ---
inviteeUserId | The user ID of the invitee

**i Note**
Only `inviteeEmail` or `inviteeUserId` should be used, not both.

inviterName | The display name of the user who sends the invitation.
targetUrl | The URL that the user is redirected to after registration.

**→ Recommendation**
From a usability perspective we recommend you to use URL of a protected page.

**i Note**
The `targetUrl` parameter is optional if a `Home URL` is set for the application, and the application does not use overlay.

If `targetUrl` is not specified, or the application uses overlay, the user is redirected to the application’s `Home URL`, which must be set.

For more information how to configure `Home URL`, see Configure an Application’s Home URL [page 50].

sourceUrl | The URL for the invitation link in the e-mail sent to the invitee. The URL must be a public page.

**i Note**
The `sourceUrl` parameter is optional if a `Home URL` is set for the application, and the application does not use overlay.

If `sourceUrl` is not specified, or the application uses overlay, the user is redirected to the application’s `Home URL`, which must be set.

For more information how to configure `Home URL`, see Configure an Application’s Home URL [page 50].

Optional Parameters for the POST Method

| Optional Parameter | Description |
--- | ---
inviteeFirstName | The first name of the invitee
inviteeLastName | The last name of the invitee
footerText | The footer text of the invitation e-mail
### Optional Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>headerText</td>
<td>The header text of the invitation e-mail</td>
</tr>
</tbody>
</table>

### Example

```
POST /cps/invite/
Content-Type: application/json

{
    "inviteeEmail": "john.miller@company.com",
    "inviteeFirstName": "John",
    "inviteeLastName": "Miller",
    "inviterName": "Donna Moore",
    "footerText": "Invitation footer sample text",
    "headerText": "Invitation header sample text",
    "targetUrl": "http://www.myserviceprovider.com/protected_home_page/",
}
```

### Related Information

- Add Logon Overlays in Customer Applications [page 396]
- Configure an Application's Home URL [page 50]
- Configure a Certificate for API Authentication [page 80]
- Troubleshooting for Developers [page 399]
- Configure an Application's Home URL [page 50]

### 1.7.2.2 User Management REST API

This REST API allows you to implement a request for user management, such as user registration, as well as SP user retrieval, deactivation and deletion.

### Prerequisites

You need to set up the authentication type to access the API. For more information about this configuration, see API Authentication [page 79].

### Methods
<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>Action</th>
<th>URI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>POST</strong></td>
<td>User Registration [page 320]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/service/users</td>
</tr>
<tr>
<td><strong>GET</strong></td>
<td>SP User ID Retrieval [page 324]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/service/users</td>
</tr>
<tr>
<td><strong>GET</strong></td>
<td>SP User Information [page 325]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/service/users/&lt;SP user ID&gt;</td>
</tr>
<tr>
<td><strong>PUT</strong></td>
<td>SP User Deactivation [page 327]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/service/users/&lt;SP user ID&gt;</td>
</tr>
<tr>
<td><strong>DELETE</strong></td>
<td>SP User Deletion [page 328]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/service/users/&lt;SP user ID&gt;</td>
</tr>
</tbody>
</table>

## 1.7.2.2.1 User Registration

The user registration is used for registration of new users or for on-behalf registration of partners.

### Prerequisites

You need to set up the authentication type to access the API. For more information about this configuration, see API Authentication [page 79].

### Request

**URI:** https://<tenant ID>.accounts.ondemand.com/service/users

**HTTP Method:** POST

**Request Headers**

<table>
<thead>
<tr>
<th>Header</th>
<th>Required</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Authorization</td>
<td>Yes</td>
<td>For more information, see API Authentication [page 79].</td>
</tr>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td>application/x-www-form-urlencoded</td>
</tr>
</tbody>
</table>
### Request Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Data Type</th>
<th>Description</th>
<th>Parameter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>email</td>
<td>Yes</td>
<td>String</td>
<td>The e-mail of the user you register.</td>
<td>Request body</td>
</tr>
<tr>
<td>user_profile_id</td>
<td>No</td>
<td>String</td>
<td>The user ID</td>
<td>Request body</td>
</tr>
<tr>
<td>login_name</td>
<td>No</td>
<td>String</td>
<td>The logon name of the user</td>
<td>Request body</td>
</tr>
<tr>
<td>first_name</td>
<td>No</td>
<td>String</td>
<td>The first name of the user you register. The allowed maximum length for the first name is 32 characters.</td>
<td>Request body</td>
</tr>
<tr>
<td>last_name</td>
<td>No</td>
<td>String</td>
<td>The last name of the user you register. The allowed maximum length for the last name is 64 characters.</td>
<td>Request body</td>
</tr>
<tr>
<td>language</td>
<td>No</td>
<td>String</td>
<td>The preferred language of the user you register</td>
<td>Request body</td>
</tr>
<tr>
<td>valid_from</td>
<td>No</td>
<td>String</td>
<td>The valid from date</td>
<td>Request body</td>
</tr>
<tr>
<td>valid_from</td>
<td>No</td>
<td>String</td>
<td>The valid from date</td>
<td>Request body</td>
</tr>
<tr>
<td>valid_to</td>
<td>No</td>
<td>String</td>
<td>The valid until date</td>
<td>Request body</td>
</tr>
<tr>
<td>name_id</td>
<td>No</td>
<td>String</td>
<td>The name ID of the user you register.</td>
<td>Request body</td>
</tr>
<tr>
<td>source_url</td>
<td>No</td>
<td>String</td>
<td>The URL to the public page of the application where the SAP Cloud Platform Identity Authentication service overlays are integrated. If not provided, the activation screen is shown without overlays. This parameter value must be URL-encoded.</td>
<td>Request body</td>
</tr>
<tr>
<td>target_url</td>
<td>No</td>
<td>String</td>
<td>The URL to the application page that the user should be redirected to after he or she has completed account activation. If target_url is not provided, the user is redirected to the home URL configured for the service provider. For more information how to configure Home URL, see Configure an Application’s Home URL [page 50].</td>
<td>Request body</td>
</tr>
</tbody>
</table>
### Parameter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Data Type</th>
<th>Description</th>
<th>Parameter Type</th>
</tr>
</thead>
</table>
| send_email        | No       | Boolean   | Values: true (default value), false  
- If true - activation e-mail is sent to the user.  
- If false - activation e-mail is not sent to the user. |
| spCustomAttribute1 | No       | String    | Custom attributes are used to store additional information for the SP users. It is allowed to pass five customer attributes for a user |
| spCustomAttribute2 | No       | String    | Custom attributes are used to store additional information for the SP users. It is allowed to pass five customer attributes for a user |
| spCustomAttribute3 | No       | String    | Custom attributes are used to store additional information for the SP users. It is allowed to pass five customer attributes for a user |
| spCustomAttribute4 | No       | String    | Custom attributes are used to store additional information for the SP users. It is allowed to pass five customer attributes for a user |
| spCustomAttribute5 | No       | String    | Custom attributes are used to store additional information for the SP users. It is allowed to pass five customer attributes for a user |

#### Request Example

**⚠️ Example**

**⚠️ Caution**

All parameters for the POST method must be written on one line.

```
POST /service/users 
Content-Type: application/x-www-form-urlencoded 
name_id=johns&user_profile_id=p987654&email=john.smith@sap.com&first_name=John 
&last_name=Smith&language=en&valid_from=20110901120000Z&valid_to=201209011100
```
Response

Response Status and Error Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Created</td>
<td>The user is successfully created.</td>
</tr>
<tr>
<td>400</td>
<td>Bad Request</td>
<td>The user for whom you are trying to create an SP user is inactive.</td>
</tr>
<tr>
<td>409</td>
<td>Conflict</td>
<td>The SP user already exists.</td>
</tr>
</tbody>
</table>

For more information about the general error codes that may be returned, see General Error Codes [page 395].

Response Example

❖ Example

The URI of the created user is returned in the location header of the HTTP Response.

Location: https://<tenant ID>.accounts.ondemand.com/service/users/0800200c9a66

❖ Example

In case of conflict, the URI of the conflicting user is returned in the location header of the HTTP Response.

Location: https://<tenant ID>.accounts.ondemand.com/service/users/467345637aa

❖ Example

In case of creating a new user with "send_email=false", the activation link is returned in the HTTP Response body.

Content-Type: application/json

```json
{
    "activationLink" : "https://<tenant ID>.accounts.ondemand.com/ids/activation?
token=I1830C497BF9B857B7d6298E5F117AF39711F59A28838A3276E8B68FFFP54414C8843ACF395A05401ABE6568FF3659D6EE96"
}
```
1.7.2.2.2 SP User ID Retrieval

To retrieve an SP (service provider) user's ID, you use the GET method.

Prerequisites

You need to set up the authentication type to access the API. For more information about this configuration, see API Authentication [page 79].

Request

URI: https://<tenant ID>.accounts.ondemand.com/service/users

HTTP Method: GET

Request Headers

<table>
<thead>
<tr>
<th>Header</th>
<th>Required</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Authorization</td>
<td>Yes</td>
<td>For more information, see API Authentication [page 79].</td>
</tr>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td>application/vnd.sap-id-service.sp-user-id+xml</td>
</tr>
</tbody>
</table>

Request Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Data Type</th>
<th>Description</th>
<th>Parameter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>name_id</td>
<td>Yes</td>
<td>String</td>
<td>The name ID of the user you register.</td>
<td>Query string</td>
</tr>
<tr>
<td>sp_name</td>
<td>Yes</td>
<td>String</td>
<td>The ID of the service provider.</td>
<td>Query string</td>
</tr>
</tbody>
</table>

Request Example

GET /service/users?name_id=johns&sp_name=jpaas.developer
Response

Response Headers

<table>
<thead>
<tr>
<th>Header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>The ID of the created SP user is in the location header of the HTTP Response.</td>
</tr>
</tbody>
</table>

Response Example

```
Location: https://<tenant ID>.accounts.ondemand.com/service/users/<SP user ID>
```

Related Information

User Management REST API [page 319]

1.7.2.2.3 SP User Information

To retrieve information for an SP (service provider) user, you use a GET method.

Prerequisites

You need to set up the authentication type to access the API. For more information about this configuration, see API Authentication [page 79].

Request

URI: https://<tenant ID>.accounts.ondemand.com/service/users/<SP user id>

HTTP Method: GET

Request Headers

<table>
<thead>
<tr>
<th>Header</th>
<th>Required</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Authorization</td>
<td>Yes</td>
<td>For more information, see API Authentication [page 79].</td>
</tr>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td>application/vnd.sap-id-service.sp-user-id+xml</td>
</tr>
</tbody>
</table>
Request Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Data Type</th>
<th>Description</th>
<th>Parameter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;SP user ID&gt;</td>
<td>Yes</td>
<td>String</td>
<td>The SP user id.</td>
<td>Path</td>
</tr>
</tbody>
</table>

Request Example

GET /service/users/<the ID of the SP user>

Response

Response Attributes

The response returns the following attributes. Only the attributes that exist for the user are returned.

- user_profile_id
- name_id
- status
- profile_status
- valid_from
- valid_to
- activation_time
- email
- language
- first_name
- last_name
- sp_name
- login_name
- country
- city
- company_city

Response Status and Error Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK</td>
<td>The information for the user is returned in the response.</td>
</tr>
<tr>
<td>404</td>
<td>Not Found</td>
<td>The SP user with the provided ID does not exist.</td>
</tr>
</tbody>
</table>

Related Information

User Management REST API [page 319]
1.7.2.4 \textit{SP User Deactivation}

To deactivate an SP (service provider) user, you use a \textit{PUT} method.

\section*{Prerequisites}

You need to set up the authentication type to access the API. For more information about this configuration, see \textit{API Authentication} [page 79].

\section*{Request}

\begin{itemize}
\item **URI:** \texttt{https://<tenant ID>.accounts.ondemand.com/service/users/<SP user ID>}
\item **HTTP Method:** \textit{PUT}
\end{itemize}

\begin{center}
\begin{tabular}{|c|c|c|}
\hline
\textbf{Header} & \textbf{Required} & \textbf{Values} \\
\hline
Basic Authorization & Yes & For more information, see \textit{API Authentication} [page 79]. \\
Content-Type & Yes & application/vnd.sap-id-service.sp-user-id+xml \\
\hline
\end{tabular}
\end{center}

\begin{center}
\begin{tabular}{|c|c|c|c|}
\hline
\textbf{Parameter} & \textbf{Required} & \textbf{Data Type} & \textbf{Description} & \textbf{Parameter Type} \\
\hline
status & Yes & String & When the user activates his or her e-mail, the \textit{status} is set to \textbf{active}. To deactivate the SP user, update the \textit{status} parameter by setting it to \textbf{inactive}. To activate the SP user, set it to \textbf{active}. & Request body \\
\hline
\end{tabular}
\end{center}

\section*{Request Example}

\begin{verbatim}
PUT /service/users/<the ID of the SP user>
Content-type: application/vnd.sap-id-service.sp-user-id+xml; version=1.0
\<user>
  \<status>inactive</status>
\</user>
\end{verbatim}
Response

Response Status and Error Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>Deactivated</td>
<td>SP user is successfully deactivated</td>
</tr>
</tbody>
</table>

For more information about the general error codes that may be returned, see [General Error Codes](#page395).

i Note

If a user logs into an application he or she is deactivated for, the identity provider will block the logon and notify the application.

Response Example

```xml
<Response Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
            Destination="https://example.com/saml2/acs"
            Version="2.0"
            xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion"
            xmlns="urn:oasis:names:tc:SAML:2.0:protocol"
            xmlns:ns4="http://www.w3.org/2001/04/xmlenc#"
            xmlns:ns3="http://www.w3.org/2000/09/xmldsig#">
  <ns2:Issuer>accounts.sap.com</ns2:Issuer>
  <Status>
    <StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Responder">
    </StatusCode>
    <StatusMessage>The SP user [URI of the sp user] is with status inactive for Service Provider [example.com]</StatusMessage>
  </Status>
</Response>
```

Related Information

[User Management REST API](#page319)

1.7.2.2.5 SP User Deletion

Delete an SP (service provider) user.

Prerequisites

You need to set up the authentication type to access the API. For more information about this configuration, see [API Authentication](#page79).
Caution
If the last SP user is deleted, and the user is of type public, then the whole user profile is deleted.

Request

URI: https://<tenant ID>.accounts.ondemand.com/service/users/<SP user ID>
HTTP Method: DELETE

Request Headers

<table>
<thead>
<tr>
<th>Header</th>
<th>Required</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Authentication</td>
<td>Yes</td>
<td>For more information, see API Authentication [page 79].</td>
</tr>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td>application/vnd.sap-id-service.sp-user-id+xml</td>
</tr>
</tbody>
</table>

Request Example

DELETE /service/users/0800200c9a66

Response

Response Status and Error Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>The operation is successful.</td>
<td>The SP user is deleted.</td>
</tr>
</tbody>
</table>

For more information about the general error codes that may be returned, see General Error Codes [page 395].

Related Information

User Management REST API [page 319]

1.7.2.3 Password Service REST API

The password service is used for operations related to user passwords, such as verification of the user name and the password combination.
Verify Username and Password Combination

Verify the username and password combination, or verify the thing ID and password combination.

Request

URI: `https://<tenant ID>.accounts.ondemand.com/service/users/password`

**i Note**

*Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

**HTTP Method:** POST

**Request Headers**

<table>
<thead>
<tr>
<th>Header</th>
<th>Required</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Authorization</td>
<td>Yes</td>
<td>Username and password are provided by the user.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>i Note</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The username can be either the user e-mail or the user logon name of the user profile ID according to the HTTP Basic authentication scheme.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Caution</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the user provides wrong password, then each verification counts as a failed logon attempt. The password locks when the number of the allowed failed logon attempts is reached. The number depends on the password policy applied for the application. For more information, see Configuring Password Policies [page 166].</td>
</tr>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td>application/json</td>
</tr>
</tbody>
</table>

**Request Example**

```
POST /service/users/password
Authorization: Basic cDk4NzY1NDphYmNkMTIzNA==
```
Response

Response Status and Error Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Result or X-Message Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>Success</td>
<td>When the username and password combination or thing ID and password combination is verified.</td>
</tr>
<tr>
<td>401 Unauthorized</td>
<td>PASSWORD_LOCKED</td>
<td>When the password is locked for 60 minutes.</td>
</tr>
<tr>
<td></td>
<td>PASSWORD_DISABLED</td>
<td>When the password is disabled.</td>
</tr>
<tr>
<td></td>
<td>USER_INACTIVE</td>
<td>When the user is not in status active.</td>
</tr>
<tr>
<td></td>
<td>PASSWORD_RESET_REQUIRED</td>
<td>When the user must reset his or her password before logon.</td>
</tr>
<tr>
<td></td>
<td>PASSWORD_CHANGE_REQUIRED</td>
<td>When the user must change his or her password before logon.</td>
</tr>
</tbody>
</table>

Response Example

On success, the HTTP Response Body contains:

```json
{
  "uid": "P000000",
  "first_name": "Dona",
  "last_name": "Moore",
  "mail": "dona.moore@example.com",
  "type": "employee"
}
```

Related Information

General Error Codes [page 395]
Configure Risk-Based Authentication [page 82]
Configure User Access to the Application [page 87]

1.7.2.4 Forgot Password REST API

The forgot password REST API sends a reset password e-mail.

