# Content

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>SAP Cloud Platform Identity Authentication Service.</td>
<td>4</td>
</tr>
<tr>
<td>1.1</td>
<td>Release Notes for Identity Authentication.</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td>Release Notes 2016.</td>
<td>6</td>
</tr>
<tr>
<td></td>
<td>Release Notes 2015.</td>
<td>9</td>
</tr>
<tr>
<td></td>
<td>Release Notes 2014.</td>
<td>12</td>
</tr>
<tr>
<td>1.2</td>
<td>Overview</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Product Details</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td>Web-Based Logon Interface.</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td>Landscape Host.</td>
<td>15</td>
</tr>
<tr>
<td></td>
<td>Supported Browser Versions.</td>
<td>16</td>
</tr>
<tr>
<td></td>
<td>Supported Languages.</td>
<td>17</td>
</tr>
<tr>
<td>1.3</td>
<td>Get Started</td>
<td>19</td>
</tr>
<tr>
<td>1.4</td>
<td>Scenarios</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Business-to-Consumer Scenario.</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Business-to-Business Scenario.</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Business-to-Employee Scenario.</td>
<td>24</td>
</tr>
<tr>
<td>1.5</td>
<td>Operation Guide</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Configure Applications</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Configure Tenant Settings</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>Password Policies</td>
<td>102</td>
</tr>
<tr>
<td></td>
<td>Configure Privacy Policies</td>
<td>109</td>
</tr>
<tr>
<td></td>
<td>Configure Terms of Use</td>
<td>113</td>
</tr>
<tr>
<td></td>
<td>User Management</td>
<td>117</td>
</tr>
<tr>
<td></td>
<td>User Groups</td>
<td>125</td>
</tr>
<tr>
<td></td>
<td>User Provisioning</td>
<td>133</td>
</tr>
<tr>
<td></td>
<td>Manage Administrators</td>
<td>141</td>
</tr>
<tr>
<td></td>
<td>Corporate Identity Providers</td>
<td>148</td>
</tr>
<tr>
<td></td>
<td>Social Identity Providers</td>
<td>169</td>
</tr>
<tr>
<td></td>
<td>Export Change Logs with a History of Administration Operations</td>
<td>173</td>
</tr>
<tr>
<td></td>
<td>Export Existing Users of a Tenant of SAP Cloud Platform Identity Authentication Service</td>
<td>177</td>
</tr>
<tr>
<td></td>
<td>View Usage Statistics</td>
<td>179</td>
</tr>
<tr>
<td></td>
<td>SAML 2.0</td>
<td>179</td>
</tr>
<tr>
<td></td>
<td>Troubleshooting for Administrators</td>
<td>180</td>
</tr>
<tr>
<td>1.6</td>
<td>User Guide</td>
<td>182</td>
</tr>
<tr>
<td></td>
<td>Two-Factor Authentication</td>
<td>184</td>
</tr>
<tr>
<td></td>
<td>Social Authentication</td>
<td>187</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>Use the Remember Me Option</td>
<td>189</td>
<td></td>
</tr>
<tr>
<td>Access Applications with Single Sign-On on Mobile Devices</td>
<td>190</td>
<td></td>
</tr>
<tr>
<td>Change Password</td>
<td>192</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting for Users</td>
<td>193</td>
<td></td>
</tr>
<tr>
<td>1.7 Developer Guide</td>
<td>194</td>
<td></td>
</tr>
<tr>
<td>API Authentication</td>
<td>194</td>
<td></td>
</tr>
<tr>
<td>API Documentation</td>
<td>197</td>
<td></td>
</tr>
<tr>
<td>Add Logon Overlays in Customer Applications</td>
<td>248</td>
<td></td>
</tr>
<tr>
<td>Configure Clickjacking Protection</td>
<td>250</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting for Developers</td>
<td>251</td>
<td></td>
</tr>
<tr>
<td>1.8 Security</td>
<td>253</td>
<td></td>
</tr>
<tr>
<td>1.9 Integration Scenarios</td>
<td>255</td>
<td></td>
</tr>
<tr>
<td>Integration with SAP Cloud Platform</td>
<td>255</td>
<td></td>
</tr>
<tr>
<td>Integration with SAP Web IDE</td>
<td>262</td>
<td></td>
</tr>
<tr>
<td>Integration with SAP Document Center</td>
<td>267</td>
<td></td>
</tr>
<tr>
<td>Integration with SAP Identity Management 8.0</td>
<td>272</td>
<td></td>
</tr>
<tr>
<td>Integration with Microsoft Azure AD</td>
<td>272</td>
<td></td>
</tr>
<tr>
<td>1.10 Get Support</td>
<td>275</td>
<td></td>
</tr>
<tr>
<td>1.11 Updates and Notifications</td>
<td>275</td>
<td></td>
</tr>
</tbody>
</table>
# 1 SAP Cloud Platform Identity Authentication Service

Table 1:

<table>
<thead>
<tr>
<th>Get Started</th>
<th>What’s New</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Details [page 13]</td>
<td></td>
</tr>
<tr>
<td>Get Started [page 19]</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scenarios</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security [page 253]</td>
</tr>
<tr>
<td></td>
<td>Integration Scenarios [page 255]</td>
</tr>
<tr>
<td></td>
<td>Get Support [page 275]</td>
</tr>
<tr>
<td></td>
<td>Download This Documentation as PDF</td>
</tr>
<tr>
<td></td>
<td>Terms of Use</td>
</tr>
<tr>
<td></td>
<td>Copyright and Trademarks</td>
</tr>
<tr>
<td></td>
<td>Privacy</td>
</tr>
<tr>
<td></td>
<td>Legal Disclosure</td>
</tr>
<tr>
<td></td>
<td>Disclaimer</td>
</tr>
</tbody>
</table>
## 1.1 Release Notes for Identity Authentication