The language of the reset password e-mail is defined in the following order of importance:

Custom Template Sets Configured for Application

1. If the user is set with a specific language:
   1. if the language exists in the custom template, the system sends the reset password e-mail in that language
2. if the language does not exist in the custom template, the system sends the reset password e-mail in English, if English exists in the custom template set
3. if the language of the user, and the English language do not exist in the custom template, the system sends the reset password e-mail in English from the Default template set

2. If the user is not set with a specific language:
   1. if English exists in the custom template set, the system sends the reset password e-mail in English from the custom template set
   2. if English does not exist in the custom template set, the system sends the reset password e-mail in English from the Default template set

Default Template Set Configured for Application

If the user is set with a specific language, the system sends the reset password e-mail in that language, if it exists in the Default set. Otherwise, it sends the reset password e-mail in English from the Default template set.

For more information about the e-mail template sets, see Configuring E-Mail Templates [page 184].

→ Tip
(For SAML 2.0 Applications) To log out the user from all active session, when a new password is set, configure the SOAP endpoint. For more information, see Configure SAML 2.0 Service Provider [page 55].

Request

URL: https://<tenant ID>.accounts.ondemand.com/service/users/forgotPassword

i Note

Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

HTTP Method: POST

Request Headers

<table>
<thead>
<tr>
<th>Header</th>
<th>Required</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Authorization</td>
<td>Yes</td>
<td>• via application ((service provider (SP)) Authentication certificate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• via SP REST API username and password</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information, see API Authentication [page 79].</td>
</tr>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td>application/json</td>
</tr>
</tbody>
</table>
Request Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Data Type</th>
<th>Description</th>
<th>Parameter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>identifier</td>
<td>Yes</td>
<td>string</td>
<td>supported attributes:</td>
<td>Request body</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● email</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● loginName</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● uid</td>
<td></td>
</tr>
</tbody>
</table>

Request Example

```
{
  "identifier": "dona.moore@example.com"
}
```

Response

Response Status and Error Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>The user exists and password reset is allowed for the user profile.</td>
<td>Forgot password e-mail is sent to the provided user.</td>
</tr>
<tr>
<td></td>
<td>iNote</td>
<td>Forgot password e-mail is not sent when the response is 200 OK in following cases:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● the user does not exist</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● the limit of three forgot password e-mails sent for the last 24 hours has been reached</td>
</tr>
<tr>
<td>400 Bad Request</td>
<td>PASSWORD_TOO_NEW</td>
<td>When the password has already been changed for the last 24 hours.</td>
</tr>
<tr>
<td></td>
<td>USER_INACTIVE</td>
<td>When the user status is inactive.</td>
</tr>
<tr>
<td></td>
<td>PASSWORD_DISABLED</td>
<td>When the password is disabled.</td>
</tr>
</tbody>
</table>

Related Information

General Error Codes [page 395]
List and Edit User Details [page 205]
1.7.2.5 SCIM REST API

This section contains information about the SAP Cloud Platform Identity Authentication service implementation of the System for Cross-domain Identity Management (SCIM) REST API protocol.

Prerequisites

To call the methods of this SCIM REST API you must have a system as administrator (T user) with an assigned Manage Users role. For more details about how to add a system as administrator and assign administrator roles, see Add System as Administrator [page 240], and Edit Administrator Authorizations [page 241].

Additional Attributes Supported Values

Some of the attributes have predefined supported values. They are returned as a map of key value pairs. See some examples in the table below. For the full set of attributes, copy the URL from the table, replace <tenant ID> with your Tenant ID, and open the edited URL in a web browser.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Examples</th>
<th>Full Sets</th>
</tr>
</thead>
<tbody>
<tr>
<td>name.honorificPrefix</td>
<td>[Mr., Ms.]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/md/salutations</td>
</tr>
<tr>
<td>addresses.country</td>
<td>[AF, AX]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/md/countries</td>
</tr>
<tr>
<td>addresses.region</td>
<td>[NY]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/md/states/us</td>
</tr>
<tr>
<td></td>
<td>[AB]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/md/states/ca</td>
</tr>
</tbody>
</table>

i Note

The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Examples</th>
<th>Full Sets</th>
</tr>
</thead>
<tbody>
<tr>
<td>industryCrm</td>
<td>• [Aerospace and Defense]</td>
<td>• https://&lt;tenant ID&gt;.accounts.ondemand.com/md/industries</td>
</tr>
<tr>
<td>timeZone</td>
<td>• [Africa/Abidjan]</td>
<td>• https://&lt;tenant ID&gt;.accounts.ondemand.com/md/timezones</td>
</tr>
<tr>
<td>department</td>
<td>• [Administration]</td>
<td>• https://&lt;tenant ID&gt;.accounts.ondemand.com/md/departments</td>
</tr>
<tr>
<td>companyRelationship</td>
<td>• [Consultant]</td>
<td>• https://&lt;tenant ID&gt;.accounts.ondemand.com/md/relationships</td>
</tr>
<tr>
<td>locale</td>
<td>• [EN]</td>
<td>• https://&lt;tenant ID&gt;.accounts.ondemand.com/md/languages</td>
</tr>
</tbody>
</table>

**Restricted Characters**

The characters <, >, : are not allowed for the attributes `displayName`, `name.familyName`, and `name.givenName`.

**Methods**

**Manage Users**

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>Action</th>
<th>URI</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>Users Search [page 337]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/service/scim/Users/</td>
</tr>
<tr>
<td>GET</td>
<td>User Resource [page 343]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/service/scim/Users/&lt;id&gt;</td>
</tr>
</tbody>
</table>
HTTP Method | Action | URI |
--- | --- | --- |
**PUT** | Update User Resource [page 358] | https://<tenant ID>.accounts.ondemand.com/service/scim/Users/<id> |

**DELETE** | Delete User Resource [page 368] | https://<tenant ID>.accounts.ondemand.com/service/scim/Users/<id> |

**Manage Groups**

HTTP Method | Action | URI |
--- | --- | --- |
**GET** | Groups Search [page 370] | https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/ |
**GET** | Group Resource [page 373] | https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/<id of the group> |
**POST** | Create Group Resource [page 375] | https://<tenant ID>.accounts.ondemand.com/service/scim/Groups |
**PUT** | Update Group Resource [page 377] | https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/<id of the group> |
**DELETE** | Delete Group Resource [page 380] | https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/<id of the group> |

### Related Information

- System for Cross-Domain Identity Management
- SCIM Data Types

### 1.7.2.5.1 Manage Users SCIM REST API

**Users Search [page 337]**

The user search method of the Identity Authentication implementation of the SCIM REST API protocol allows you to perform a request for user search. User search is implemented as defined by the System for Cross-domain Identity Management (SCIM) protocol for querying and filtering resources.

**User Resource [page 343]**

The user resource method of the SAP Cloud Platform Identity Authentication service implementation of the SCIM REST API protocol provides information on a known user.
Create User Resource [page 348]

The create user resource method of the Identity Authentication implementation of the SCIM REST API protocol provides information on the creation of a user.

Update User Resource [page 358]

The update user method of the implementation of the SCIM REST API protocol provides information on the update of a known user. The method does not create a new user.

Delete User Resource [page 368]

The delete user resource method of the Identity Authentication implementation of the SCIM REST API protocol allows you to delete an existing user. Delete user resource is implemented as defined by the System for Cross-domain Identity Management (SCIM) protocol.

Related Information

SCIM REST API [page 334]

1.7.2.5.1.1 Users Search

The user search method of the Identity Authentication implementation of the SCIM REST API protocol allows you to perform a request for user search. User search is implemented as defined by the System for Cross-domain Identity Management (SCIM) protocol for querying and filtering resources.

Request

**URI:** https://<tenant ID>.accounts.ondemand.com/service/scim/Users/

**HTTP Method:** GET

**Content-Type:** application/scim+json

**Authentication mechanisms:**
- Client certificate
- Basic authentication

**Request Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter</td>
<td>No</td>
<td>Defines the search criteria. If missing, the search criteria will depend on the other parameters.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Required</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>count</td>
<td>No</td>
<td>Paginates the response. Represents the number of items which will be returned per page. The maximum number of items returned per page is limited to 100.</td>
</tr>
<tr>
<td>startIndex</td>
<td>No</td>
<td>Paginates the response. Represents the start index from which the results are returned.</td>
</tr>
</tbody>
</table>

**i Note**

If you have more than 100 user, and you want to get the full list, you have to perform multiple requests.

<table>
<thead>
<tr>
<th>Operator</th>
<th>Description</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>eq</td>
<td>equal</td>
<td>The attribute and attribute values must be identical for a match.</td>
</tr>
<tr>
<td>and</td>
<td>Logical And</td>
<td>The filter is only a match if all expressions evaluate to true.</td>
</tr>
</tbody>
</table>

**User Search Attributes**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Public user ID of the user</td>
</tr>
<tr>
<td>emails</td>
<td>E-mail address of the user</td>
</tr>
<tr>
<td>userName</td>
<td>Custom logon name of the user</td>
</tr>
<tr>
<td>name.familyName</td>
<td>Last name of the user</td>
</tr>
<tr>
<td>addresses.country</td>
<td>The [home]country of the user. The value is in the ISO 3166-1 alpha 2 “short” code format. <a href="#">ISO3166</a>.</td>
</tr>
<tr>
<td>groups</td>
<td>User group assignment information</td>
</tr>
</tbody>
</table>
Request Example

Example

GET /service/scim/Users?filter=emails eq "john.smith@sap.com" and addresses.country eq "US"&count=10&startIndex=1

Response

Format: **JSON**

The response contains a list of users with the following user attributes:

- meta
- userType
- id
- emails.value
- name.honorificPrefix
- name.givenName
- name.familyName
- name.middleName
- userName
- addresses[work].streetAddress
- addresses[work].locality

**i Note**

The attribute equals to city.

- addresses[work].region

**i Note**

The attribute is relevant only for Canada and the United States of America. It equals to the **state** in these countries.

- addresses[work].postalCode
- addresses[work].country
- addresses[home].streetAddress
- addresses[home].locality

**i Note**

The attribute equals to city.

- addresses[home].region
The attribute is relevant only for Canada and the United States of America. It equals to the state in these countries.

- addresses[home].postalCode
- addresses[home].country
- locale
- phoneNumbers[work].value
- phoneNumbers[mobile].value
- phoneNumbers[fax].value
- timeZone
- active

If the active parameter and its value are not present in the response, the user status is equivalent to the new status in Identity Authentication.

- displayName
- contactPreferenceEmail
- contactPreferenceTelephone
- industryCrm
- company
- companyRelationship
- department
- groups
- corporateGroups

This attribute is applicable for the corporate user store scenarios and contains the groups the user in the corporate user store is assigned to.

- mailVerified
- passwordStatus

Supported values: initial, enabled, and disabled.

- userType

Supported values: public, partner, customer, and employee.

- telephoneVerified

Supported values: true or false.
- telephoneVerificationAttempts
  
  **Note**
  
  telephoneVerificationAttempts can take values from 0 to 5 including.

- passwordPolicy
  
  **Note**
  
  Returns the URL of the valid password policy.

- passwordStatus
  
  **Note**
  
  Supported values: importedPassword, initial, enabled, and disabled.

- passwordFailedLoginAttempts
  
  **Note**
  
  passwordFailedLoginAttempts can take values from 0 to 5 including.

- otpFailedLoginAttempts
  
  **Note**
  
  otpFailedLoginAttempts can take values from 0 to 4 including.

- termsOfUse
  
  - timeOfAcceptance
  
  - name
  
  - id
  
  - locale
  
  - version

- privacyPolicy
  
  - timeOfAcceptance
  
  - name
  
  - id
  
  - locale
  
  - version

- socialIdentities
  
  **Note**
  
  Returns information about the social accounts that are linked to the user's account in Identity Authentication. Supported values: socialId, socialProvider, and dateOfLinking.

- passwordLoginTime

- loginTime

- passwordSetTime

**Enterprise User Schema Extension**
i Note
The values of the following attributes are returned when the Enterprise User Schema Extension is used.

- employeeNumber
- costCenter
- organization

i Note
Equals the company attribute from the Core schema.

- division
- department

i Note
Equals the department attribute from the Core schema.

- manager
  - value
  - $ref
  - displayName

i Note
Read only.

Custom Attributes Schema Extension

Administrators at Identity Authentication can store, read, create, and update customer specific data in up to 10 custom attributes via the SCIM API.

i Note
The values of the following attributes are returned when the Custom Attributes Schema Extension (urn:sap:cloud:scim:schemas:extension:custom:2.0:User) is used.

- attributes
  - name

  i Note
  name can take values from customAttribute1 to customAttribute10.

  - value

  i Note
  value must be a string with a maximum length of 256 characters.

The response does not contain the whole User resource object. It returns only the specified attributes here, as if you have limited the response to those attributes using the attributes query parameter. totalResults shows the total number of results matching the query.
Response Status and Error Codes

Success Codes

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
<th>Response Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK</td>
<td>Operation Successful</td>
</tr>
</tbody>
</table>

For more information about the general error codes that may be returned, see General Error Codes [page 395].

Parent topic: Manage Users SCIM REST API [page 336]

Related Information

User Resource [page 343]
Create User Resource [page 348]
Update User Resource [page 358]
Delete User Resource [page 368]
SCIM REST API [page 334]

1.7.2.5.1.2 User Resource

The user resource method of the SAP Cloud Platform Identity Authentication service implementation of the SCIM REST API protocol provides information on a known user.

**Note**

User resource is implemented as defined by the SCIM protocol.

Request

**URI:** https://<tenant ID>.accounts.ondemand.com/service/scim/Users/<id>

**HTTP Method:** GET

**Content-Type:** application/scim+json

**Authentication mechanisms:**
- Client certificate
- Basic authentication

**Request Parameters**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path</td>
<td>Yes</td>
<td>The current path parameter is id.</td>
</tr>
</tbody>
</table>

**Request Example**

```plaintext
Example
GET /service/scim/Users/P000000
```

**Response**

**Format**: application/scim+json

**Response**

The response contains user object with the following user attributes:

- meta
- userType
- id
- emails.value
- name.honorificPrefix
- name.givenName
- name.familyName
- name.middleName
- userName
- addresses[work].streetAddress
- addresses[work].locality

**i Note**

The attribute equals to city.

- addresses[work].region

**i Note**

The attribute is relevant only for Canada and the United States of America. It equals to the **state** in these countries.

- addresses[work].postalCode
- addresses[work].country
- addresses[home].streetAddress
- addresses[home].locality
- **addresses[home].region**

  *Note* The attribute equals to city.

- **addresses[home].country**

  *Note* The attribute is relevant only for Canada and the United States of America. It equals to the `state` in these countries.

- **locale**

- **phoneNumbers[work].value**

- **phoneNumbers[mobile].value**

- **phoneNumbers[fax].value**

- **timeZone**

- **active**

  *Note* If the `active` parameter and its value are not present in the response, the user status is equivalent to the `new` status in Identity Authentication.

- **displayName**

- **contactPreferenceEmail**

- **contactPreferenceTelephone**

- **industryCrm**

- **company**

- **companyRelationship**

- **department**

- **groups**

- **corporateGroups**

  *Note* This attribute is applicable for the corporate user store scenarios and contains the groups the user in the corporate user store is assigned to.

- **mailVerified**

- **passwordStatus**

  *Note* Supported values: `initial`, `enabled`, and `disabled`.

- **userType**

  *Note* Supported values: `public`, `partner`, `customer`, and `employee`.
- telephoneVerified

  **Note**
  Supported values: true or false.

- telephoneVerificationAttempts

  **Note**
  telephoneVerificationAttempts can take values from 0 to 5 including.

- passwordPolicy

  **Note**
  Returns the URL of the valid password policy.

- passwordStatus

  **Note**
  Supported values: importedPassword, initial, enabled, and disabled.

- passwordFailedLoginAttempts

  **Note**
  passwordFailedLoginAttempts can take values from 0 to 5 including.

- otpFailedLoginAttempts

  **Note**
  otpFailedLoginAttempts can take values from 0 to 4 including.

- termsOfUse
  - timeOfAcceptance
  - name
  - id
  - locale
  - version

- privacyPolicy
  - timeOfAcceptance
  - name
  - id
  - locale
  - version

- socialIdentities

  **Note**
  Returns information about the social accounts that are linked to the user’s account in Identity Authentication. Supported values: socialId, socialProvider, and dateOfLinking.
Enterprise User Schema Extension

The values of the following attributes are returned when the Enterprise User Schema Extension is used.

- employeeNumber
- costCenter
- organization

\[\text{iNote}\]
Equals the company attribute from the Core schema.

- division
- department

\[\text{iNote}\]
Equals the department attribute from the Core schema.

- manager
  - value
  - $ref
  - displayName

\[\text{iNote}\]
Read only.

Custom Attributes Schema Extension

Administrators at Identity Authentication can store, read, create, and update customer specific data in up to 10 custom attributes via the SCIM API.

\[\text{iNote}\]
The values of the following attributes are returned when the Custom Attributes Schema Extension (urn:sap:cloud:scim:schemas:extension:custom:2.0:User) is used.

- attributes
  - name

\[\text{iNote}\]
name can take values from customAttribute1 to customAttribute10.
i Note

value must be string with a maximum length of 256 characters.

Parent topic: Manage Users SCIM REST API [page 336]

Related Information

Users Search [page 337]
Create User Resource [page 348]
Update User Resource [page 358]
Delete User Resource [page 368]
SCIM REST API [page 334]

1.7.2.5.1.3  Create User Resource

The create user resource method of the Identity Authentication implementation of the SCIM REST API protocol provides information on the creation of a user.

i Note

Create user resource is implemented as defined by the SCIM protocol.

Request

URI: https://<tenant ID>.accounts.ondemand.com/service/scim/Users

HTTP Method: POST

Content-Type: application/scim+json

Authentication mechanisms:
- Client certificate
- Basic authentication

Supported Attributes
- emails.value

i Note

Only one value is supported.
sendMail

**iNote**
The parameter supports Boolean values `true` and `false` in String format. The default value is `true`. If you do not want to send an e-mail, the value should be passed with value `false`.

mailVerified

**iNote**
The parameter supports Boolean values `true` and `false` in String format. The default value is `false`.

**Possible Combinations**

<table>
<thead>
<tr>
<th>sendMail</th>
<th>mailVerified</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
<td>The user will receive e-mail. He or she will be able to log on.</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>The user will receive e-mail. He or she has to click the verification link in the e-mail.</td>
</tr>
<tr>
<td>false</td>
<td>true</td>
<td>The user will be able to log on to the application directly.</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
<td>The user will not be able to log on.</td>
</tr>
</tbody>
</table>

name.honorificPrefix

**iNote**
The characters `<`, `>`, `:` are not allowed for this attribute.

name.givenName

**iNote**
The characters `<`, `>`, `:` are not allowed for this attribute.

name.familyName

**iNote**
The characters `<`, `>`, `:` are not allowed for this attribute.

name.middleName

**iNote**
The characters `<`, `>`, `:` are not allowed for this attribute.

userName

$addresses[work].streetAddress$

$addresses[work].locality$

**iNote**
The attribute equals to `city`.

$addresses[work].region$
i Note
The attribute is relevant only for Canada and the United States of America. It equals to the state in these countries.

- addresses[work].postalCode
- addresses[work].country
- addresses[home].streetAddress
- addresses[home].locality

i Note
The attribute equals to city.

- addresses[home].region

i Note
The attribute is relevant only for Canada and the United States of America. It equals to the state in these countries.

- addresses[home].postalCode
- addresses[home].country
- locale
- password

i Note
If the attribute password is provided, user is prompted to change the password on first logon. passwordStatus will be initial as a default value.

- passwordStatus

i Note
If the attribute password is provided, user is prompted to change the password on first logon. passwordStatus will be initial as a default value.

- phoneNumbers[work].value
- phoneNumbers[mobile].value
- phoneNumbers[fax].value
- timeZone
- active

i Note
The parameter supports only Boolean values true and false in Boolean format. They are equivalent to the active and inactive status in Identity Authentication.

If the active parameter is not present in the request the user is created with a status new.

- displayName
i Note
The characters <, >, : are not allowed for this attribute.

- contactPreferenceEmail
- contactPreferenceTelephone
- industryCrm
- company
- companyRelationship

i Note
If the userType attribute is provided and has one of the values Customer, Employee, or Partner, the companyRelationship attribute value is overwritten and takes the same value as the userType attribute.

- department
- groups

i Note
It is possible to assign companyGroups to a user only if the groups are already existing.

- corporateGroups

i Note
This attribute is applicable for the corporate user store scenarios and contains the groups the user in the corporate user store is assigned to.

- sourceSystem
- userType

i Note
Supported values: public, partner, customer, and employee.

- telephoneVerified

i Note
Supported values: true or false.

- telephoneVerificationAttempts

i Note
telephoneVerificationAttempts can take values from 0 to 5 including.

- passwordPolicy

i Note
Returns the URL of the valid password policy.
- **passwordStatus**
  
  **i Note**
  
  **Supported values:** importedPassword, initial, enabled, and disabled.

- **passwordFailedLoginAttempts**
  
  **i Note**
  
  passwordFailedLoginAttempts can take values from 0 to 5 including.

- **otpFailedLoginAttempts**
  
  **i Note**
  
  otpFailedLoginAttempts can take values from 0 to 4 including.

- **newsletters**
  
  **i Note**
  
  A set of strings.

- **termsOfUse**
  
  - **timeOfAcceptance**
    
    **i Note**
    
    timeOfAcceptance should be in the format yyyy-MM-dd'T'HH:mm:ss'Z'.

    - name
    - id
    - locale
    - version

- **privacyPolicy**
  
  - **timeOfAcceptance**
    
    - name
    - id
    - locale
    - version

**Enterprise User Schema Extension**

- **i Note**
  
  The values of the following attributes are returned when the Enterprise User Schema Extension is used.

- **employeeNumber**
- **costCenter**
- **organization**

  **i Note**
  
  Equals the company attribute.
- division
- department

i Note
Equals the department attribute from the Core schema.

- manager
  - value

  i Note
  The id of the user's manager.

  i Note
  The resource URL of the manager.

  displayName

  i Note
  Read only.

Custom Attributes Schema Extension

Administrators at Identity Authentication can store, read, create and, update customer specific data in up to 10 custom attributes via the SCIM API.

i Note

The values of the following attributes are returned when the Custom Attributes Schema Extension (urn:sap:cloud:scim:schemas:extension:custom:2.0:User) is used.

- attributes
  - name

    i Note
    name can take values from customAttribute1 to customAttribute10.

  - value

    i Note
    value must be in a String format with a maximum length of 256 characters.
Create User Scenarios

The following scenarios are possible via the SCIM REST API:

<table>
<thead>
<tr>
<th>password</th>
<th>provided</th>
<th>provided</th>
<th>not provided</th>
</tr>
</thead>
<tbody>
<tr>
<td>passwordStatus</td>
<td>enabled</td>
<td>enabled</td>
<td>not provided</td>
</tr>
<tr>
<td>sendMail</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>mailVerified</td>
<td>false</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

**Result**

- **A new user will be created.**
  - The user will be able to log on. He or she will receive e-mail, but does not have to click a verification link in the e-mail.

- **Create a user that is provisioned from another system.**
  - The user will be able to log on. He or she will receive e-mail, but does not have to click a verification link in the e-mail.

- **Create a user that comes from the corporate user store.**
  - The user will be able to log on to the application directly.

---

**Request Example**

```json
{
  "userName": "johnsmith",
  "name": {
    "givenName": "John",
    "familyName": "Smith",
    "middleName": "Smith",
    "honorificPrefix": "Mr."
  },
  "emails": [{
    "value": "john.smith@sap.com"
  }],
  "addresses": [{
    "type": "work",
    "streetAddress": "100 Universal City Plaza",
    "locality": "Hollywood",
    "region": "CA",
    "postalCode": "91608",
    "country": "US"
  }, {
    "type": "home",
    "streetAddress": "456 Hollywood Blvd",
    "locality": "Hollywood",
    "region": "CA",
    "postalCode": "91608",
    "country": "US"
  }],
  "phoneNumbers": [{
    "value": "555-555-5555",
    "type": "work"
  }, {
```
The URI of the newly created user is in the location header of the HTTP Response.

Response Example

Example

Location: https://<tenant ID>.accounts.ondemand.com/service/users/P057607

Body:

{
  "schemas": [
    "urn:sap:cloud:scim:schemas:extension:custom:2.0:User"],
  "userName": "johnsmith",
  "id": "P057607",
  "meta": {
    "location": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P000000",
    "resourceType": "User",
    "version": "1.0",
    "created": "2013-06-18T13:05:51Z",
    "lastModified": "2015-08-21T11:19:50Z"
  },
  "name": {
    "givenName": "John",
    "familyName": "Smith"}
"familyName": "Smith",
"middleName": "Smith",
"honorificPrefix": "Mr.
"},
"emails": [{
"value": "john.smith@sap.com"
}]
"addresses": [{
"type": "work",
"streetAddress": "100 Universal City Plaza",
"locality": "Hollywood",
"region": "CA",
"postalCode": "91608",
"country": "US"
},
{"type": "home",
"streetAddress": "456 Hollywood Blvd",
"locality": "Hollywood",
"region": "CA",
"postalCode": "91608",
"country": "US"
}]
"phoneNumbers": [{
"value": "555-555-5555",
"type": "work"
},
{"value": "555-555-4444",
"type": "mobile"
},
{"value": "555-555-4444",
"type": "fax"
}]
"locale": "DE",
"timeZone": "Europe/Berlin",
"userType": "partner",
"mailVerified": "true",
"active": true,
"groups": [{
"value": "admin",
$ref": "https://<tenant ID>.accounts.ondemand.com/service/groups/55b87ab4e4b0fca00bbc070",
"displayName": "John Smith",
"contactPreferenceEmail": "yes",
"contactPreferenceTelephoneNumber": "no",
"industryCrm": "Consumer Products",
"company": "SFSF",
"department": "Administration",
"telephoneVerified": "true",
"termsOfUse": [{
"timeOfAcceptance": "2015-08-21T11:19:50Z",
"name": "ToU",
"id": "ToU",
"locale": "en_US",
"version": "1"
}]
"privacyPolicy": [{
"timeOfAcceptance": "2015-08-21T11:19:50Z",
"name": "PP",
"id": "b3452casd-8670-7341-945h-5e0288b9gee4",
"locale": "en_US",
"version": "1"}]}
The update user method of the implementation of the SCIM REST API protocol provides information on the update of a known user. The method does not create a new user.

**Note**

Update is provided only on the attributes with new values. The other attributes remain the same.
Request

URI: https://<tenant ID>.accounts.ondemand.com/service/scim/Users/<id>

HTTP Method: PUT

Content-Type: application/scim+json

Authentication mechanisms:

- Client certificate
- Basic authentication

Supported Attributes

Attributes are case sensitive and only the exact case should be used.

- **id**
  
  _Note_
  
  Attribute `id` is required in the request json and must match the path parameter `id`.

- **emails.value**
  
  _Note_
  
  Only one value is supported.

- **name.honorificPrefix**
- **name.givenName**
  
  _Note_
  
  The characters `<`, `>`, `:` are not allowed for this attribute.

- **name.familyName**
  
  _Note_
  
  The characters `<`, `>`, `:` are not allowed for this attribute.

- **name.middleName**
- **userName**
- **addresses[work].streetAddress**
- **addresses[work].locality**
  
  _Note_
  
  The attribute is relevant only for Canada and the United States of America. It equals to the `state` in these countries.

- **addresses[work].region**
  
  _Note_
  
  The attribute equals to city.
- addresses[work].postalCode
- addresses[work].country
- addresses[home].streetAddress
- addresses[home].locality

**i Note**
The attribute equals to city.

- addresses[home].region

**i Note**
The attribute is relevant only for Canada and the United States of America. It equals to the state in these countries.

- addresses[home].postalCode
- addresses[home].country
- locale
- phoneNumbers[work].value
- phoneNumbers[mobile].value
- phoneNumbers[fax].value
- timeZone
- active

**i Note**
If the active parameter and its value are not present in the request, this means that the user status remains unchanged.

- displayName

**i Note**
The characters <, >, : are not allowed for this attribute.

- contactPreferenceEmail
- contactPreferenceTelephone
- industryCrm
- company
- companyRelationship

**i Note**
If the userType attribute is provided and has one of the values Customer, Employee, or Partner, the companyRelationship attribute value is overwritten and takes the same value as the userType attribute.
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>companyGroups</strong></td>
<td>It is possible to assign <code>companyGroups</code> to a user only if the groups are already existing.</td>
</tr>
<tr>
<td><strong>corporateGroups</strong></td>
<td>This attribute is applicable for the corporate user store scenarios and contains the groups the user in the corporate user store is assigned to. The following options are possible:</td>
</tr>
<tr>
<td></td>
<td>- If the attribute <code>corporateGroups</code> is provided with a specific value, this value will overwrite the previous one.</td>
</tr>
<tr>
<td></td>
<td>- If the attribute <code>corporateGroups</code> is not provided, this previous value of the attribute will be preserved.</td>
</tr>
<tr>
<td></td>
<td>- If the attribute <code>corporateGroups</code> is provided without a value, the previous value will be deleted.</td>
</tr>
<tr>
<td><strong>password</strong></td>
<td>If attribute <code>password</code> is provided the password will be changed.</td>
</tr>
<tr>
<td><strong>passwordStatus</strong></td>
<td>If the <code>password</code> attribute is provided the <code>passwordStatus</code> can be set to enabled or initial. When this attribute is provided the <code>password</code> attribute is a required parameter.</td>
</tr>
<tr>
<td><strong>userType</strong></td>
<td>Supported values: <code>public</code>, <code>partner</code>, <code>customer</code>, and <code>employee</code>.</td>
</tr>
<tr>
<td><strong>sendMail</strong></td>
<td>The parameter supports Boolean values <code>true</code> and <code>false</code> in String format. The default value is <code>true</code>. If you do not want to send an e-mail, the value should be passed with value <code>false</code>.</td>
</tr>
</tbody>
</table>
• **mailVerified**

  **i Note**
  The parameter supports Boolean values `true` and `false` in String format. The default value is `false`.

  **Possible Combinations**

<table>
<thead>
<tr>
<th>sendMail</th>
<th>mailVerified</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
</tr>
</tbody>
</table>

  **Result**
  - The user will receive e-mail. He or she will be able to log on.
  - The user will receive e-mail. He or she has to click the verification link in the e-mail.
  - The user will be able to log on to the application directly.
  - The user will not be able to log on.

• **telephoneVerified**

  **i Note**
  Supported values: `true` or `false`.

• **telephoneVerificationAttempts**

  **i Note**
  TelephoneVerificationAttempts can take values from 0 to 5 including.

• **passwordPolicy**

  **i Note**
  Returns the URL of the valid password policy.

• **passwordStatus**

  **i Note**
  Supported values: `importedPassword`, `initial`, `enabled`, and `disabled`.

• **passwordFailedLoginAttempts**

  **i Note**
  PasswordFailedLoginAttempts can take values from 0 to 5 including.

• **otpFailedLoginAttempts**

  **i Note**
  OtpFailedLoginAttempts can take values from 0 to 4 including.

• **termsOfUse**

  - **timeOfAcceptance**
Enterprise User Schema Extension

**i Note**

The values of the following attributes are returned when the Enterprise User Schema Extension is used.

- employeeNumber
- costCenter
- organization

**i Note**

Equals the company attribute from the Core schema.

- division
- department

**i Note**

Equals the department attribute from the Core schema.

- manager
  - value
  - $ref
  - displayName

Custom Attributes Schema Extension

**i Note**

Read only.
Administrators at Identity Authentication can store, read, create and, update customer specific data in up to 10 custom attributes via the SCIM API.

**Note**

The values of the following attributes are returned when the Custom Attributes Schema Extension (urn:sap:cloud:scim:schemas:extension:custom:2.0:User) is used.

- **attributes**
  - **name**
    - **Note**
      - name can take values from customAttribute1 to customAttribute10.
  - **value**
    - **Note**
      - value must be string with a maximum length of 256 characters.

      If you provide empty value, it will delete the attribute if it already exists.

      If you provide an empty list of attributes, the custom attributes that are already set will be deleted.