### 28 March 2017 - Identity Authentication

**Table 2:**

<table>
<thead>
<tr>
<th>Announcement</th>
</tr>
</thead>
<tbody>
<tr>
<td>To improve the failover mechanism for Identity Authentication, we will add a new IP address (155.56.128.137) for the landscape host in Europe. If you have whitelisted the current IP, you also need to whitelist the new IP for the corresponding scenarios to work. For more information about Identity Authentication landscape hosts, see [Landscape Host](page 15).</td>
</tr>
</tbody>
</table>

### 07 March 2017 - Identity Authentication

**Table 3:**

<table>
<thead>
<tr>
<th>Enhancement</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP Cloud Identity service is renamed to SAP Cloud Platform Identity Authentication service (in short, Identity Authentication). The renaming includes changes in the following:</td>
</tr>
<tr>
<td>- UI texts, labels, and titles</td>
</tr>
<tr>
<td>- messages</td>
</tr>
<tr>
<td>- e-mail templates</td>
</tr>
<tr>
<td>- tenant logo</td>
</tr>
</tbody>
</table>

**Table 4:**

<table>
<thead>
<tr>
<th>Enhancement</th>
</tr>
</thead>
<tbody>
<tr>
<td>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](page 15).</td>
</tr>
</tbody>
</table>

### 10 January 2017 - Identity Authentication

**Table 5:**

<table>
<thead>
<tr>
<th>Enhancement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certain configuration options for the system applications are read-only. For more information, see [Configure a Trusted Service Provider](page 35), [Configure the User Attributes Sent to the Application](page 38), [Configure the Name ID Attribute Sent to the Application](page 41), [Configure the Default Attributes Sent to the Application](page 43), and [Choose Identity Provider for an Application](page 73).</td>
</tr>
</tbody>
</table>
Table 6:

**Enhancement**

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

Older Release Notes

- Release Notes 2015 [page 9]
- Release Notes 2014 [page 12]

1.1.1 Release Notes 2016

Table 7: Release Notes

The following table provides information about what was released in 2016. For more information about the latest release notes, see Release Notes for Identity Authentication [page 5]:

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2016-12-12 | ● Added search field for the master lists in the Import Users, Applications, Terms of Use Documents, Privacy Policy Documents, and Corporate Identity Providers tiles in the administration console.  
           | ● 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 Configure Applications [page 26]. |
| 2016-11-17 | ● 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 204].  
<pre><code>       | ● 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 Configure Applications [page 26]. |
</code></pre>
<p>| 2016-10-26 | ● The screen that appears after successful authentication is simplified. |
| 2016-10-10 | ● 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 38]. |
| 2016-10-03 | ● 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 76]. |
| 2016-09-14 | ● 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 106]. |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-08-30</td>
<td>● The SAP UI5 extension 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 250].</td>
</tr>
</tbody>
</table>
| 2016-08-05| ● Tenant administrator can change user type via the administration console for Identity Authentication. For more information, see List and Edit User Details [page 122].  
● Tenant administrator can upload terms of use and privacy policy documents, and e-mail templates in all supported languages. For more information, see Configure Privacy Policies [page 109], and Define an E-Mail Template Set for an Application [page 61]. |
| 2016-07-18| ● Identity Authentication master data texts can be changed and updated via API. For more information, see Change Master Data Texts [page 241].  
● Identity Authentication provides support for languages written in Right-To-Left (RTL) direction. For more information about the supported languages, see Supported Languages [page 17]. |
| 2016-07-04| ● Extended the user import via CSV file with the language 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 Import or Update Users for a Specific Application [page 68]. |
| 2016-06-20| ● Tenant administrator can specify a link, which 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. For more information, see Configure Logout URL [page 159].  
● Tenant administrator can change the user attributes taken from Microsoft Active Directory, or can also add additional attributes that are defined in the SCIM Enterprise User Schema Extension. For more information, see Configure SAP Cloud Platform [page 84]. |
| 2016-06-06| ● Tenant administrators can edit the E-Mail information in the administration console for Identity Authentication. For more information, see List and Edit User Details [page 122].  
● Added new attributes that are sent to the remote system in user provisioning. For more information about the supported attributes and the mapping between Identity Authentication and SAP Jam, see Provision Users to SAP Jam Target Systems [page 133]. |
| 2016-05-25| ● Country field in registration and upgrade form is required when Zip/Postal Code is filled in. For more information, see Configure Registration and Upgrade Forms [page 63].  
● Extended SCIM REST API with the possibility to create and update users with no password and no activation e-mail sending. Added new attributes: sendMail, mailVerified. For more information, see SCIM REST API [page 204].  
● Extended the SCIM REST API with corporateGroups attribute. For more information, see SCIM REST API [page 204]. |
| 2016-05-10| ● Extended SCIM REST API with new attributes: employeeNumber, costCenter, organization, division, department, manager, in accordance with the Enterprise User Schema Extension. For more information, see SCIM REST API [page 204].  
● Supports Employee Number as NameID attribute. For more information, see Configure the Name ID Attribute Sent to the Application [page 41].  
● Added Italian and Welsh to the supported languages for end user screens. For more information, see Supported Languages [page 17]. |
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2016-04-26 | ● Extended SCIM REST API with `passwordStatus`, `userType`, `sourceSystem`, and `socialIdentities` attributes. For more information, see [SCIM REST API][page 204].  
            | ● Extended the number of user attributes with a new section `Employee Information` in `User Details` view of the administration console. For more information, see [List and Edit User Details][page 122]. |
| 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 235].  
            | ● 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 51]. |
| 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 133].  
            | ● 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 SAP Jam Target System][page 140].  
            | ● Tenant administrators can search users in the administration console choosing between simple and advanced search. For more information, see [Search Users][page 120]. |
| 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 131].                                                                 |
| 2016-02-29 | ● Tenant administrators can provision users to SAP Jam instances. For more information, see [User Provisioning][page 133].  
            | ● Tenant administrators can delete a selected application in a tenant of `Identity Authentication`. For more information, see [Delete Applications][page 33].  
            | ● Tenant administrators can delete a selected corporate identity provider in a tenant of `Identity Authentication`. For more information, see [Delete Corporate Identity Providers][page 164]. |
| 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 166]. |
| 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 218], [Update User Resource][page 226], and [Delete User Resource][page 234].  
            | ● 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 166]. |
| 2016-01-18 | ● Tenant administrators can define rules for authentication in accordance with the risk. For more information, see [Configure Risk-Based Authentication][page 51].  
            | ● Tenant administrators can enable or disable the reload of the application’s parent page after a successful logon. For more information, see [Enable or Disable Reload Parent Page Option][page 60].  
            | ● SCIM REST API implementation of `Identity Authentication` supports create, update, and delete of user resources. For more information, see [Create User Resource][page 218], [Update User Resource][page 226], and [Delete User Resource][page 234]. |
# 1.1.2 Release Notes 2015