**Request Example**

```json
{
  "userName": "johnsmith",
  "id": "P000000",
  "name": {
    "givenName": "John",
    "familyName": "Smith",
    "middleName": "Smith",
    "honorificPrefix": "Mr."
  },
  "emails": [{
    "value": "john.smith@sap.com"
  }],
  "addresses": [{
    "type": "work",
    "streetAddress": "100 Universal City Plaza",
    "locality": "Hollywood",
    "region": "CA",
    "postalCode": "91608",
    "country": "US"
  }, {
    "type": "home",
    "streetAddress": "456 Hollywood Blvd",
    "locality": "Hollywood",
    "region": "CA",
    "postalCode": "91608",
    "country": "US"
  }],
}
"phoneNumbers": [{
  "value": "555-555-5555",
  "type": "work"
}, {
  "value": "555-555-4444",
  "type": "mobile"
}, {
  "value": "555-555-4444",
  "type": "fax"
}],
"locale": "DE",
"timeZone": "Europe/Berlin",
"userType": "partner",
"active": true,
"groups": [{
  "value": "admin"
}]
],
"displayName": "John Smith",
"contactPreferenceEmail": "yes",
"contactPreferenceTelephone": "no",
"industryCrm": "Consumer Products",
"companyRelationship": "Partner",
"company": "SFSF",
"department": "Administration",
"password": "Abcd1234",
"passwordStatus": "enabled",
"sendMail": "false",
"mailVerified": "true",
"telephoneVerified": "true",
"termsOfUse": [{
  "timeOfAcceptance": "2015-08-21T11:19:50Z",
  "name": "ToU",
  "id": "ToU",
  "locale": "en_US",
  "version": "1"
}]
],
"privacyPolicy": [{
  "timeOfAcceptance": "2015-08-21T11:19:50Z",
  "name": "PP",
  "id": "b3452casd-8670-7341-945h-5e0288b9gee4",
  "locale": "en_US",
  "version": "1"
}]
],
"corporateGroups": [
  { "value": "admin"
}]
],
  "employeeNumber": "JohnS",
  "costCenter": "costCenter",
  "organization": "SFSF",
  "division": "Finance",
  "department": "Administration",
  "manager": {
    "value": "P999913",
    "$ref": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P999913"
  }
}
Response

Format: application/scim+json

Response Status Code

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
<th>Response Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK</td>
<td>Operation successful</td>
</tr>
</tbody>
</table>

**Note**

Response code is **400 Bad Request** if user with id provided in the value attribute of the manager attribute from the enterprise schema does not exist.

For more information about the general error codes that may be returned, see General Error Codes [page 395].

Response Example

```json
{
  "schemas": [
    "urn:sap:cloud:scim:schemas:extension:custom:2.0:User"],
  "userName": "johnsmith",
  "meta": {
    "location": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P000000",
    "resourceType": "User",
    "version": "1.0",
    "created": "2013-06-18T13:05:51Z",
    "lastModified": "2015-08-21T11:19:50Z"
  },
  "id": "P000000",
  "attributes": [
    {"name": "customAttribute1", "value": "Home Address2"},
    {"name": "customAttribute2", "value": "Telephone2"}
  ]
}
```
The delete user resource method of the Identity Authentication implementation of the SCIM REST API protocol allows you to delete an existing user. Delete user resource is implemented as defined by the System for Cross-domain Identity Management (SCIM) protocol.
**Request**

**URI:** https://<tenant ID>.accounts.ondemand.com/service/scim/Users/<id>

**HTTP Method:** DELETE

**Content-Type:** application/scim+json

**Authentication mechanisms:**
- Client certificate
- Basic authentication

**Response Status Code**

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
<th>Response Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>204</td>
<td>No Content</td>
<td>User is successfully deleted.</td>
</tr>
</tbody>
</table>

**Note**

Response code if user does not exist is **404 Not Found**. When user resource is deleted, it is not possible to get information about it via a GET request.

For more information about the general error codes that may be returned, see [General Error Codes](page 395).

**Parent topic:** Manage Users SCIM REST API [page 336]

**Related Information**

- Users Search [page 337]
- User Resource [page 343]
- Create User Resource [page 348]
- Update User Resource [page 358]
- SCIM REST API [page 334]

**1.7.2.5.2 Manage Groups SCIM REST API**

- **Groups Search** [page 370]
  The group search method of the Identity Authentication implementation of the SCIM REST API protocol allows you to perform a request for group search. Group search is implemented as defined by the System for Cross-domain Identity Management (SCIM) protocol.

- **Group Resource** [page 373]
  The group resource method of the SAP Cloud Platform Identity Authentication service implementation of the SCIM REST API protocol provides information on a known group.
The create group resource method of the Identity Authentication implementation of the SCIM REST API protocol provides information on the creation of a user group.

The update group method of the Identity Authentication implementation of the SCIM REST API protocol provides information on the update of an existing group. The method does not create a new group.

The delete group resource method of the Identity Authentication implementation of the SCIM REST API protocol allows you to delete an existing group. Delete group resource is implemented as defined by the System for Cross-domain Identity Management (SCIM) protocol.

Related Information

SCIM REST API [page 334]

1.7.2.5.2.1 Groups Search

The group search method of the Identity Authentication implementation of the SCIM REST API protocol allows you to perform a request for group search. Group search is implemented as defined by the System for Cross-domain Identity Management (SCIM) protocol.

Request

URI: https://<tenant ID>.accounts.ondemand.com/service/scim/Groups

HTTP Method: GET

Authentication mechanisms:
- Client certificate
- Basic authentication

Request Headers

<table>
<thead>
<tr>
<th>Header</th>
<th>Required</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td>application/scim+json</td>
</tr>
</tbody>
</table>

Request Parameters
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>No</td>
<td>Paginates the response. Represents the number of items which will be returned per page. The maximum number of items returned per page is limited to 100.</td>
</tr>
<tr>
<td>startIndex</td>
<td>No</td>
<td>Paginates the response. Represents the start index from which the results are returned.</td>
</tr>
</tbody>
</table>

**i Note**
If you have more than 100 user, and you want to get the full list, you have to perform multiple requests.

**Request Example**
GET /service/scim/Groups?count=10&startIndex=1
Content-Type: application/scim+json

**Response**

**Response Status and Error Codes**

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK</td>
<td>Lists all the groups in a tenant.</td>
</tr>
</tbody>
</table>

For more information about the general error codes that may be returned, see [General Error Codes](#) [page 395].

**Response Example**

```json
{
   "schemas": [
      "urn:ietf:params:scim:schemas:core:2.0:Group",
      "urn:sap:cloud:scim:schemas:extension:custom:2.0:Group"
   ],
   "totalResults": 2,
   "itemsPerPage": 2,
   "startIndex": 1,
   "Resources" : [ {
      "id": "57aadecee4b0c8e9241d1635",
      "displayName": "New Administrators",
      "schemas": [ "urn:ietf:params:scim:schemas:core:2.0:Group",
      "urn:sap:cloud:scim:schemas:extension:custom:2.0:Group"
   ]
}```
"members": [
  {
    "value": "P000001",
    "$ref": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P000001",
    "display": "Dona Moore"
  },
  {
    "value": "P000002",
    "$ref": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P000002",
    "display": "Michael Adams"
  },
],
"urn:sap:cloud:scim:schemas:extension:custom:2.0:Group": {  
  "name": "Administrators",
  "description": "Group Administrators description."
},
"meta": {
  "location": "https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/57aadecee4b0c8e9241d1635",
  "resourceType": "Group",
  "version": "1.0"
}
},
{
  "id": "35asdfqaass50s8r8751d1721",
  "displayName": "Managers",
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:Group",
    "urn:sap:cloud:scim:schemas:extension:custom:2.0:Group"
  ],
  "members": [
    {
      "value": "P000001",
      "$ref": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P000001",
      "display": "Dona Moore"
    },
    {
      "value": "P000002",
      "$ref": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P000002",
      "display": "Michael Adams"
    }
  ],
  "urn:sap:cloud:scim:schemas:extension:custom:2.0:Group": {  
    "name": "Managers"
  },
  "meta": {
    "location": "https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/35asdfqaass50s8r8751d1721",
    "resourceType": "Group",
    "version": "1.0"
  }
}]

Parent topic: Manage Groups SCIM REST API [page 369]

Related Information

Group Resource [page 373]
1.7.2.5.2.2 Group Resource

The group resource method of the SAP Cloud Platform Identity Authentication service implementation of the SCIM REST API protocol provides information on a known group.

**i Note**

Group resource is implemented as defined by the SCIM protocol.

**Prerequisites:**

You have the `id` of the group whose resource you want to get.

**i Note**

To get the `id` of the group, list all the groups in the tenant and copy the `id` of the group whose resource you want to get. For more information, see Groups Search [page 370].

**Request**

**URI:** https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/<id of the group>

**HTTP Method:** GET

**Authentication mechanisms:**

- Client certificate
- Basic authentication

**Request Headers**

<table>
<thead>
<tr>
<th>Header</th>
<th>Required</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td>application/scim+json</td>
</tr>
</tbody>
</table>

**Request Example**

```
GET /service/scim/Groups/<id of the group>
Content-Type: application/scim+json
```
Response

Response Status and Error Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK</td>
<td>List details for a specific group in a tenant of Identity Authentication.</td>
</tr>
</tbody>
</table>

For more information about the general error codes that may be returned, see General Error Codes [page 395].

Response Example

```json

Example

```{"id": "57aadecee4b0c8e9241d1635", "displayName": "Identity Authentication Admins", "schemas": [
"urn:ietf:params:scim:schemas:core:2.0:Group",
"urn:sap:cloud:scim:schemas:extension:custom:2.0:Group"
],
"urn:sap:cloud:scim:schemas:extension:custom:2.0:Group": {
"name": "Administrators"
},
"meta": {
"location": "https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/57aadecee4b0c8e9241d1635",
"resourceType": "Group",
"version": "1.0"
},
"members": [{
"value": "P000001",
"$ref": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P000001",
"display": "Dona Moore"
}]
}
```

Parent topic: Manage Groups SCIM REST API [page 369]

Related Information

- Groups Search [page 370]
- Create Group Resource [page 375]
- Update Group Resource [page 377]
- Delete Group Resource [page 380]
- SCIM REST API [page 334]
1.7.2.5.2.3 Create Group Resource

The create group resource method of the Identity Authentication implementation of the SCIM REST API protocol provides information on the creation of a user group.

**Note**

Create group resource is implemented as defined by the System for Cross-domain Identity Management (SCIM) protocol.

### Request

**URI:** https://<tenant ID>.accounts.ondemand.com/service/scim/Groups

**HTTP Method:** POST

**Authentication mechanisms:**
- Client certificate
- Basic authentication

**Request Headers**

<table>
<thead>
<tr>
<th>Header</th>
<th>Required</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td>application/scim+json</td>
</tr>
</tbody>
</table>

**Request Attributes**

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Required</th>
<th>Data Type</th>
<th>Description</th>
<th>Parameter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>displayName</td>
<td>Yes</td>
<td>String</td>
<td>Human readable name for the group.</td>
<td>Request body</td>
</tr>
<tr>
<td>name</td>
<td>No</td>
<td>String</td>
<td>The name of the group.</td>
<td>Request body</td>
</tr>
</tbody>
</table>

**Note**

If `name` is missing, `displayName` is taken as the name of the group.

**Remember**

The name must be unique within the Identity Authentication tenant.

**Restriction**

The name can contain lower-case Latin characters (a-z), upper-case Latin characters (A-Z), base 10 digits (0-9), hyphens, and underscores.
<table>
<thead>
<tr>
<th>Attributes</th>
<th>Required</th>
<th>Data Type</th>
<th>Description</th>
<th>Parameter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>No</td>
<td>String</td>
<td>Description for the group.</td>
<td>Request body</td>
</tr>
<tr>
<td>members</td>
<td>No</td>
<td>Complex</td>
<td>The members of the group. Use it to assign users to the group at the creation of the group.</td>
<td>Request body</td>
</tr>
</tbody>
</table>

**Request Example**

```json
POST /service/scim/Groups
Content-Type: application/scim+json
{
  "displayName": "Identity Authentication Administrators",
  "urn:sap:cloud:scim:schemas:extension:custom:2.0:Group": {
    "name": "Administrators",
    "description": "Group Administrators description"
  },
  "members": [
    {
      "value": "P000001"
    }
  ]
}
```

**Response**

**Response Status and Error Codes**

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Created</td>
<td>Indicates success.</td>
</tr>
<tr>
<td>409</td>
<td>Conflict</td>
<td>The group cannot be created, because a group with the same name already exists.</td>
</tr>
</tbody>
</table>

For more information about the general error codes that may be returned, see [General Error Codes](#page 395).

**Response Example**

```json
{
  "id": "57aadecee4b0c8e9241d1635",
  "displayName": "Administrators",
  "schemas": [
    "urn:ietf:params:scim:schemas:core:2.0:Group",
    "urn:sap:cloud:scim:schemas:extension:custom:2.0:Group"
  ],
  "members": [
    {
      "value": "P000001",
    }
  ]
}
```
The update group method of the Identity Authentication implementation of the SCIM REST API protocol provides information on the update of an existing group. The method does not create a new group.

**Note**

Update group resource is implemented as defined by the System for Cross-domain Identity Management (SCIM) protocol.

**Prerequisites:**

You have the id of the group whose resource you want to update.

**Note**

To get the id of the group, list all the groups in the tenant and copy the id of the group whose resource you want to get. For more information, see Groups Search [page 370].
Request

URI: https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/<id of the group>

HTTP Method: PUT

Authentication mechanisms:
- Client certificate
- Basic authentication

Request Headers

<table>
<thead>
<tr>
<th>Header</th>
<th>Required</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td>application/scim+json</td>
</tr>
</tbody>
</table>

Request Attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Required</th>
<th>Data Type</th>
<th>Description</th>
<th>Parameter Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Yes</td>
<td>String</td>
<td>The id of the group whose resource you want to update.</td>
<td>Request body</td>
</tr>
<tr>
<td>displayName</td>
<td>Yes</td>
<td>String</td>
<td>Use it to change the human readable name for the group.</td>
<td>Request Body</td>
</tr>
<tr>
<td>members</td>
<td>No</td>
<td>Complex</td>
<td>Use it to assign users to the group.</td>
<td>Request Body</td>
</tr>
</tbody>
</table>

Remember

Only the users that are included in the request will be assigned to the group.

To assign new users to the group, and at the same time keep the existing users assigned, include both the new and existing users in the request.

If the members attribute is missing all the users will be unassigned from the group.

Caution

Make sure that the id of the group in the URI and the id of the group in the request body match. If they differ, the system returns 400 Bad Request with the Mismatched group id message.
### Request Example

```json
{
   "id": "<id of the group>",
   "displayName": "New Administrators",
   "members": [
      {
         "value": "P000001"
      },
      {
         "value": "P000002"
      }
   ]
}
```

### Response

#### Response Status and Error Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK</td>
<td>Operation successful</td>
</tr>
</tbody>
</table>

For more information about the general error codes that may be returned, see [General Error Codes](#page 395).

**i Note**

The `display` attribute returns the name of the user that is assigned to the group.

#### Response Example

#### Example

```json
{
   "id": "57aadecee4b0c8e9241d1635",
   "displayName": "New Administrators",
   "schemas": [
      "urn:ietf:params:scim:schemas:core:2.0:Group",
      "urn:sap:cloud:scim:schemas:extension:custom:2.0:Group"
   ],
   "members": [
      {
         "value": "P000001",
         "$ref": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P000001",
         "display": "Dona Moore"
      },
      {
         "value": "P000002",
         "$ref": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P000002",
         "display": "Michael Adams"
      }
   ],
   "urn:sap:cloud:scim:schemas:extension:custom:2.0:Group": {
      "name": "Administrators"
   },
   "meta": {
```
1.7.2.5.2.5 Delete Group Resource

The delete group resource method of the Identity Authentication implementation of the SCIM REST API protocol allows you to delete an existing group. Delete group resource is implemented as defined by the System for Cross-domain Identity Management (SCIM) protocol.

Prerequisites:
You have the id of the group whose resource you want to delete.

iNote
To get the id of the group, list all the groups in the tenant and copy the id of the group whose resource you want to get. For more information, see Groups Search [page 370].

Request

URI: https://<tenant ID>.accounts.ondemand.com/service/scim/Groups/<id of the group>

HTTP Method: DELETE

Authentication mechanisms:
- Client certificate
- Basic authentication
Request Headers

<table>
<thead>
<tr>
<th>Header</th>
<th>Required</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content-Type</td>
<td>Yes</td>
<td>application/scim+json</td>
</tr>
</tbody>
</table>

i Note

The delete group resource method removes the user group and unassigns all users from them.

When group resource is deleted, it is not possible to get information about it via a GET request.

If selected groups are used in Risk-Based Authentication or Conditional Authentication rules, then these rules may not work as expected after deletion.

Request Example

DELETE /service/scim/Groups/<id of the group>
Content-Type: application/scim+json

Response

Response Status and Error Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>204</td>
<td>No Content</td>
<td>Group is successfully deleted.</td>
</tr>
<tr>
<td>404</td>
<td>Not Found</td>
<td>The group does not exist</td>
</tr>
</tbody>
</table>

For more information about the general error codes that may be returned, see General Error Codes [page 395].

Parent topic: Manage Groups SCIM REST API [page 369]

Related Information

Groups Search [page 370]
Group Resource [page 373]
Create Group Resource [page 375]
Update Group Resource [page 377]
1.7.2.6 Change Tenant Texts REST API

The Change Tenant Texts REST API of SAP Cloud Platform Identity Authentication service can be used to change the predefined texts and messages for end-user screens available per tenant in the Identity Authentication.

Prerequisites

To call the methods of this Change Tenant Texts REST API you must have a system as administrator (T user) with an assigned Manage Tenant Configuration role. For more details about how to add a system as administrator and assign administrator roles, see Add System as Administrator [page 240], and Edit Administrator Authorizations [page 241].

Usage

The predefined tenant texts are stored in the tenant_texts.properties file which can be downloaded from: Tenant Texts. The file contains configurable parameters stored as key value pairs of strings. Each key stores the name of a parameter, and the corresponding value is the text that can be changed and updated. The keys are self-explanatory and show where the texts are used. For example, the logon.ui.label.user=E-Mail key value pair is for the type of information that the user must provide to log on to the application. In this case, this is the E-Mail.

Depending on your requirements, you can:
Use the **GET** method to obtain the texts that overwrote part of the predefined tenant texts when your custom tenant was created, change the texts that you want, add them to the **POST** request and upload them.

Use the **GET** method to obtain the texts that overwrote part of the predefined tenant texts when your custom tenant was created, delete a key value pair, add the texts without this line to the **POST** request and upload them. This will replace the deleted key value pair with the predefined one.

Download the `tenant_texts.properties` file from the link, use the **GET** method to obtain the texts that overwrote part of the predefined tenant texts when your custom tenant was created, from the downloaded file copy the key value pairs that were not included in the response, change the texts in the copied key value pairs, add these new key value pairs to the **POST** request, and execute it.

Download the `tenant_texts.properties` file, copy it to the **POST** request, and execute it. This will replace all texts in the tenant with the predefined ones.

### Methods

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>See</th>
<th>URI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GET</strong></td>
<td><strong>GET Tenant Texts</strong> [page 383]</td>
<td><code>https://&lt;tenant ID&gt;.accounts.ondemand.com/service/resource?resourceType=RESOURCE_I18N_BUNDLE&amp;locale=&lt;value&gt;</code></td>
</tr>
<tr>
<td><strong>POST</strong></td>
<td><strong>POST Tenant Texts</strong> [page 386]</td>
<td><code>https://&lt;tenant ID&gt;.accounts.ondemand.com/service/resource/SAP_DEFAULT</code></td>
</tr>
</tbody>
</table>

**iNote**

`Tenant ID` is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with an URL in it. This URL contains the `tenant ID`.

### 1.7.2.6.1 GET Tenant Texts

Download the texts that overwrote part of the predefined tenant texts when your custom tenant was created.

#### Request

URI: `https://<tenant ID>.accounts.ondemand.com/service/resource?resourceType=RESOURCE_I18N_BUNDLE&locale=<value>`

HTTP Method: **GET**

Content-Type: application/json
Permissio ns: You must have a system as administrator (T user) with an assigned Manage Tenant Configuration role. For more details about how to add a system as administrator and assign administrator roles, see Add System as Administrator [page 240], and Edit Administrator Authorizations [page 241].

URL Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>setId</td>
<td>No</td>
<td>The identifier of the scenario that the resource is related to.</td>
<td>The default value is SAP_DEFAULT</td>
</tr>
<tr>
<td>resourceType</td>
<td>Yes</td>
<td>The type of the resource.</td>
<td>Use RESOURCE_I18N_BUNDLE</td>
</tr>
<tr>
<td>locale</td>
<td>Yes</td>
<td>The locale of the resource.</td>
<td>The default languages are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Chinese (zh_CN)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Dutch (nl)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● English (en)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● French (fr)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● German (de)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Hebrew (iw)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Italian (it)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Japanese (ja)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Korean (ko)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Polish (pl)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Portuguese (pt)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Russian (ru)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Spanish (es)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Welsh (cy)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Swedish (sv)</td>
</tr>
</tbody>
</table>

Request Example

GET /service/resource?resourceType=RESOURCE_I18N_BUNDLE&locale=en

Response

Response Status and Error Codes

Success Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK</td>
<td>The request was successful.</td>
</tr>
</tbody>
</table>

Error Codes

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>Bad Request</td>
<td>Validate JSON data. Validate that the special characters are escaped properly and new lines are added.</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized</td>
<td>The client is not authenticated.</td>
</tr>
<tr>
<td>Response Code</td>
<td>Meaning</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>403</td>
<td>Forbidden</td>
<td>Access to the resource is denied.</td>
</tr>
<tr>
<td>404</td>
<td>Not Found</td>
<td>The requested resource cannot be found.</td>
</tr>
<tr>
<td>405</td>
<td>Method Not Allowed</td>
<td>The requested method is not supported for the given resource.</td>
</tr>
<tr>
<td>415</td>
<td>Unsupported Media Type</td>
<td>The REST service does not support the API version requested by the REST client.</td>
</tr>
<tr>
<td>500</td>
<td>Internal Server Error</td>
<td>The operation cannot be completed due to a service error.</td>
</tr>
<tr>
<td>503</td>
<td>Service Unavailable</td>
<td>The service is currently unavailable.</td>
</tr>
</tbody>
</table>

**Response Example**

```
registerSuccess.thankyou=Thank you for registering with {0}
registerForm.validation.accept.privacy.statement=To accept the privacy statement, click the box above
registerSuccess.activateAccount=To activate your account, click the link contained in the e-mail. Note that it might take a few minutes for the e-mail to reach your inbox.
accountActivation.ui.label.activationsuccesstext=Thank you for registering and activating your account
accountActivation.ui.label.activationtext=This account can also be used to access other applications
createForgottenPasswordMail.user=E-Mail
logon.ui.label.user=E-Mail
profileManagement.socialSignOn.unlinkWarning=Choose "Unlink" to remove your social logon information from your account. You can re-link your account the next time you log on with a social sign-on-enabled site.
accountActivation.ui.label.notlinkedtext=Your account does not currently use social sign-on. To link your account with a social sign-on account, click one of the social network buttons next time you log on.
profileManagement.socialSignOn.nolinktext=Your account does not currently use social sign-on. To link your account with a social sign-on provider, click one of the social network buttons next time you log on.
linkSocialSignOnAccount.headline=Link your account with {0}
linkSocialSignOnAccount.message.profile=Profile Page
linkSocialSignOnAccount.message=As a final step, you can either link an existing account to your {0} account, or create a new account that will be linked to your {0} account.
logon.ui.tooltip.SOCIAL_NOT_ALLOWED=The site you are attempting to access requires your password. Enter your password and click Continue.
oauth.network=The selected social sign-on service is currently unavailable. Use a different social sign-on or your credentials to log on.
logon.ui.tooltip.MISSING_GOOGLE_PLUS_PROFILE=This Google account has not joined Google yet. Join Google and link your account, or log on with an existing account.
general.auth.request.error=Identity Provider could not process the authentication request received. Delete your browser cache and stored cookies, and restart your browser. If you still experience issues after doing this, please contact your administrator.
```
1.7.2.6.2 POST Tenant Texts

Update the tenant texts.

⚠️ Caution
Make sure that you have removed the comment lines and applied the proper escaping in your POST request. The comment lines are introduced by the # (number or hash) sign.

You should add \n at the end of each line in the data property content.

<table>
<thead>
<tr>
<th>Escape Sequences</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backspace (ascii code 08)</td>
<td>\b</td>
</tr>
<tr>
<td>Form feed (ascii code 0C)</td>
<td>\f</td>
</tr>
<tr>
<td>New line</td>
<td>\n</td>
</tr>
<tr>
<td>Carriage return</td>
<td>\r</td>
</tr>
<tr>
<td>Tab</td>
<td>\t</td>
</tr>
<tr>
<td>Double quote</td>
<td>&quot;</td>
</tr>
<tr>
<td>Backslash character</td>
<td>\</td>
</tr>
</tbody>
</table>

Tip
Instead of editing the request manually, you can use an on-line tool for converting a normal string into a quoted one.

Request

**URI:** https://<tenant ID>.accounts.ondemand.com/service/resource/SAP_DEFAULT

**HTTP Method:** POST

**Content-Type:** application/json

**Permissions:** You must have a system as administrator (T user) with an assigned Manage Tenant Configuration role. For more details about how to add a system as administrator and assign administrator roles, see Add System as Administrator [page 240], and Edit Administrator Authorizations [page 241].

**Request Example**

```json
[
  {
    "resourceType": "RESOURCE_I18N_BUNDLE",
    "locale": "en",
    "contentType": "text/html;charset=UTF-8"
  }
]
```
"data": "registerSuccess.thankyou=Thank you for registering with {0}\nregisterForm.validation.accept.privacy.statement=To accept the privacy\nstatement, click the box above\nregisterSuccess.activateAccount=To activate your account, click the link\ncontained in the e-mail. Note that it might take a few minutes for the e-mail to\oreach your inbox.\naccountActivation.ui.label.activationsuccesstext=Thank you for registering and\nactivating your account\naccountActivation.ui.label.activationtext=\ncreateForgottenPasswordMail.user=E-Mail\nlogon.ui.label.user=E-Mail\nlogon.ui.label.forgotpassword=Forgot/Reset Password\nprofileManagement.socialSignOn.unlinkWarning=Choose "Unlink" to remove your\nsocial logon information from your account. You can re-link your account the\next time you log on with a social sign-on-enabled site.\naccountActivation.ui.label.notlinkedtext=Your account does not currently use\nsocial sign-on. To link your account with a social sign-on account, click one of\nthe social network buttons next time you log on.\nprofileManagement.socialSignOn.nolinktext=Your account does not currently use\nsocial sign-on. To link your account with a social sign-on provider, click one\nof the social network buttons next time you log on.\nlinkSocialSignOnAccount.headline=Link your account with {0}\nlinkSocialSignOnAccount.message.profile=Profile Page\nlinkSocialSignOnAccount.message=As a final step, you can either link an existing\naccount to your {0} account, or create a new account that will be linked to your\n{0} account.\nlogon.ui.tooltip.SOCIAL_NOT_ALLOWED=The site you are attempting to access\nrequires your password. Enter your password and click Continue.\n.oauth.network=The selected social sign-on service is currently unavailable. Use\na different social sign-on or your credentials to log on.\nlogon.ui.tooltip.MISSING_GOOGLE_PLUS_PROFILE=This Google account has not joined\nGoogle yet. Join Google and link your account, or log on with an existing\naccount.\ngeneral.auth.request.error=Identity Provider could not process the\nauthentication request received. Delete your browser cache and stored cookies,\nand restart your browser. If you still experience issues after doing this,\nplease contact your administrator.\n
Response

Response Status and Error Codes

Success Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>The request was successful.</td>
<td>OK</td>
</tr>
</tbody>
</table>

Error Codes

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>Bad Request</td>
<td>Validate JSON data. Validate that the special characters are escaped properly and new lines are added.</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized</td>
<td>The client is not authenticated.</td>
</tr>
<tr>
<td>403</td>
<td>Forbidden</td>
<td>Access to the resource is denied.</td>
</tr>
</tbody>
</table>
### 1.7.2.7 Change Master Data Texts REST API

The Change Master Data Texts REST API can be used to change the predefined master data for each resource in Identity Authentication.

#### Prerequisites

To call the methods of this Change Master Data Texts REST API you must have a system as administrator (T user) with an assigned Manage Tenant Configuration role. For more details about how to add a system as administrator and assign administrator roles, see Add System as Administrator [page 240], and Edit Administrator Authorizations [page 241].

#### Usage

The predefined master data represents records in Identity Authentication that contain all relevant system data about a resource (Salutations, Functions, Departments, Company Relationships, Industries, Languages, Countries). That data can be used by the system for different classifications in the organization, for example, job titles, departments, or countries. The predefined master data texts are stored in properties files which can be downloaded from the links in the table below.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Link</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Salutations</td>
<td>Salutations</td>
<td>Key value pairs with a predefined set of honorifics.</td>
</tr>
<tr>
<td>Resource</td>
<td>Link</td>
<td>Notes</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Functions</td>
<td>Functions</td>
<td>Key value pairs with a predefined set of job titles.</td>
</tr>
<tr>
<td>Departments</td>
<td>Departments</td>
<td>Key value pairs with a predefined set of departments.</td>
</tr>
<tr>
<td>Company Relationships</td>
<td>Relationships</td>
<td>Key value pairs with a predefined set of business entities, such as customer, partner, employee.</td>
</tr>
<tr>
<td>Industries</td>
<td>Industries</td>
<td>Key value pairs with a predefined set of industries.</td>
</tr>
<tr>
<td>Languages</td>
<td>Languages</td>
<td>Key value pairs with a predefined set of languages.</td>
</tr>
<tr>
<td>Countries</td>
<td>Countries</td>
<td>Key value pairs with a predefined set of countries.</td>
</tr>
</tbody>
</table>

The files contain configurable parameters stored as key value pairs of strings. Each key stores the unified key of the resource, and the corresponding value is the unified value of the resource that can be changed and updated.

The example below shows the customized values of the *Functions* file. The dropdown list in the *Job Function* field on the *Registration* form shows the new values that have overwritten the predefined texts in the file.
Depending on your requirements, you can:

- Use the **GET** method to obtain the texts that you have already overwritten in the predefined master data texts, change the texts that you want, add them to the **POST** request and upload them.
- Use the **GET** method to obtain the texts that you have already overwritten in the predefined master data texts, delete a key value pair, add the texts without this line to the **POST** request and upload them. This will replace the deleted key value pair with the predefined one.
- Download the respective **properties** file from the link in the table, use the **GET** method to obtain the texts that overwrote part of the predefined master data texts when your custom tenant was created, from the downloaded file copy the key value pairs that were not included in the response, change the texts in the copied key value pairs, add these new key value pairs to the **POST** request, and execute it.
- Download the respective **properties** file from the link in the table, copy it to the **POST** request, and execute it. This will replace all texts with the predefined ones.

⚠️ **Caution**

Be careful if you change the keys when overwriting data texts, because this can result in invalid values. If a user has a certain value assigned, and the key value pair is overwritten with a different key, then the value for that property of the user will be no longer valid and visualized. For example, if you have set "Mr." to a user, and the key-value pair is "01=Mr.", "Mr." will not be visualized for that user.
When overwriting data texts, the keys for the different languages must be one and the same. For example, the master data texts for the German locale are overwritten, and the tenant administrator wants to overwrite the texts for the French locale. The keys for the German locale should be obtained first and used as keys for the French locale. After that the values can be translated in French.

### Methods

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>See</th>
<th>URI</th>
</tr>
</thead>
<tbody>
<tr>
<td>GET</td>
<td>GET Master Data Texts [page 391]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/service/resource?resourceType=RESOURCE_MD_&lt;VALUE&gt;&amp;locale=&lt;value&gt;</td>
</tr>
<tr>
<td>POST</td>
<td>POST Master Data Texts [page 394]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/service/resource/SAP_DEFAULT</td>
</tr>
</tbody>
</table>

**Note**

_Tenant ID_ is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the _tenant ID_.

### 1.7.2.7.1 GET Master Data Texts

Download the texts that you have already overwritten in the predefined master data texts.

**Request**

**URI:** https://<tenant ID>.accounts.ondemand.com/service/resource?resourceType=<value>&locale=<value>

**HTTP Method:** GET

**Permissions:** You must have a system as administrator (T user) with an assigned _Manage Tenant Configuration_ role. For more details about how to add a system as administrator and assign administrator roles, see _Add System as Administrator [page 240]_, and _Edit Administrator Authorizations [page 241]_.

---

_SAP Cloud Platform Identity Authentication Service_

PUBLIC 391
### URL Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Required</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>setId</td>
<td>No</td>
<td>The identifier of the scenario that the resource is related to.</td>
<td>The default value is SAP_DEFAULT</td>
</tr>
</tbody>
</table>
| resourceType    | Yes      | The type of the resource.                                        | Use:
|                 |          |                                                                  | ● RESOURCE_MD_SALUTATIONS                  |
|                 |          |                                                                  | ● RESOURCE_MD_FUNCTIONS                    |
|                 |          |                                                                  | ● RESOURCE_MD_DEPARTMENTS                  |
|                 |          |                                                                  | ● RESOURCE_MD_RELATIONSHIPS                |
|                 |          |                                                                  | ● RESOURCE_MD_INDUSTRIES                   |
|                 |          |                                                                  | ● RESOURCE_MD_LANGUAGES                    |
|                 |          |                                                                  | ● RESOURCE_MD_COUNTRIES                    |
| locale          | Yes      | The locale of the resource.                                     | The default languages are:
|                 |          |                                                                  | ● Chinese (zh-CN)                          |
|                 |          |                                                                  | ● Dutch (nl)                               |
|                 |          |                                                                  | ● English (en)                             |
|                 |          |                                                                  | ● French (fr)                              |
|                 |          |                                                                  | ● German (de)                              |
|                 |          |                                                                  | ● Hebrew (iw)                              |
|                 |          |                                                                  | ● Italian (it)                             |
|                 |          |                                                                  | ● Japanese (ja)                            |
|                 |          |                                                                  | ● Korean (ko)                              |
|                 |          |                                                                  | ● Polish (pl)                              |
|                 |          |                                                                  | ● Portuguese (pt)                          |
|                 |          |                                                                  | ● Russian (ru)                             |
|                 |          |                                                                  | ● Spanish (es)                             |
|                 |          |                                                                  | ● Welsh (cy)                               |
|                 |          |                                                                  | ● Swedish (sv)                             |

### Request Example

```
GET /service/resource?resourceType=RESOURCE_MD_SALUTATIONS&locale=en
Content-Type: application/json
```
Response

Response Status and Error Codes

Success Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>The request was successful.</td>
<td>OK</td>
</tr>
</tbody>
</table>

Error Codes

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>Bad Request</td>
<td>Validate JSON data. Validate that the special characters are escaped properly and new lines are added.</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized</td>
<td>The client is not authenticated.</td>
</tr>
<tr>
<td>403</td>
<td>Forbidden</td>
<td>Access to the resource is denied.</td>
</tr>
<tr>
<td>404</td>
<td>Not Found</td>
<td>The requested resource cannot be found.</td>
</tr>
<tr>
<td>405</td>
<td>Method Not Allowed</td>
<td>The requested method is not supported for the given resource.</td>
</tr>
<tr>
<td>415</td>
<td>Unsupported Media Type</td>
<td>The REST service does not support the API version requested by the REST client.</td>
</tr>
<tr>
<td>500</td>
<td>Internal Server Error</td>
<td>The operation cannot be completed due to a server error.</td>
</tr>
<tr>
<td>503</td>
<td>Service Unavailable</td>
<td>The service is currently unavailable.</td>
</tr>
</tbody>
</table>

Response Example

Example of response that returns overwritten values of the Salutations file.