The following table provides information about what was released in 2015. For more information about the latest release notes, see [Release Notes for Identity Authentication](#page:5):

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-12-08</td>
<td>● Tenant administrators can delete one or more corporate identity providers in a tenant of Identity Authentication. For more information, see <a href="#page:164">Delete Corporate Identity Providers</a>.</td>
</tr>
<tr>
<td></td>
<td>● Added a new tenant administrator’s role - Manage Groups. For more details how to assign administrator roles, see <a href="#page:146">Edit Administrator Authorizations</a>.</td>
</tr>
<tr>
<td></td>
<td>2015-11-23</td>
</tr>
<tr>
<td></td>
<td>● Tenant administrators can configure the validity of the link sent to a user in the different application processes. For more information, see <a href="#page:78">Configure E-Mail Link Validity</a>.</td>
</tr>
<tr>
<td></td>
<td>● Tenant administrators can edit the user details information in the administration console for Identity Authentication. For more information, see <a href="#page:122">List and Edit User Details</a>.</td>
</tr>
<tr>
<td></td>
<td>2015-10-27</td>
</tr>
<tr>
<td></td>
<td>● Added optional parameter in the User Management REST API allowing the option not to send the activation e-mail. For more information, see <a href="#page:200">User Registration Service</a>.</td>
</tr>
<tr>
<td></td>
<td>● 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.</td>
</tr>
<tr>
<td></td>
<td>2015-10-12</td>
</tr>
<tr>
<td></td>
<td>● Tenant administrators can delete one or more user groups in a tenant of Identity Authentication. For more information, see <a href="#page:131">Delete User Groups</a>.</td>
</tr>
<tr>
<td></td>
<td>● Tenant administrators can change the certificate used by the identity provider to digitally sign the messages for the applications. For more information, see <a href="#page:76">Tenant SAML 2.0 Configuration</a>.</td>
</tr>
<tr>
<td></td>
<td>● 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 <a href="#page:95">Configure Kerberos Authentication</a>.</td>
</tr>
<tr>
<td></td>
<td>2015-09-28</td>
</tr>
<tr>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 189].  
● Users can access applications with single sign-on on mobile devices. For more details, see *Access Applications with Single Sign-On on Mobile Devices* under *Use the Remember Me Option* [page 189]. See also *Set Mobile Single Sign-On* [page 74].  
● Administrators can list the users that are assigned to a given user group. For more details, see *List Users in User Groups* [page 128]. |
| 2015-08-31 | ● Tenant administrator can disable IdP-Initiated process on tenant level. For more information see, *Configure IdP-Initiated SSO* [page 99].  
● 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 204]. |
| 2015-08-04 | ● Tenant administrator can list user groups in the tenant. For more information, see *List User Groups* [page 127].  
● Tenant administrator can create new user groups via the administration console for Identity Authentication. For More information, see *Create a New User Group* [page 126].  
● 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 129], *Unassign Users from Groups* [page 130].  
● 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 68].  
● Applications can search users by attribute via the SCIM REST API. For more information, see *Users Search* [page 205].  
● 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 38]. |
| 2015-07-06 | ● Tenant administrator creates new users in the administration console for Identity Authentication. For more information, see *Create a New User* [page 119].  
● Tenant administrator can configure social providers separately. For more information, see *Configure Social Identity Providers* [page 169]. |
| 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 120].  
● Tenant administrator deletes users in the administration console for Identity Authentication For more information, see *Delete Users* [page 123].  
● 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 84]. |
<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 48].  
• Administrator can set custom attributes with a CSV file. For more information, see Import or Update Users for a Specific Application [page 68].                                                                                                                                                                           |
| 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, and in the SAML 2.0 assertions. For the full list of the attributes, see Configure Registration and Upgrade Forms [page 63].  
• Application sets custom attributes via the user registration service. For more details, see User Registration Service [page 200].  
• 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 38].                                                                                     |
| 2015-04-13| • Administrator configures applications for two-factor authentication.  
  **Note**  
  This functionality has been updated. Now it is part of the Risk Based Authentication. For more information, see Configure Risk-Based Authentication [page 51].  
• Administrator deactivates all user mobile devices that generate passcodes for applications with two-factor authentication. For more information, see Deactivate User Devices for Two-Factor Authentication [page 124].  
• Administrator unlocks user passcode for two-factor authentication. For more information, see Unlock User Passcode [page 124].  
• 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 184], Activate a Device for Two-Factor Authentication [page 185], Deactivate Devices Configured for Two-Factor Authentication [page 186]. |
| 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 Identity Provider for an Application [page 73].  
• 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 122].                                                                                                           |
| 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 160].                                                                                                                                                                                                                          |
| 2015-03-02| • Delete one or more applications in a tenant of Identity Authentication. For more information, see Delete Applications [page 33].  
• Configure and visit the Home URL of an application. For more information, see Configure an Application’s Home URL [page 31], Visit an Application’s Web Page [page 32].  
• 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 68].                                                                                                                                 |
2015-02-16  • Edit administrators’ roles in the administration console for Identity Authentication. For more information, see Edit Administrator Authorizations [page 146].