```json
{
  0001=Dr.,
  0002=Prof.
}
```

Example of response that returns overwritten keys of the Salutations file. The keys can differ from the original in the master data file. It is not necessary to be in sequence.

```json
{
  01=Ms.,
  05=Mr.
}
```
1.7.2.7.2  POST Master Data Texts

Update the master data texts.

⚠️ Caution

Make sure that you have applied the proper escaping in your POST request.

You should add \n at the end of each line in the data property content.

<table>
<thead>
<tr>
<th>Escape Sequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
</tr>
<tr>
<td>Backspace (ascii code 08)</td>
</tr>
<tr>
<td>Form feed (ascii code 0C)</td>
</tr>
<tr>
<td>New line</td>
</tr>
<tr>
<td>Carriage return</td>
</tr>
<tr>
<td>Tab</td>
</tr>
<tr>
<td>Double quote</td>
</tr>
<tr>
<td>Backslash character</td>
</tr>
</tbody>
</table>

→ Tip

Instead of editing the request manually, you can use an on-line tool for converting a normal string into a quoted one.

**Request**

**URI:** https://<tenant ID>.accounts.ondemand.com/service/resource/SAP_DEFAULT

**HTTP Method:** POST

**Permissions:** You must have a system as administrator (T user) with an assigned Manage Tenant Configuration role. For more details about how to add a system as administrator and assign administrator roles, see Add System as Administrator [page 240], and Edit Administrator Authorizations [page 241].

**Request Example**

```json
https://<tenantId>.accounts.ondemand.com/service/resource/SAP_DEFAULT
Content-Type: application/json
Body:
[
  {
    "resourceType": "RESOURCE_MD_DEPARTMENTS",
    "locale": "en",
    "contentType": "text/html;charset=UTF-8",
```
Response

Response Status and Error Codes

Success Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 OK</td>
<td>The request was successful.</td>
<td>OK</td>
</tr>
</tbody>
</table>

Error Codes

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>Bad Request</td>
<td>Validate JSON data. Validate that the special characters are escaped properly and new lines are added.</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized</td>
<td>The client is not authenticated.</td>
</tr>
<tr>
<td>403</td>
<td>Forbidden</td>
<td>Access to the resource is denied.</td>
</tr>
<tr>
<td>404</td>
<td>Not Found</td>
<td>The requested resource cannot be found.</td>
</tr>
<tr>
<td>405</td>
<td>Method Not Allowed</td>
<td>The requested method is not supported for the given resource.</td>
</tr>
<tr>
<td>415</td>
<td>Unsupported Media Type</td>
<td>The REST service does not support the API version requested by the REST client.</td>
</tr>
<tr>
<td>500</td>
<td>Internal Server Error</td>
<td>The operation cannot be completed due to a server error.</td>
</tr>
<tr>
<td>503</td>
<td>Service Unavailable</td>
<td>The service is currently unavailable.</td>
</tr>
</tbody>
</table>

1.7.2.8 General Error Codes

The following table lists error codes that may be returned from any method on any resource URI.

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>301</td>
<td>Permanent Location</td>
<td>The requested resource resides on a URI other than the requested one.</td>
</tr>
<tr>
<td>400</td>
<td>Bad Request</td>
<td>The requested operation cannot be executed because the service cannot understand the data sent in the entity body of the request.</td>
</tr>
</tbody>
</table>
### 1.7.3 Add Logon Overlays in Customer Applications

This document describes how service providers that delegate authentication to Identity Authentication can use embedded frames, also called overlays, for the logon pages of their applications.

#### Context

The use of overlays maintains the application context, by keeping the application page as dimmed background, to provide for minimum disturbance to the work flow. By default, after a successful logon via an overlay page, the application’s parent page reloads. For more information how to configure that option, see [Enable or Disable Reload Parent Page Option](page 95).

#### i Note

When the application uses overlay for the logon page, but the client’s browser does not accept third party cookies, the logon page opens in fullscreen.

To open the logon page of the application in an overlay instead of in fullscreen when the browser is set not to accept third party cookies, the user has to add an exception for the domain of this application. The users can consult the documentations of the different browsers for more information about how to enable third party cookies for specific websites and domains.
To add a logon overlay into your application proceed as follows:

**Procedure**

1. Include the following libraries to the landing page of your application:
   - **jQuery**
     If you have already included jQuery you do not need to do it again.
     You can download the jQuery from a Content Delivery Network (CDN), or you can use the following pattern:
     
     "Sample Code"
     ```html
     <script src="https://<tenant ID>.accounts.ondemand.com/ui/resources/javascripts/jquery-1.8.2.min.js" />
     ```
   - **SAP_IDS.js**
     Use the following pattern:
     
     "Sample Code"
     ```html
     <script src="https://<tenant ID>.accounts.ondemand.com/ui/resources/javascripts/SAP_IDS.js" />
     ```

   **Caution**
   Make sure that the reference to the javascript file is pointing to the same Identity Authentication tenant that is used for authentication of this application. Have this in mind when you migrate your applications from quality to productive environment, if different Identity Authentication tenants are used.

2. Add a logon link.

   **Note**
   The logon link must be an HTML anchor with the following attributes:

<table>
<thead>
<tr>
<th>attribute</th>
<th>value</th>
</tr>
</thead>
<tbody>
<tr>
<td>rel</td>
<td>IDS_login</td>
</tr>
<tr>
<td>href</td>
<td>points to an actual resource in your application that generates SAML 2.0 authentication request to Identity Authentication</td>
</tr>
<tr>
<td></td>
<td>the name of the resource is not important</td>
</tr>
</tbody>
</table>

   "Sample Code"
   ```html
   <a href="/login.jspa" rel="IDS_login">Log in</a>
   ```
Results

When the user chooses the logon link, the following happens:

- If the user is not logged on, the log on overlay is displayed.
- If the user is logged on to an application with the same Identity Authentication tenant, in other words he or she has an active application session, the user is automatically logged on to the second application.

⚠️ Caution

The logon link should be visible only if the user does not have an active application session.

If you still want to show the log on link when the user has an active application session, you must change the logic for the log on link for this case. The log on link should not contain `rel="IDS_Login"` in this case. For example, the logic could be that, when the user chooses the logon link, he or she is directly redirected to the protected resource.

Next Steps

Protect applications against clickjacking when using overlays. For more information, see Configure Clickjacking Protection [page 399].

Further Options

Locale

If the locale is known, this can be communicated to Identity Authentication by adding a locale parameter to `SAP_IDS.js`.

⚠️ Source Code

```
```

ℹ️ Note

The locale parameter follows the Java specifications for a locale and must be of the format `ll_CC` where:

- `ll` is the language two letter code in small letters
- `CC` is the country (region) two letter code in capital letters
1.7.4 Configure Clickjacking Protection

Clickjacking is an attempt to trick users into clicking hidden user interface elements without the user realizing it. The user thinks he or she is clicking on the underlying frame, but is actually clicking on an action chosen by the attacker.

You have two options to protect your applications against clickjacking when using embedded frames, also called overlays, for the logon pages of the applications:

- If the applications are SAP UI5 or Web Dynpro, or they use the overlays of SAP Cloud Platform Identity Authentication service, add the domains of these applications as trusted in the administration console for Identity Authentication. For more information, see Configure Trusted Domains [page 138].
- If the applications are not SAP UI5 or Web Dynpro, or they do not use the overlays of Identity Authentication, add the following code to your message handler:

```
function messageHandler(oEvent){
    if(oEvent.data=='SAPFrameProtection*require-origin'){
        oEvent.source.postMessage('SAPFrameProtection*parent-origin','*');
    }
}
```

Related Information

Add Logon Overlays in Customer Applications [page 396]

1.7.5 Troubleshooting for Developers

This section is to help developers with solutions to the REST API response codes.

Error Codes

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>301</td>
<td>Permanent Location</td>
<td>The requested resource resides on a URI other than the requested one.</td>
</tr>
<tr>
<td>400</td>
<td>Bad Request</td>
<td>The requested operation cannot be executed because the service cannot understand the data sent in the entity body of the request.</td>
</tr>
<tr>
<td>Response Code</td>
<td>Meaning</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>--------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>401</td>
<td>Unauthorized</td>
<td>The client is not authenticated.</td>
</tr>
<tr>
<td>403</td>
<td>Forbidden</td>
<td>Access to the resource is denied.</td>
</tr>
<tr>
<td>404</td>
<td>Not Found</td>
<td>The requested resource cannot be found.</td>
</tr>
<tr>
<td>405</td>
<td>Method Not Allowed</td>
<td>The requested method is not supported for the given resource.</td>
</tr>
<tr>
<td>406</td>
<td>Not Acceptable</td>
<td>The requested method does not produce any of the media types requested in the HTTP request.</td>
</tr>
<tr>
<td>409</td>
<td>Conflict</td>
<td>The operation cannot be completed because it conflicts with an existing resource.</td>
</tr>
<tr>
<td>415</td>
<td>Unsupported Media Type</td>
<td>The REST service does not support the API version requested by the REST client.</td>
</tr>
<tr>
<td>500</td>
<td>Internal Server Error</td>
<td>The operation cannot be completed due to a service error.</td>
</tr>
<tr>
<td>503</td>
<td>Service Unavailable</td>
<td>The service is currently unavailable.</td>
</tr>
</tbody>
</table>

In addition to the general error codes, the REST APIs return one of the following detailed error codes as an `X-message-code` HTTP response header:

<table>
<thead>
<tr>
<th>REST API</th>
<th>X-message code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invitation REST API</td>
<td>INVITATION_API_PARAMETER_INCORRECT</td>
<td>You have used an invalid parameter.</td>
</tr>
<tr>
<td></td>
<td>INVITATION_API_EMAIL_INCORRECT</td>
<td>You have specified an incorrect e-mail address or the email address does not exist.</td>
</tr>
<tr>
<td></td>
<td>PASSWORD_LOCKED</td>
<td>The password is locked for 60 minutes after 5 failed logon attempts with wrong value.</td>
</tr>
<tr>
<td>User Management REST API</td>
<td>PASSWORD_LOCKED</td>
<td>The password is locked for 60 minutes after 5 failed logon attempts with wrong value.</td>
</tr>
<tr>
<td>Update Group Resource SCIM REST API</td>
<td>Mismatched group id</td>
<td>The id of the group in the URI and the id of the group in the request body are different. Make sure that the id of the group is one and the same in both places.</td>
</tr>
</tbody>
</table>
Success Codes

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>OK</td>
<td>Operation successful.</td>
</tr>
<tr>
<td>201</td>
<td>Created</td>
<td>Entity created successfully.</td>
</tr>
<tr>
<td>204</td>
<td>No Content</td>
<td>The service received and understood the request, but there is no need to send any content back.</td>
</tr>
</tbody>
</table>

Related Information

Get Support [page 432]

1.8 Security

This section describes the security features at SAP Cloud Platform Identity Authentication service.

In this section:
- Security Information [page 401]
- Data Protection and Privacy [page 404]

1.8.1 Security Information

This document is an overview of security-relevant information that applies to SAP Cloud Platform Identity Authentication service, and contains recommendations about how administrators should secure it.

While this document is intended to support administrators and security responsible specialists to use Identity Authentication in a secure manner, there may be further elements to consider depending on usage, integrations as well as applicable industry or local legal regulations.

Updates and Notifications

For more information, see Updates and Notifications [page 432].
**Before You Start**

Before you secure Identity Authentication, protect the cloud application that trusts Identity Authentication. For more information about protecting SAP Cloud Platform applications, see *Security in the Neo Environment*.

**Communication Protocol**

Identity Authentication is fully web browser based application, with all access over HTTPS. Every page of the Identity Authentication application is currently delivered via Transport Layer Security (TLS). Access to Identity Authentication is encrypted-in-transit over HTTPS using 256-bit TLS encryption.

**User Administration**

Set user permissions in accordance with the scenario you are configuring. For more information, see *Scenarios [page 33]*.

You have the following options:

- For a business-to-consumer scenario, allow **Public** user application access.
- For a business-to-business scenario, allow **Private** user application access.
- For a business-to-employee scenario, allow **Internal** user application access.

For more information about the settings for user application access, see *Configure User Access to the Application [page 87]*.

You can also define rules for authentication according to different risk factors. For more information, see *Configure Risk-Based Authentication [page 82]*.

**User Authentication**

Identity Authentication protects your users during authentication in the following ways:

- With SAML 2.0 or OpenID Connect
  Identity Authentication supports the single sign-on (SSO) mechanism. Every user with an account is able to use SSO for the cloud applications that use Identity Authentication.

- With an application certificate
  The Identity Authentication authentication interfaces that receive REST API calls are protected, since they require an application certificate. Use the certificate when implementing REST APIs for your application. For more information, see the REST API configurations in *Developer Guide [page 313]*.
Password Security

Identity Authentication does not store plain text passwords in the database, but only their iterated random-salted secure hash values. The random salt is at least 512 bits, and it is different for each password. Only generic hash functions are used with minimum 512 bits key length. No default passwords are delivered, used, or accepted anywhere.

Identity Authentication can use also passwords from on-premise systems for user authentication. These passwords are not stored by Identity Authentication. It sends the user ID and the password for authentication to the on-premise system via the Transport Layer Security (TLS) connection. The management of these passwords depends on the integrated on-premise system that supports them, for example Microsoft Active Directory.

Identity Authentication supports three levels of password security. You should use the highest level of security that matches the requirements of your application. The passwords are managed based on password policy rules. For more information, see Configuring Password Policies [page 166].

Session Security

Session cookies in Identity Authentication are protected with a Transport Layer Security (TLS) and with the Secure and HttpOnly attributes. You do not need to make any additional configurations for Identity Authentication.

Network and Communication Security

Identity Authentication is setup in a fenced network, separated from the SAP internal network.

Customer applications run in a shared environment where the business data is isolated from each other, the SAP Cloud Platform services uses a shared SAP Cloud Platform infrastructure. The internal traffic is controlled by firewalls. SAP administrative access is done via terminal service that requires strong authentication.

All communication channels are protected with TLS, and you should configure the cloud application to use TLS and to check the SAML 2.0 signature.

Data Storage Security

Data storage security is about how Identity Authentication protects its own database. Data storage security is ensured by the isolated tenant that each customer receives. Only tenant-specific requests can access the tenant’s database. These requests are performed by a tenant service, which works with a dependency injection framework and makes sure that all the services. For example the persistence service and the mail service, are injected with the instances dedicated to the given tenant.
Security-Relevant Logging and Tracing

You can download a CSV file with a history of operations performed by administrators. For more information, see Export Change Logs with a History of Administration Operations [page 277].

You can retrieve the statistics on the number of user logon request per month. This number is counted on each single authentication managed via Identity Authentication. For more information, see View Usage Statistics [page 273].

Related Information

Security on SAP Community Network
SAP Data Center
SAP Security Notes
SAP Security Certificates

1.8.2 Data Protection and Privacy

Governments place legal requirements on industry to protect data and privacy. We provide features and functions to help you meet these requirements.

Note

SAP does not provide legal advice in any form. SAP software supports data protection compliance by providing security features and data protection-relevant functions, such as blocking and deletion of personal data. In many cases, compliance with applicable data protection and privacy laws is not covered by a product feature. Furthermore, this information should not be taken as advice or a recommendation regarding additional features that would be required in specific IT environments. Decisions related to data protection must be made on a case-by-case basis, taking into consideration the given system landscape and the applicable legal requirements. Definitions and other terms used in this documentation are not taken from a specific legal source.

Handle personal data with care. You as the data controller are legally responsible when processing personal data. It is not permitted to deal with sensitive personal data in Identity Authentication.

Remember

Custom attributes must not be used to store sensitive personal data. For more information, see Configure the User Attributes Sent to the Application [page 64].

Glossary for Data Protection and Privacy [page 405]

The following terms are general to SAP products. Certain terms might not be relevant for SAP Cloud Platform Identity Authentication service.

Change Logging and Audit Logging [page 407]
Change logging records changes to personal data, while audit logging provides access to personal data, successful, and failed authentications. You may be required to gather this information for auditing purposes or legal requirements.

Information Report [page 408]
An information report is a collection of data relating to a data subject. A data privacy specialist may be required to provide such a report or an application may offer a self-service.

Erasure [page 408]
When handling personal data, consider the legislation in the different countries where your organization operates. After the data has passed the end of purpose, regulations may require you to delete the data. However, additional regulations may require you to keep the data longer. During this period, you must block access to the data by unauthorized persons until the end of the retention period, when the data is finally deleted.

Consent [page 409]
We assume that software operators, such as SAP customers, collect and store the consent of data subjects, before collecting personal data from data subjects. A data privacy specialist can later determine whether data subjects have granted, withdrawn, or denied consent.

1.8.2.1 Glossary for Data Protection and Privacy

The following terms are general to SAP products. Certain terms might not be relevant for SAP Cloud Platform Identity Authentication service.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocking</td>
<td>A method of restricting access to data for which the primary business purpose has ended.</td>
</tr>
<tr>
<td>Business purpose</td>
<td>A legal, contractual, or in other form justified reason for the processing of personal data. The assumption is that any purpose has an end that is usually already defined when the purpose starts.</td>
</tr>
<tr>
<td>Consent</td>
<td>The action of the data subject confirming that the usage of his or her personal data shall be allowed for a given purpose. A consent functionality allows the storage of a consent record in relation to a specific purpose and shows if a data subject has granted, withdrawn, or denied consent.</td>
</tr>
<tr>
<td>Deletion</td>
<td>Deletion of personal data so that the data is no longer available.</td>
</tr>
<tr>
<td>End of business</td>
<td>Date where the business with a data subject ends, for example the order is completed, the subscription is canceled, or the last bill is settled.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>End of purpose (EoP)</td>
<td>End of purpose and start of blocking period. The point in time, when the primary processing purpose ends (for example contract is fulfilled).</td>
</tr>
<tr>
<td>End of purpose (EoP) check</td>
<td>A method of identifying the point in time for a data set when the processing of personal data is no longer required for the primary business purpose. After the EoP has been reached, the data is blocked and can only be accessed by users with special authorization (for example, tax auditors).</td>
</tr>
<tr>
<td>Personal data</td>
<td>Any information relating to an identified or identifiable natural person (“data subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person</td>
</tr>
<tr>
<td>Purpose</td>
<td>The information that specifies the reason and the goal for the processing of a specific set of personal data. As a rule, the purpose references the relevant legal basis for the processing of personal data.</td>
</tr>
<tr>
<td>Residence period</td>
<td>The period of time between the end of purpose (EoP) for a data set during which the data remains in the database and can be used in case of subsequent processes related to the original purpose. At the end of the longest configured residence period, the data is blocked or deleted. The residence period is part of the overall retention period.</td>
</tr>
<tr>
<td>Retention period</td>
<td>The period of time between the end of the last business activity involving a specific object (for example, a business partner) and the deletion of the corresponding data, subject to applicable laws. The retention period is a combination of the residence period and the blocking period.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sensitive personal data</td>
<td>A category of personal data that usually includes the following type of information:</td>
</tr>
<tr>
<td></td>
<td>- Special categories of personal data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health or sex life or sexual orientation.</td>
</tr>
<tr>
<td></td>
<td>- Personal data subject to professional secrecy</td>
</tr>
<tr>
<td></td>
<td>- Personal data relating to criminal or administrative offenses</td>
</tr>
<tr>
<td></td>
<td>- Personal data concerning insurances and bank or credit card accounts</td>
</tr>
<tr>
<td>Where-used check (WUC)</td>
<td>A process designed to ensure data integrity in the case of potential blocking of business partner data. An application’s where-used check (WUC) determines if there is any dependent data for a certain business partner in the database. If dependent data exists, this means the data is still required for business activities. Therefore, the blocking of business partners referenced in the data is prevented.</td>
</tr>
</tbody>
</table>

### 1.8.2.2 Change Logging and Audit Logging

Change logging records changes to personal data, while audit logging provides access to personal data, successful, and failed authentications. You may be required to gather this information for auditing purposes or legal requirements.

**Audit Logs**

Tenant administrators can access the audit logs for changes in the personal data, successful, and failed authentications in SAP Cloud Platform Identity Authentication. If you want to view the audit logs, you should generate Client ID and Client Secret for audit logs in the administration console for Identity Authentication, obtain an access token, and call the audit log retrieval API to access the data. For more information, see Access Audit Logs [page 274].

**Change Logs**

Tenant administrators can access information about configuration changes made by administrators in Identity Authentication. You can download a CSV file with a history of the operations performed by administrators. For more information, see Export Change Logs with a History of Administration Operations [page 277].
1.8.2.3  Information Report

An information report is a collection of data relating to a data subject. A data privacy specialist may be required to provide such a report or an application may offer a self-service.

Information About Own Personal Data

Data subjects can obtain information about their personal data in SAP Cloud Platform Identity Authentication service, via the profile page at https://<tenant ID>.accounts.ondemand.com/.

- Users can open a printable overview of all the data on file for them by clicking the View button in the My Data section.

  i  Note
  The data includes the Terms of Use and Privacy Policy documents signed by the user. The documents can be seen by clicking on their names. They open in a new tab.

- Users can download an overview of all the data for them on a JSON file by clicking the Download button in the My Data section.

Information About Users' Data

Tenant administrators can view detailed information about the users in the administration console for SAP Cloud Platform Identity Authentication service. Optionally they can edit this information. For more information, see List and Edit User Details [page 205].

1.8.2.4  Erasure

When handling personal data, consider the legislation in the different countries where your organization operates. After the data has passed the end of purpose, regulations may require you to delete the data. However, additional regulations may require you to keep the data longer. During this period, you must block access to the data by unauthorized persons until the end of the retention period, when the data is finally deleted.

Only the service provider is aware of the retention policies of the user, and thus whether a user record has to be blocked first, and deleted at a certain time in the future, or whether a user record can be deleted immediately.

The end user who wants to cancel his or her registration from the service should start the process via the service provider, not via Identity Authentication. Identity Authentication keeps user information for every service provider. Each service provider deletes its specific data stored about the user in Identity Authentication via an API call. If the user has accounts in more than one service provider, his or her whole user profile in Identity Authentication is deleted when the information for the last service provider is deleted. For more information, see SP User Deletion [page 328].
Apart from deleting, users can be blocked. When users are blocked, they exist in Identity Authentication, but cannot be authenticated when they try to log on. For more information, see SP User Deactivation [page 327].

Tenant administrators can delete and block users via the administration console for Identity Authentication. For more information, see Delete Users [page 207] and Deactivate Users [page 208].

1.8.2.5 Consent

We assume that software operators, such as SAP customers, collect and store the consent of data subjects, before collecting personal data from data subjects. A data privacy specialist can later determine whether data subjects have granted, withdrawn, or denied consent.

Every (service provider) application that trusts SAP Cloud Platform Identity Authentication service can configure its own privacy policy and terms of use documents. For more information, see Configuring Privacy Policies [page 173], and Configuring Terms of Use [page 178].

Identity Authentication takes care the documents to be accepted by the users. Whenever a new version of the document becomes available, an upgrade process is started.

The end users can view the signed Terms of Use and Privacy Policy documents by them at the profile page. For more information, see Information Report [page 408].

The tenant administrators can view a history of the signed Terms of Use and Privacy Policy documents of the users in the administration console for Identity Authentication. The information is in the format <document name><document version><time stamp>.

1.9 Integration Scenarios

You can integrate SAP Cloud Platform Identity Authentication service with SAP and non-SAP systems as service providers.

Related Information

Integration with SAP Cloud Platform [page 410]
Integration with SAP Web IDE [page 417]
1.9.1 Integration with SAP Cloud Platform

Context

In this setup, SAP Cloud Platform acts as a service provider, and SAP Cloud Platform Identity Authentication service acts as an identity provider. For the integration, you must set the trust on both sides.

As a result of the trust setting, when you have deployed an application to SAP Cloud Platform that has protected resources and requires SAML authentication, the user is redirected to the logon page of SAP Cloud Platform Identity Authentication service to provide credentials.

\[\text{Note}\]
Once setting Identity Authentication as a trusted identity provider for SAP Cloud Platform all the services in the SAP Cloud Platform would be authenticated via Identity Authentication. For more information about the services provided by SAP Cloud Platform, see Services.

For the integration you need to make configurations in the cockpit of SAP Cloud Platform and in the administration console for Identity Authentication. The configurations made in the administration console do not affect the authentication for the cockpit, which is carried out via the SAP-defined tenant, SAP ID service.

\[\text{Tip}\]
If you want to use a custom Identity Authentication tenant as an identity provider for the cockpit, see Platform Identity Provider (for the cockpit or console client).

For more information about the access to SAP Cloud Platform and Identity Authentication, see the following sections:

- Access to SAP Cloud Platform Cockpit
- Access to Identity Authentication

Access to SAP Cloud Platform Cockpit

Once you purchase a customer or partner account of SAP Cloud Platform, an e-mail is sent to the contact person from your company with a link to your SAP Cloud Platform cockpit. The contact person is specified in the Order Form for SAP Cloud Services. He or she is the first subaccount member of the SAP Cloud Platform cockpit.
The cockpit is the central point for managing all activities associated with your cloud-based business applications. For more information about the cockpit, see Cloud Cockpit.

To deploy applications on SAP Cloud Platform and to make configurations in the cockpit, you need a subaccount that corresponds to your role. For more information, see Getting a Global Account.

Access to SAP Cloud Platform Identity Authentication Service

Identity Authentication does not use for authentication the users registered in the SAP Service Marketplace, but maintains an own user store for administrators and users.

Once you purchase a customer or partner account of SAP Cloud Platform, a user account for Identity Authentication is created for the same contact person, specified in the Order Form. The contact person is the first administrator in the administration console for Identity Authentication. He or she receives an activation e-mail for the administration console account. The subject of the e-mail is: Activate Your Account for Administration Console. Following the required steps, the administrator activates the account and can continue to the administration console for Identity Authentication via the console’s URL.

i Note

The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

Tenant ID is an automatically generated ID by the system. The URL is in the activation e-mail received by the first administration contains the tenant ID.

⚠️ Caution

If new SAP Cloud Platform members are added into the Members page of the SAP Cloud Platform cockpit these members are not added as administrators of Identity Authentication. This is done only for the first account member. For more information about how to add new administrators in Identity Authentication, see Add User as Administrator [page 238].
1.9.1.1 Configure SAP Cloud Platform

Prerequisites

- You have a subaccount for SAP Cloud Platform. For more information, see Getting a Global Account.
- You have a tenant of SAP Cloud Platform Identity Authentication service.
- You have protected your SAP Cloud Platform application. For more information about how to protect your resource, see Enabling Authentication.

Note

If you want to use SAP Cloud Platform in a productive environment, you should purchase a customer account or join a partner account. The trial account for SAP Cloud Platform uses the default SAP tenant.

By default, SAP Cloud Platform uses SAP ID service as a trusted identity provider. SAP ID service is an SAP-defined tenant that cannot be configured by external administrators. If your environment contains SAP applications such as SAP Jam, SAP Community Network or Success Map that use authentication through SAP ID service, you can use the default tenant.

Context

You have two configuration options based on the following cases:

<table>
<thead>
<tr>
<th>You want to</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add a tenant of Identity Authentication registered for your company or organization as an identity provider.</td>
<td>Follow the procedure in: Identity Authentication Tenant as an Application Identity Provider.</td>
</tr>
</tbody>
</table>

Note

In this case, the trust is established automatically upon registration in both the SAP Cloud Platform and the Identity Authentication tenant. Automatically the SAP Cloud Platform Account is registered as an application in the tenant of Identity Authentication. You can find it in the administration console under the CUSTOM APPLICATIONS list, representing your SAP Cloud Platform account.
You want to | Procedure
--- | ---
Configure manual trust | 1. Download the metadata file of Identity Authentication. For more details, see: Tenant SAML 2.0 Configuration [page 130].
2. Use this metadata to configure the trust on SAP Cloud Platform. For more details about this configuration, see Application Identity Provider.

→ Tip
Once setting Identity Authentication as a trusted identity provider for SAP Cloud Platform all SAP Cloud Platform applications and services use the trust and configuration settings. If you need different settings for the different SAP Cloud Platform applications or services, open a new subaccount. For more information, see Create Subaccounts. Once you have created the new subaccount, add the tenant of Identity Authentication in the new subaccount. Repeat the procedure from the table above to set the trust for each subaccount.