2015-02-02  • Add users as administrators in the administration console for Identity Authentication. For more information, see Add Administrators [page 143].

2015-01-19  • List administrators in the administration console for Identity Authentication. For more information, see List Administrators [page 142].

1.1.3 Release Notes 2014

Table 9: Release Notes
The following table provides information about what was released in 2014. For more information about the latest release notes, see Release Notes for Identity Authentication [page 5]:

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
</table>
| 2014-12-08 | • Change the tenant’s display name. For more information, see Change a Tenant’s Display Name [page 81].
           | • Users created via CSV upload receive activation mail.
           | • Application specific logo. For more information, see Configure a Logo for an Application [page 55].
           | • Global tenant logo. For more information, see Configure a Tenant Logo [page 77].
           | • Configure SAML 2.0 trust by uploading metadata or by entering the service provider’s information manually. For more information, see Configure a Trusted Service Provider [page 35].
           | • 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 38].
           | • Configure attributes with default values for the application. For more information, see Configure the Default Attributes Sent to the Application [page 43].
           | • Choose which user attributes to be on the application’s registration and upgrade forms. For more information, see Configure Registration and Upgrade Forms [page 63].
           | • 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 44], Configure Social Identity Providers [page 169]. |
| 2014-09-01 | • Initial release.                                                                                                                                 |

1.2 Overview

SAP Cloud Platform Identity Authentication service is a cloud solution for identity lifecycle management for SAP Cloud Platform applications, and optionally for on-premise applications. It provides services for authentication,
single sign-on, and on-premise integration as well as self-services such as registration or password reset for employees, customer partners, and consumers. For administrators, Identity Authentication provides features for user lifecycle management and application configurations.

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.

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 25].

Related Information

Get Started [page 19]

1.2.1 Product Details

Table 10: 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>Users can log on to applications with their user name and password.</td>
<td>Scenarios [page 20]</td>
</tr>
<tr>
<td>Single sign-on to applications on SAP Cloud Platform</td>
<td>Users can access multiple cloud applications in the current session by authenticating just once in the Identity Authentication.</td>
<td>Scenarios [page 20]</td>
</tr>
<tr>
<td>Social sign-on to applications on SAP Cloud Platform</td>
<td>Users can link their Identity Authentication account with a social network account. That way users can be authenticated through a social identity provider.</td>
<td>Scenarios [page 20]Social Identity Providers [page 169], Social Authentication [page 187].</td>
</tr>
<tr>
<td>Customized branding</td>
<td>Administrators can configure branding styles for UI elements, e-mails, and error pages so that they comply with the company's branding requirements.</td>
<td>Configure a Tenant Logo [page 77], Configure a Logo for an Application [page 55], Configure a Branding Style for an Application [page 59], Define an E-Mail Template Set for an Application [page 61], Configure Registration and Upgrade Forms [page 63]</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 accept before registering. They are shown on the registration and upgrade forms.</td>
<td>Define a Terms of Use Document for an Application [page 116], Define a Privacy Policy Document for an Application [page 112].</td>
</tr>
</tbody>
</table>
### Feature | Description | More Information
--- | --- | ---
Customer security policy | Administrators can select a password policy from a list in accordance with the security requirements and the rules for resetting passwords. | Set a Password Policy for an Application [page 104]
Dedicated customer tenant | Customers are provided with guaranteed availability and specific configuration of their tenants. | Configure Tenant Settings [page 75]
User import functionality | Administrators can import new users into Identity Authentication or can update data for existing users. | Import or Update Users for a Specific Application [page 68]
User export functionality | Administrators can download information about existing users in the current tenant. | Export Existing Users of a Tenant of SAP Cloud Platform Identity Authentication Service [page 177]
Detailed change logs | Administrators can download a CSV file with information about the history of operations by tenant administrators. | Export Change Logs with a History of Administration Operations [page 173]
User Management | Administrators can manage the users in the tenant. | User Management [page 117]
Administrator Management | Administrators can add new administrators and edit administrator authorizations. | Manage Administrators [page 141]
User Groups | Administrators can create and delete user groups, and assign and unassign users. | User Groups [page 125]
Corporate User Store | SAP Cloud Platform Identity Authentication service can be configured to use a corporate user store in addition to its own user store. | Configure Connection to a Corporate User Store [page 84]
Kerberos Authentication | Administrators configure Kerberos authentication to allow users to log on without a username and password when they are in the corporate network. | Configure Kerberos Authentication [page 95]
Risk-Based Authentication | Administrators define rules for authentication in accordance with the risk | Configure Risk-Based Authentication [page 51]
Self-services | Users can use services to maintain or update their user profiles and to log on to applications. | User Guide [page 182]

### 1.2.2 Web-Based Logon Interface

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

When the overlay is not integrated in the application or the application does not provide a public one, or the user opens directly a protected page of the application, then the user is redirected to the logon page and it is displayed on fullscreen in the browser.

Related Information

Add Logon Overlays in Customer Applications [page 248]

1.2.3 Landscape Host

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

Use the landscapes as follows:

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

The productive landscape is available on a regional basis, where each region represents the location of a data center:

- Europe (the central region): accounts.ondemand.com
- United States: accounts.ondemand.com (US East)

A customer or partner account is associated with a particular data center and this is independent of your own location. You could be located in the United States, for example, but operate your account in Europe (that is, use a data center that is situated in Europe).

The landscape hosts and IP addresses are listed below:

<table>
<thead>
<tr>
<th>Data Center</th>
<th>Landscape Host</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td>accounts.ondemand.com</td>
<td>155.56.47.66 / 155.56.128.137</td>
</tr>
<tr>
<td>United States (US East)</td>
<td>accounts.ondemand.com</td>
<td>169.145.56.16</td>
</tr>
</tbody>
</table>
1.2.4 Supported Browser Versions

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 12: Microsoft Windows Browser Versions

<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 13: MAC OS X Browser Versions

<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, reset password, etc, of the applications that use SAP Cloud Platform Identity Authentication service for authentication support the following browsers:

Supported Desktop Browsers

Table 14:

<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 15:

<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>

1.2.5 Supported Languages
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, such as logon, forgot password, reset password, etc, of the applications that use SAP Cloud Platform Identity Authentication service for authentication support the following languages:

Table 16:

<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>
</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.

   **Note**

   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`.

   ![Source Code]
The locale is communicated to Identity Authentication by a direct GET request.

Source Code


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.

1.3 Get 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 have purchased a subscription for your Identity Authentication tenant, you receive an e-mail with a link to the landing of the administration console for Identity Authentication and you can confirm the registration of your first administrator user.

Note

If you experience troubles in accessing your Identity Authentication tenant, you can create an Incident on SAP Support Portal with a component BC-IAM-IDS.

Related Information

SAP Cloud Platform Pricing and Packaging Options
Overview [page 12]
Product Details [page 13]
Operation Guide [page 25]
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).

Related Information

Business-to-Consumer Scenario [page 20]
Business-to-Business Scenario [page 22]
Business-to-Employee Scenario [page 24]

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
- Customized privacy policy and terms of use
- Consumer security policy
- User import and export

Example

Michael Adams is an administrator at retail company A, and 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 and chooses 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.

Related Information

Operation Guide [page 25]
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 SAP Cloud Platform Identity Authentication service, 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.
Related Information

Operation Guide [page 25]
Developer Guide [page 194]
Configure User Access to the Application [page 67]
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 SAP Cloud Platform Identity Authentication service 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 about how to activate their accounts via the Forgot Password process. She also configures the trust on SAP Cloud Platform.

Because 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.
1.5 Operation Guide

This guide is for administrators, and 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.
1.5.1 Configure Applications

This section describes how you can configure the user authentication and access to an application, and how you can set your application to use a custom privacy policy, terms of use, a branding style, and e-mail templates in accordance with your company requirements. It also explains the trust configuration between SAP Cloud Platform Identity Authentication service and a service provider.

Types of Applications

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

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

**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, create a ticket on SAP Support Portal 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 29].

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 SAP Cloud Platform Identity Authentication service, or via the SCIM REST API.
- to customize the look and feel of the logon page of the Profile Page.

Configuring Applications

Table 17: 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>• [Create a New Application](page 29)</td>
</tr>
<tr>
<td></td>
<td>• [Change an Application's Display Name](page 30)</td>
</tr>
<tr>
<td></td>
<td>• [Configure an Application's Home URL](page 31)</td>
</tr>
<tr>
<td></td>
<td>• [Visit an Application's Web Page](page 32)</td>
</tr>
<tr>
<td>How to delete an application</td>
<td>• [Delete Applications](page 33)</td>
</tr>
<tr>
<td>How to configure trust</td>
<td>• [Configure a Trusted Service Provider](page 35)</td>
</tr>
<tr>
<td></td>
<td>• [Configure the Name ID Attribute Sent to the Application](page 41)</td>
</tr>
<tr>
<td></td>
<td>• [Configure the User Attributes Sent to the Application](page 38)</td>
</tr>
<tr>
<td></td>
<td>• [Configure the Default Attributes Sent to the Application](page 43)</td>
</tr>
<tr>
<td>How to manage authentications</td>
<td>• [Configure Authentication](page 44)</td>
</tr>
<tr>
<td>To learn about</td>
<td>See</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>How to configure API Authentication</td>
<td>• Configure a Certificate for API Authentication [page 49]</td>
</tr>
<tr>
<td></td>
<td>• Configure Credentials for HTTP Basic Authentication [page 48]</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>• Configure Terms of Use [page 113]</td>
</tr>
<tr>
<td></td>
<td>• Configure Privacy Policies [page 109]</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 116]</td>
</tr>
<tr>
<td></td>
<td>• Define a Privacy Policy Document for an Application [page 112]</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 77]</td>
</tr>
<tr>
<td></td>
<td>Specific for the application</td>
</tr>
<tr>
<td></td>
<td>• Display Application Name on Logon Page [page 57]</td>
</tr>
<tr>
<td></td>
<td>• Configure a Logo for an Application [page 55]</td>
</tr>
<tr>
<td></td>
<td>• Configure a Branding Style for an Application [page 59]</td>
</tr>
<tr>
<td></td>
<td>• Define an E-Mail Template Set for an Application [page 61]</td>
</tr>
<tr>
<td></td>
<td>• Configure Registration and Upgrade Forms [page 63]</td>
</tr>
<tr>
<td>How to configure access</td>
<td>• Configure an Application’s Home URL [page 31]</td>
</tr>
<tr>
<td></td>
<td>• Visit an Application’s Web Page [page 32]</td>
</tr>
<tr>
<td></td>
<td>• Configure User Access to the Application [page 67]</td>
</tr>
<tr>
<td></td>
<td>• Set a Password Policy for an Application [page 104]</td>
</tr>
<tr>
<td></td>
<td>• Import or Update Users for a Specific Application [page 68]</td>
</tr>
<tr>
<td>How to choose an identity provider for an application</td>
<td>• Choose Identity Provider for an Application [page 73]</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

To create a new 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.

   **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.

   **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.*

4. Configure the SAML 2.0 trust with the service provider.
5. If necessary, configure the application.

Related Information

- Configure a Trusted Service Provider [page 35]
- Configure Applications [page 26]
- Troubleshooting for Administrators [page 180]
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 146].

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 29].