1.9.1.2 Configure SAP Cloud Platform Identity Authentication Service

Prerequisites

- You have a tenant of SAP Cloud Platform Identity Authentication service.
- You have added the tenant of SAP Cloud service as an identity provider in SAP Cloud Platform cockpit. For more information, see: Identity Authentication Tenant as an Application Identity Provider.
- You have downloaded the metadata for SAP Cloud Platform as a service provider (SP). For more information, see Application Identity Provider.

Context

You need this configuration if you have added a tenant of Identity Authentication which is not registered for the organization or company for which the SAP Cloud Platform account is created.

If you have added a tenant of Identity Authentication registered for your company or organization as an identity provider, see Configure SAP Cloud Platform [page 412].
Procedure

1. Set the trust with SAP Cloud Platform. For more details, see Configure Trust [page 55].
2. **Optional**: Customize the settings for the application. For more information, see Configuring Applications [page 40].

### 1.9.1.3 Configure IdP-Initiated SSO with SAP Cloud Platform

**Context**

You can perform IdP-initiated single sign-on (SSO) in SAP Cloud Platform by sending the SAML Response directly to the application URL that is protected with SAML. This requires you to change the assertion consumer service (ACS) endpoint on the identity provider side to point to this URL.

To configure IdP-initiated SSO with SAP Cloud Platform, follow the steps below:

**Procedure**

1. Change the ACS endpoint on the identity provider side to point to the application protected URL. For more information, see Step 6 in Configure Trust [page 55].
2. Configure IdP-initiated SSO. For more information, see Configure IdP-Initiated SSO [page 162].

### 1.9.1.4 Configure Assertion Attributes Mapping

You have to specify how the assertion attributes are sent to SAP Cloud Platform in the assertion, and define their mapping.

### 1. Configure User Attributes in Identity Authentication

**Procedure**

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
i Note

The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.

Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
   This operation opens a list of the applications.
3. Choose your SAP Cloud Platform application from the list.
4. Choose the Trust tab.
5. Under SINGLE SIGN-ON, choose Assertion Attributes.
6. Add the assertion attributes.
7. Save your configuration.

If the operation is successful, you receive the message Assertion attributes updated.

Related Information

Configure the User Attributes Sent to the Application [page 64]

2. Configure Mapping in SAP Cloud Platform

Procedure

1. Log on to SAP Cloud Platform cockpit. For more information, see Navigating to a Subaccount.
2. Select the subaccount and choose TRUST in the navigation bar.
3. Choose the Trusted Service Provider the identity provider that the platform uses for authentication.
4. Choose [Attributes] > [Add Assertion-Based Attribute].

5. Enter the fields as follows:

<table>
<thead>
<tr>
<th>Assertion Attribute</th>
<th>Principal Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

**Note**
- This specifies that all assertion attributes will be mapped to the corresponding principal attributes without a change.
- The **Assertion Attribute** field is for the attribute that comes from the assertion.
- The **Principal Attribute** field is the user attribute that the users will have at SAP Cloud Platform.

6. Save your changes.

**Related Information**

**Application Identity Provider**

**1.9.1.5 Configure SAP Cloud Platform Custom Domains**

You can make your SAP Cloud Platform applications accessible on your own domain different from hana.ondemand.com - for example www.myshop.com.

**Prerequisites**

You have configured your application’s custom domain using the SAP Cloud Platform console client. For more information, see Configuring Custom Domains.

**Context**

When a custom domain is used, both the domain name and the server certificate for this domain are owned by the customer.

To use a custom domain for the application that uses your Identity Authentication tenant for authentication, follow the procedure as described in the current document.
Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console's URL.

   ![Note]
   
   The URL has the `https://<tenant ID>.accounts.ondemand.com/admin` pattern.
   
   *Tenant ID* is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the *tenant ID*.

2. Choose the *Applications* tile.
   
   This operation opens a list of the applications.

3. Choose the list item of the application that will use a custom domain.

4. Choose the *Trust* tab.

5. Under *SAML 2.0*, choose *SAML 2.0 Configuration*.

6. Edit the *Assertion Consumer Service Endpoint* URL field and the *Single Logout Endpoint* URLs fields by replacing `authn.hana.ondemand.com` with your custom domain name. In the example above, this would be `www.myshop.com`.

7. Save your changes.

Results

Once the configuration has been changed, the system displays the message *Application <name of application> updated*. The application can only be accessed via the custom domain.

1.9.2 Integration with SAP Web IDE

You can use SAP Cloud Platform Identity Authentication service as identity provider for SAP Web IDE.

Prerequisites

- You have a subaccount for SAP Cloud Platform. For more information, see *Getting a Global Account*.
- You have an Identity Authentication tenant. For more information about how to get Identity Authentication, see *SAP Cloud Platform Pricing and Packaging Options* or contact your SAP sales representative.
- You have registered the Identity Authentication as a trusted identity provider for your SAP Cloud Platform account. See *Identity Authentication Tenant as an Application Identity Provider*.
- You have set the trust with SAP Cloud Platform. For more details, see *Configure Trust [page 55]*.
You have switched off the *Reload Parent Page* option for SAP Web IDE in the administration console for Identity Authentication. For more information, see Enable or Disable Reload Parent Page Option [page 95].

You have added your SAP Web IDE host to the list of the trusted domains in the administration console for Identity Authentication. For more information, see Configure Trusted Domains [page 138].

You have checked the User ID of the users that will be able to access SAP Web IDE. The User ID is a six-digit number preceded by the letter P. For more information about how to check the User ID, see List and Edit User Details [page 205].

**Context**

The integration between SAP Web IDE and Identity Authentication enables users to access SAP Web IDE with their Identity Authentication credentials.

SAP Web IDE access can be protected by permissions. To grant a user the permission to access a protected resource, you can either assign a custom role or one of the predefined virtual roles to such a permission. The following predefined virtual roles are available:

- **AccountAdministrator** - equivalent to the list of account members with administrator permission.
- **AccountDeveloper** - equivalent to the list of account members with developer permission.
- **Everyone** - equivalent to all authenticated users of the configured Identity Provider.

If you want to use the AccountDeveloper or AccountAdministrator role to enable users to access SAP Web IDE with their Identity Authentication credentials, see Assign AccountAdministrator or AccountDeveloper Roles [page 418].

If you want to use the Everyone role to enable the users to access SAP Web IDE with their Identity Authentication credentials, see Assign Everyone Role [page 420].

### 1.9.2.1 Assign AccountAdministrator or AccountDeveloper Roles

**Context**

If you want to use the AccountDeveloper or AccountAdministrator role together with SAP Cloud Platform Identity Authentication service as an identity provider, complete the following steps:

**Procedure**

1. Log on to SAP Cloud Platform cockpit with the cockpit administrator role. For more information, see Navigating to a Subaccount.
2. In the navigation area, choose Services > SAP Web IDE tile.
3. Choose SAP Web IDE configuration under Service Configuration.
4. Choose Edit under Application Permissions in the Destinations and Permissions section, and select either the AccountAdministrator role or the AccountDeveloper role from the dropdown list.

5. Choose the Roles section on the left.

6. Choose New Role and enter the name of the role in the corresponding field.

   Enter AccountAdministrator or AccountDeveloper in accordance with the Application Permissions you set in Step 4.

7. Choose Assign from the users section.

8. Enter the User ID (the P number) of the user in question and choose Assign.

   **Note**
   For more information how to check the User ID, see List and Edit User Details [page 205]. The User ID is a six-digit number preceded by the letter P.

**Results**

The assigned users can log on to SAP Web IDE with their credentials for SAP Cloud Platform Identity Authentication service (e-mail and password).
1.9.2.2 Assign Everyone Role

Context

If you want to use the Everyone role together with SAP Cloud Platform Identity Authentication service as an identity provider, complete the following steps:

Procedure

1. Log on to SAP Cloud Platform cockpit with the cockpit administrator role. For more information, see Navigating to a Subaccount.
2. In the navigation area, choose Services SAP Web IDE tile.
3. Choose SAP Web IDE configuration under Service Configuration.
4. Choose Edit under Application Permissions in the Destinations and Permissions section, and select the Everyone role from the dropdown list.

Results

Users can log on to SAP Web IDE with their credentials for SAP Cloud Platform Identity Authentication service (e-mail and password).

Related Information

Managing Roles and Permissions
Using the Subscriptions Panel
1.9.2.3 Show User's Name on SAP Web IDE Home Page

Context

When you use Identity Authentication as a trusted identity provider for SAP Web IDE you can configure the application to display the first name of the user that is logged on in the menu bar and the welcome screen.

For this scenario, you have to configure the user attribute First Name in Identity Authentication to be sent to SAP Web IDE in the assertion attribute. You also have to configure the First Name user attribute mapping for Identity Authentication in the SAP Cloud Platform cockpit.

Configure First Name User Attribute in SAP Cloud Platform Identity Authentication Service

Procedure

1. Access the tenant's administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
   This operation opens a list of the applications.
3. Choose your SAP Web IDE application from the list.
4. Choose the Trust tab.
5. Under SAML 2.0, choose Assertion Attributes.
6. Add the First Name assertion attributes.
7. Save your configuration.
If the operation is successful, you receive the message *Assertion attributes updated.*

## Configure Mapping in SAP Cloud Platform

### Procedure

1. In your Web browser, open the SAP Cloud Platform cockpit using the following URLs:
   - Europe: https://account.hana.ondemand.com/cockpit
   - United States: https://account.us1.hana.ondemand.com/cockpit
   - Australia: https://account.ap1.hana.ondemand.com/cockpit
2. Select the customer account and choose *Trust* in the navigation bar.
3. Choose the *Trusted Service Provider* subtab, and then choose the identity provider that SAP Web IDE uses for authentication.
4. Choose **Attributes** ➤ **Add Assertion-Based Attribute** ➤
5. Enter the fields as follows:

<table>
<thead>
<tr>
<th>Assertion Attribute</th>
<th>Principal Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>first_name</td>
<td>firstname</td>
</tr>
</tbody>
</table>

**Note**

- The *Assertion Attribute* field is for the attribute that comes from the SAML Assertion.
- The *Principal Attribute* field is the user attribute that the users will have at SAP Cloud Platform.

6. Save your changes.

### Results

Once the user has been successfully authenticated to SAP Web IDE, his or her name will appear in *Menu bar* on the right.
1.9.3 Integration with SAP Document Center

You can use SAP Cloud Platform Identity Authentication service as identity provider for SAP Document Center.

Prerequisites

- You have a subaccount for SAP Cloud Platform. For more information, see Getting a Global Account.
- You have an Identity Authentication tenant. For more information about how to get Identity Authentication, see SAP Cloud Platform Pricing and Packaging Options, or contact your SAP sales representative.
- You have registered the Identity Authentication as a trusted identity provider for your SAP Cloud Platform account. See Identity Authentication Tenant as an Application Identity Provider.
- You have set the trust with SAP Cloud Platform. For more details, see Configure Trust [page 55].
- You have added your SAP Document Center host to the list of the trusted domains in the administration console for Identity Authentication. For more information, see Configure Trusted Domains [page 138]. You have checked the User ID of the users that can access SAP Document Center. The User ID is a six-digit number preceded by the letter P. For more information about how to check the User ID, see List and Edit User Details [page 205].
- Optional (for the group assignment): You have created a user group in Identity Authentication and assigned that group to the users you want to give authorizations to access SAP Document Center.

Context

The integration between SAP Document Center and Identity Authentication enables users to access SAP Document Center with their Identity Authentication credentials. Identity Authentication users must be assigned to the specific Web roles for SAP Document Center. The specific roles contain the access authorizations for the user interfaces (UIs). For more information about the specific Web roles of SAP Document Center, see Assigning Users to Roles.

The configuration steps are done in the administration console of Identity Authentication and in the cockpit of SAP Cloud Platform.

1.9.3.1 Assign Identity Authentication Users to Roles

Context

You can use Java EE roles to define access to SAP Document Center. You can assign the respective roles for SAP Document Center to users or to groups of users of SAP Cloud Platform Identity Authentication service. For more information about the specific web roles for SAP Document Center, see Assigning Users to Roles.

You have three options to define access:
Assign Users to Roles

Context

Assign the respective roles for SAP Document Center to individual users of Identity Authentication.

Procedure

1. Log on to SAP Cloud Platform cockpit with the cockpit administrator role. For more information, see Navigating to a Subaccount.
2. In the navigation area go to Services SAP Document Center.

   ➔ Tip
   Choose Enable if the service is not enabled for this account.

3. Under Service Configuration choose Assign Roles & Set Destinations.
4. Under Roles select the role you want to manage assignments for. For more information about the specific web roles for SAP Document Center, see Assigning Users to Roles.
5. Choose Assign for the Individual Users section.
6. Enter the User ID (the P number) of the user in question and choose Assign.

   i Note
   For more information how to check the User ID, see List and Edit User Details [page 205]. The User ID is a six-digit number preceded by the letter P.

Results

The assigned user can log on to SAP Document Center with their credentials for Identity Authentication.
Assign Groups to Roles

Context

Assign the respective roles for SAP Document Center to collections of users of Identity Authentication instead of individual users. Groups allow you to easily manage the role assignments.

Assertion-based groups are groups determined by values of attributes in the SAML 2.0 assertion.

Procedure

1. Assign a group to users of Identity Authentication. For more information, see Assign Groups to a User [page 220].
   
   For example, you can have a group EVERYONE for all the users of Identity Authentication, and a group DocCenter_Admins just for the administrators. In this case, you should assign the group EVERYONE to all the users of Identity Authentication, and just the administrators to the DocCenter_Admins group.

2. Configure the groups attribute that is sent to SAP Document Center in the SAML 2.0 assertion. For more information, see Configure the User Attributes Sent to the Application [page 64]

3. In the cockpit of SAP Cloud Platform define the assertion based groups for the group-to-role mapping in the cockpit. For more information, see 4. (If Using an Identity Provider) Define the Group-to-Role Mapping.

Results

All users that are members of the group can access SAP Document Center.
1.9.3.2 Configure Assertion Attributes Mapping

You have to specify how the assertion attributes are sent to SAP Cloud Platform in the assertion, and define their mapping.

1. Configure User Attributes in Identity Authentication

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.
   - Note
   - The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   - Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Applications tile.
   - This operation opens a list of the applications.
3. Choose your SAP Cloud Platform application from the list.
4. Choose the Trust tab.
5. Under SINGLE SIGN-ON, choose Assertion Attributes.
6. Add the assertion attributes.
7. Save your configuration.

If the operation is successful, you receive the message Assertion attributes updated.
Related Information

Configure the User Attributes Sent to the Application [page 64]

2. Configure Mapping in SAP Cloud Platform

Procedure

1. Log on to SAP Cloud Platform cockpit. For more information, see Navigating to a Subaccount.
2. Select the subaccount and choose TRUST in the navigation bar.
3. Choose the Trusted Service Provider, the identity provider that the platform uses for authentication.
4. Choose Attributes > Add Assertion-Based Attribute.
5. Enter the fields as follows:

<table>
<thead>
<tr>
<th>Assertion Attribute</th>
<th>Principal Attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

i Note

This specifies that all assertion attributes will be mapped to the corresponding principal attributes without a change.

The Assertion Attribute field is for the attribute that comes from the assertion.

The Principal Attribute field is the user attribute that the users will have at SAP Cloud Platform.

6. Save your changes.

Related Information

Application Identity Provider

1.9.4 Integration with SAP Identity Management 8.0

SAP Identity Management can provision users to and from SAP Cloud Platform Identity Authentication service via the Identity Authentication connector. For more information about the setting up of an Identity Authentication system, see Setting up an Identity Authentication System.
1.9.5 Integration with Microsoft Azure AD

SAP Cloud Platform Identity Authentication service is part of the application gallery of Microsoft Azure Active Directory (Azure AD) under the name SAP Cloud Platform Identity Authentication. For more information, see SAP Cloud Platform Identity Authentication.

This integration aims to provide single sign-on (SSO) between applications using Azure AD as authenticating identity provider and applications using Identity Authentication as proxy identity provider.

Prerequisites

- You have a valid Azure AD subscription.
- You have a subscription for Identity Authentication. For more information how to get Identity Authentication, see Getting Started [page 32].

Overview

In this scenario Identity Authentication acts as a proxy identity provider and Azure AD as the main authentication authority for the applications. The authentication requests sent to Identity Authentication are redirected to Azure AD. User management and authentication is done on Azure AD side.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users who are in the Azure AD user store can use the single sign-on (SSO) functionality. Users who are provisioned to Identity Authentication, but not to Azure AD, are not able to log on.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Tip</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Authentication supports the Identity Federation option. This option allows the application to check if the users authenticated by the corporate identity provider exist in the user store of Identity Authentication. In the default setting, the Identity Federation option is disabled. If Identity Federation is enabled, only the users that are imported in Identity Authentication are able to access the application. For more information about how to enable or disable Identity Federation with Identity Authentication, see Enable Identity Federation with Identity Authentication in Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 266].</td>
</tr>
</tbody>
</table>

For this scenario, the configurations are made in Azure classic portal and in the administration console for Identity Authentication.
1. Configure Microsoft Azure AD [page 429]
2. Configure Microsoft Azure AD as Corporate Identity Provider at SAP Cloud Platform Identity Authentication Service [page 430]

1. Configure Microsoft Azure AD [page 429]
   Configure Microsoft Azure AD to integrate with SAP Cloud Platform Identity Authentication Service.

2. Configure Microsoft Azure AD as Corporate Identity Provider at SAP Cloud Platform Identity Authentication Service [page 430]
   Create and configure Azure AD as a corporate identity provider in the administration console for Identity Authentication.

### 1.9.5.1 Configure Microsoft Azure AD

Configure Microsoft Azure AD to integrate with SAP Cloud Platform Identity Authentication Service.

**Prerequisites**

You have a valid Azure AD subscription.

**Context**

For the configuration of Microsoft Azure AD see Tutorial: Azure Active Directory integration with SAP Cloud Platform Identity Authentication.

**i Note**

For the configuration you need the metadata of your Identity Authentication tenant. For more information about how to get it, see Tenant SAML 2.0 Configuration [page 130].

**Tip**

Download and save the Azure AD Metadata XML file. You will need it for the configuration of Azure AD as corporate identity provider at SAP Cloud Platform Identity Authentication Service.
1.9.5.2 Configure Microsoft Azure AD as Corporate Identity Provider at SAP Cloud Platform Identity Authentication Service

Create and configure Azure AD as a corporate identity provider in the administration console for Identity Authentication.

Prerequisites

- You have a subscription for Identity Authentication. For more information how to get Identity Authentication, see Getting Started [page 32].
- You have configured Microsoft Azure AD.

Context

To use Identity Authentication as a proxy, create, and configure Azure AD as a corporate identity provider in the administration console for Identity Authentication. This corporate identity provider is used as an authenticating authority for the applications.

Procedure

1. Access the tenant’s administration console for SAP Cloud Platform Identity Authentication service by using the console’s URL.

   i Note
   The URL has the https://<tenant ID>.accounts.ondemand.com/admin pattern.
   Tenant ID is an automatically generated ID by the system. The first administrator created for the tenant receives an activation e-mail with a URL in it. This URL contains the tenant ID.

2. Choose the Corporate Identity Providers tile.
3. Choose the Add button to create an Azure AD corporate identity provider.
i Note
If you have an Azure AD corporate identity provider in your list, choose it, and proceed with its configuration. Type the name of the identity provider in the search field to filter the list items.

4. Under SAML 2.0, choose SAML 2.0 Configuration.
5. Upload Azure AD metadata XML file or configure manually the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Provide the entity ID of the corporate identity provider.</td>
</tr>
<tr>
<td>Single Sign-On Endpoint URL</td>
<td>Provide the URL of the identity provider single sign-on endpoint that receives authentication requests. For Binding, choose the one that corresponds to respective single sign-on endpoint.</td>
</tr>
<tr>
<td>Single Logout Endpoint URL</td>
<td>Provide the URL of the identity provider’s single logout endpoint that receives logout messages. For Binding, choose the one that corresponds to respective single logout endpoint.</td>
</tr>
<tr>
<td>Signing Certificate</td>
<td>Provide the base64-encoded certificate used by the identity provider to digitally sign SAML protocol messages sent to Identity Authentication.</td>
</tr>
</tbody>
</table>

→ Tip
The information for the manual configuration is in the metadata XML file of Azure AD.

Next Steps

1. Choose Microsoft ADFS / Azure AD as the type for the configured corporate identity provider. For more information, see Choose Identity Provider Type [page 260].
2. Select the configured identity provider as the authenticating identity provider for the desired application. For more information, see Choose Default Identity Provider for an Application [page 112].

Task overview: Integration with Microsoft Azure AD [page 428]

Previous task: Configure Microsoft Azure AD [page 429]
1.10 Get Support

This document is to help users, administrators, and developers deal with issues from SAP Cloud Platform Identity Authentication service.

SAP Support Portal

You can report an incident on SAP Support Portal Home with a component BC–IAM–IDS.

SAP Community Network

You can start a discussion in the Security Community.

Related Information

Troubleshooting for Administrators [page 298]
Troubleshooting for Developers [page 399]

1.11 Updates and Notifications

SAP Cloud Platform Identity Authentication service has production releases (updates) every second Monday. For more information about the features delivered every takt, see the What’s New for Identity Authentication [page 12] published regularly. To get notifications for the new features and fixes every release, subscribe at the SAP Community wiki by choosing the Watch icon.

Reasons for Updates

- **Bi-weekly updates** (standard) - each second Monday.
- **Immediate updates** - in case of fixes required for bugs that affect productive application operations, or due to urgent security fixes.
Announcements

To receive regular information about landscape downtimes and news, you need to subscribe to the mailing list of SAP Cloud Platform. For more information, see Platform Updates and Notifications.
Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information. About the icons:

- Links with the icon 🌐: You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP’s gross negligence or willful misconduct.
- Links with the icon 🌐: You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.

The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP’s gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.