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 180]
Create a New Application [page 29]
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**

Home URL is the URL that the user is redirected to after being authenticated. Initially, the **Home URL** for an application is not configured in the administration console for Identity Authentication. Once the URL has been set, you can change it.

> **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 68].

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.

   > **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 29].

4. Select the **Home URL** anchor text.
If you are configuring the URL for the first time, type the address in the pop-up dialog that appears.

If you are editing the URL, choose Edit from the list item, and type the new address 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.

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.

   **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 29].

4. Select the *Home URL* anchor text.

5. Choose *Visit*.

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

Related Information

Configure an Application’s Home URL [page 31]  
Create a New Application [page 29]

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 146].
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.

|i 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.

   |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 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.

   **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 a Trusted Service Provider

This document is intended to help you configure a trusted service provider (SP) in the administration console for SAP Cloud Platform Identity Authentication service by uploading its metadata or by entering the service provider 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.
Context

To configure a 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.

   **Note**
   
   The URL has the pattern `https://<tenant ID>.accounts.ondemand.com/admin`.
   
   **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 29].

4. Choose the **Trust** tab.

5. Under **SAML 2.0**, 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.

   **Note**
   
   Use a file with an extension .xml.

   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>
## Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single Logout Endpoint</td>
<td>The SP’s endpoint URL that receives the logout response or request (for a scenario with multiple service providers) from Identity Authentication for the termination of all current sessions.</td>
</tr>
<tr>
<td>Signing Certificate</td>
<td>A base64-encoded certificate used by the service provider to digitally sign 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. **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**

   To see how to download the SAML 2.0 metadata describing Identity Authentication as identity provider read Tenant SAML 2.0 Configuration [page 76].

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 255].

### Related Information

- Troubleshooting for Administrators [page 180]
- Integration with SAP Cloud Platform [page 255]
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 in the SAML 2.0 assertion.

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.

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

Table 18:

<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>
</tbody>
</table>

**Note**

For example, consumer, partner, or employee.

Street Address         | street                  |
Street Address 2       | street2                 |
City                   | city                    |
ZIP/Postal Code        | zip                     |
Country                | country                 |
State/Province         | state                   |
Cost Center            | cost_center             |
<table>
<thead>
<tr>
<th>User Attribute</th>
<th>Assertion Attribute Name</th>
</tr>
</thead>
<tbody>
<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>

**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>

**Note**

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 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.

Remember

In scenarios when the application is using for authentication a corporate identity provider, and the Identity Federation option is disabled, the user attributes configurations in the administration console for Identity Authentication are not relevant. In such scenarios Identity Authentication sends to the application the user attributes that come form the corporate identity provider without changing them. For more information about the corporate identity provider scenario, see Corporate Identity Providers [page 148] and Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 166].

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 29].

4. Choose the Trust tab.
5. Under SAML 2.0, 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.
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
  
  **Note**
  This is the default setting.

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

**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.

**Remember**

In scenarios when the application is using for authentication a corporate identity provider, and the Identity Federation option 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 148] and Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 166].

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.

   **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 29].

4. Choose the Trust tab.

5. Under SAML 2.0, choose Name ID Attribute.

6. Select the checkbox for the attribute.

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 180]
Create a New Application [page 29]
SAML 2.0 [page 179]
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. These attributes are sent from SAP Cloud Platform Identity Authentication service to the application in the SAML 2.0 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.

**Remember**

In scenarios when the application is using for authentication a corporate identity provider, and the Identity Federation option 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 148] and Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 166].

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.

   **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 29].

4. Choose the Trust tab.

5. Under SAML 2.0, choose Default Attributes.

6. Add the default attributes with their values to be sent to the application.
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 38]
Troubleshooting for Administrators [page 180]
Create a New Application [page 29]
SAML 2.0 [page 179]

1.5.1.10 Configure Authentication

Table 19:

<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 51]</td>
</tr>
<tr>
<td>Enable social sign-on authentication for an application</td>
<td>Enable or Disable Social Sign-On for an Application [page 44]</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 47]</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 48]</td>
</tr>
</tbody>
</table>

1.5.1.10.1 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 169].

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.

   **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 29].

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 169].

Related Information

Create a New Application [page 29]
1.5.10.2 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 95].

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.on-demand.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 29].

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.

For more information about the API methods, see Invitation REST API [page 198] and User Management REST API [page 200].

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.

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 29].

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.

1.5.1.10.3.2 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 29].

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 29]
*Invitation REST API* [page 198]
*User Management REST API* [page 200]
1.5.1.10.4 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) and group membership 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, starting 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** or **Group**.

**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 of Identity Authentication 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 create a ticket with a subject on SAP Support Portal 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 53]</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 Two-Factor Authentication)**

Donna Moore, as an administrator of company A, would like to configure Identity Authentication to always ask the company employees for a password and a 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: Two-Factor Authentication

Michael Adams, as an employee of company A, wants to create a leave request and is prompted to provide two factors (a password and a passcode generated by an authenticator app on his mobile device) to log on to the Leave Request application, regardless of whether he 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, and approves this by logging on to the application with two factors (a password and a passcode generated by her mobile device).

**Example 2**

Donna Moore, as an administrator of company A, would like to configure Identity Authentication to allow the company employees to log on to a Leave Request application from the corporate network with a user name and a
password and from any other network with a user name, a password and a passcode (two-factor authentication). 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. For this purpose, Donna creates the following rules:

**Authentication Rules**

Table 20:

<table>
<thead>
<tr>
<th>Action</th>
<th>IP Range</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>189.101.112.1/16</td>
<td>Employees</td>
</tr>
<tr>
<td>Two-Factor Authentication</td>
<td>Any</td>
<td>Employees</td>
</tr>
<tr>
<td>Two-Factor Authentication</td>
<td>Any</td>
<td>Managers</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 his username and password. When he is on a business trip, he can create leave requests by providing two factors (a password 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 and approves this by logging on to the application with two factors (a password and a passcode generated by her Android phone).

**Related Information**

Add a New Rule [page 53]
Create a New Application [page 29]
Unlock User Passcode [page 124]
Two-Factor Authentication [page 184]

**1.5.1.10.4.1  Add a New Rule**

**Context**

Each rule contains the following information:

- **Action**
  This action will be performed if the IP range or the Groups membership 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 logon to the application, they get the following message: *Sorry, but you are currently not authorized for access.*

- **Two-Factor Authentication**
  SAP Cloud Platform Identity Authentication service asks for two factors to authenticate the user. If you set two-factor authentication, users are required to provide a one-time password (OTP) called a passcode in addition to their primary credentials. Users also need to install an authenticator application, for example SAP Authenticator, on their mobile devices to generate passcodes.

  **Note**
  Passcodes are time-based and valid for one logon attempt only.

This field is mandatory.

- **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.

  **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 125].

  The fields **IP Range** and **Group** are not mandatory, but one of both 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.
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 of SAP Cloud Platform Identity Authentication service 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 create a ticket with a subject on SAP Support Portal under the component BC-IAM-IDS.

4. Choose the Authentication and Access tab.

5. Under AUTHENTICATION, choose Risk-Based Authentication.


7. Fill in the fields on the New Risk-Based Authentication Rule window.

8. Confirm your changes.

Related Information

Create a New Application [page 29]

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.

   - **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 29].

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 29]
- Troubleshooting for Administrators [page 180]
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 146].

Context

The application's display name is the name that appears on the left side of the logon and registration pages of the applications that use SAP Cloud Platform Identity Authentication service 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 29] and Change an Application's Display Name [page 30].

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 55].

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.

   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 29].

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, or you can 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.

  **Note**
  This is the default setting.

- **Custom Theme**
  The custom theme allows you to configure a custom branding style for the buttons, and uses the Default theme for all other elements on the forms. For this configuration, you can customize the top and bottom background color of the button, the button’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.

   **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 29].

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 button colors. To configure the button colors, you can use the color picker or enter the color’s hexadecimal value.

7. Save your selection
   
   Once the application has been changed, the system displays the message Theme changed to <name of theme>.

---

**Related Information**

Troubleshooting for Administrators [page 180]
Create a New Application [page 29]

---

### 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.

**Note**

By default the **Reload Parent Page** option is enabled. Disable the option if you would like to embed the login 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.

   **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 29].

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

**Context**

The template set contains templates for different application processes such as self-registration, on-behalf registration, invitation, and password upgrade. 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, you have to set it to the respective application.

To use a custom template set, you can request it from an operator of SAP Cloud Platform Identity Authentication service. You need to create an incident on the **SAP Support Portal** with a component **BC-IAM-IDS**. You should provide information of the content of the e-mail template for the respective application process. For that purpose, you need to open the template set for the respective application process from the links in the table below, edit the texts according to your needs, and attach your versions of the documents in the incident.

If you want to use a custom template set in another language, you need to open the template set for the respective application process from the links in the table below, edit the texts in the respective language, and attach your versions of the documents in the ticket.

**Caution**

You should use the same placeholders as those used in the template documents.

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:

- English
- German
- Spanish
Table 21: E-Mail Templates

<table>
<thead>
<tr>
<th>Application Process Template</th>
<th>Usage</th>
<th>Template Set Links</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Self-Registration</strong></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 ● TXT document</td>
</tr>
<tr>
<td><strong>On-Behalf Registration</strong></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 ● TXT document</td>
</tr>
<tr>
<td><strong>Invitation</strong></td>
<td>This e-mail template is used when a user is invited to register. It should contain registration information.</td>
<td>● HTML document ● TXT document</td>
</tr>
<tr>
<td><strong>Forgot Password</strong></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 ● TXT document</td>
</tr>
<tr>
<td><strong>Locked-Password</strong></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 ● TXT document</td>
</tr>
<tr>
<td><strong>Reset Password</strong></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 ● TXT document</td>
</tr>
</tbody>
</table>

**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.

   **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 29].

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.

Related Information

Troubleshooting for Administrators [page 180]
Create a New Application [page 29]

1.5.1.16 Configure Registration and Upgrade Forms

In the administration console, you can configure which user attributes SAP Cloud Platform Identity Authentication service sends to the service provider 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.
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
- 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 field, 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 field, 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" that 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, since the legislation in some countries require 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 pattern `<tenant ID>.accounts.ondemand.com/admin`. **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 29].

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 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.

  **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 80].

- **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 119].

  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 68].

- **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 68].

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 29].

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 180]
Create a New Application [page 29]
Risk-Based Authentication as an Alternative to Restrict User Access Option in SAP Cloud Platform Identity Authentication Service

1.5.118 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, and 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 146].
● You have uploaded the service provider’s metadata or entered the information manually. For more information see, Configure a Trusted Service Provider [page 35].

**Note**
You need the metadata to configure the trust between the service provider and SAP Cloud Platform Identity Authentication service, 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 67].

The CSV file contains columns such as status, loginName, mail, firstName, lastName, language validTo, validFrom, spCustomAttribute1, spCustomAttribute2, spCustomAttribute3, spCustomAttribute4, spCustomAttribute5, and groups.

The status, mail and lastName columns are mandatory, and they must always have values.

The status, loginName, mail and firstName columns must be with a string value of up to 32 characters. The lastName column 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 will receive the activation e-mail in that language.

The validFrom and validTo columns must be with a string value in the Zulu format yyyyMMddHHmmss'Z'.

**Note**
The information in the validFrom and validTo columns can be processed by the service provider in order to limit user access, but it would not affect the authentication of the user.

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 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.
**Note**

If you enter the data in the CSV file as text, you must separate the entries with commas. If you enter more than one value in a single entry, separate the values within the entry with commas and enclose the entry in quotation marks.

**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>logName</th>
<th>mail</th>
<th>fName</th>
<th>lName</th>
<th>language</th>
<th>validFrom</th>
<th>validTo</th>
<th>spCustomAttr1</th>
<th>groups</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>EID0000 1</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>2011090112000 0Z</td>
<td>2015090112000 0Z</td>
<td>Industry</td>
<td>Managers, Employees, HR</td>
</tr>
<tr>
<td>active</td>
<td>EID0000 2</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>2011090112000 0Z</td>
<td>2015090112000 0Z</td>
<td>Department</td>
<td>Employees</td>
</tr>
<tr>
<td>active</td>
<td>EID0000 3</td>
<td><a href="mailto:donna.mooore@example.com">donna.mooore@example.com</a></td>
<td>Donna</td>
<td>Moore</td>
<td>de</td>
<td>2011090112000 0Z</td>
<td>2016090112000 0Z</td>
<td>Shift</td>
<td>HR</td>
</tr>
<tr>
<td>active</td>
<td>EID0000 4</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>2011090112000 0Z</td>
<td>2018090112000 0Z</td>
<td>Unit</td>
<td>IT</td>
</tr>
<tr>
<td>active</td>
<td>EID0000 5</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>2011090112000 0Z</td>
<td>2014090112000 0Z</td>
<td>Administrators</td>
<td></td>
</tr>
<tr>
<td>inactive</td>
<td>EID0000 6</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>2011090112000 0Z</td>
<td>2016090112000 0Z</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:
The users that have not received activation e-mails will receive such e-mails, and then can activate their accounts and log on.

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.

   **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.

   **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 29].

4. Choose the **Browse...** button and specify the location of the CSV file.
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><strong>Do nothing</strong></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 Send E-Mails.</td>
</tr>
<tr>
<td><strong>Repeat steps 1 to 5</strong></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 Send E-Mails.</td>
</tr>
<tr>
<td><strong>Choose Send E-Mails</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>

**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 31].

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 180]
Configure an Application’s Home URL [page 31]
Configure User Access to the Application [page 67]
List User Groups [page 127]
Create a New User Group [page 126]
Edit Administrator Authorizations [page 146]
Export Existing Users of a Tenant of SAP Cloud Platform Identity Authentication Service [page 177]
1.5.1.19 Choose Identity Provider for an Application

This section shows you how to choose an identity provider for an application.

Prerequisites

- You have the Manage Corporate Identity Providers role.
- You have a configured corporate identity provider. For more information how to configure a corporate identity provider, see Related Information.

Context

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

- Default Identity Provider
  Identity Authentication is set as the default identity provider. The default identity provider gives you access to all application settings in the administration console for Identity Authentication
- Corporate Identity Provider
  Identity Authentication can act as a proxy to delegate authentication to the external corporate identity provider.

Note

If you select this option, 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.

Restriction

The option to choose an identity provider for the system applications is disabled. The default setting for these applications is Identity Authentication, set as the default identity provider.

To choose an 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.

Note

The URL has the pattern https://<tenant ID>.accounts.ondemand.com/admin.
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 29).

4. Choose the **Trust** tab.
5. Under **AUTHENTICATING IDENTITY PROVIDER**, choose **Identity Provider**.
6. Select the radio button of the identity provider that the application will use.
7. Save your changes.

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

### Related Information

- [Corporate Identity Providers](page 148)
- [Configure Trust with Corporate Identity Provider](page 160)
- [Edit Administrator Authorizations](page 146)

### 1.5.1.20 Set Mobile Single Sign-On

The mobile single sign-on (SSO) feature allows users to access applications protected with two-factor authentication without the need to manually enter the one-time password (OTP), also called a passcode, 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, which 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=[username]&j_otpcode=[passcode]
```
**Note**

The QR code represents this URL. When SAP Authenticator calls the URL, it replaces the [username] part of the URL with the specified account name and the [passcode] part with two consecutive passcodes.

**Related Information**

Configure IdP-Initiated SSO [page 99]
Use the Remember Me Option [page 189]
One-Time Password Authentication User Guide

### 1.5.2 Configure Tenant Settings

Initially, the tenants are configured to use default settings. This section describes how you as a tenant administrator can update the tenant display name, configure a global logo for the tenant, and view and download SAML 2.0 configuration.

<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 77]</td>
</tr>
<tr>
<td>How to configure the tenant’s name</td>
<td>Change a Tenant’s Display Name [page 81]</td>
</tr>
<tr>
<td>How to view and download tenant SAML 2.0 metadata</td>
<td>Tenant SAML 2.0 Configuration [page 76]</td>
</tr>
<tr>
<td>How to upload a new signing certificate</td>
<td>Tenant SAML 2.0 Configuration [page 76]</td>
</tr>
<tr>
<td>How to configure the validity of the link sent to a user in the different application processes.</td>
<td>Configure E-Mail Link Validity [page 78]</td>
</tr>
<tr>
<td>The corporate user store scenario and how to configure SAP Cloud Platform Identity Authentication service to connect with your corporate user store</td>
<td>Corporate User Store [page 82] and Configure Connection to a Corporate User Store [page 84]</td>
</tr>
<tr>
<td>How to configure Kerberos authentication</td>
<td>Configure Kerberos Authentication [page 95]</td>
</tr>
<tr>
<td>How to disable or enable IdP-Initiated process via the administration console for SAP Cloud Platform Identity Authentication service.</td>
<td>Configure IdP-Initiated SSO [page 99]</td>
</tr>
<tr>
<td>How to protect an application when using responsive UIs, or embedded frames</td>
<td>Configure Trusted Domains [page 80]</td>
</tr>
</tbody>
</table>
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 via the administration console for SAP Cloud Platform Identity Authentication service.

Context

To view and download the tenant SAML 2.0 metadata, or to change the name format, or the default certificate used by the identity provider to digitally sign the messages, 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 **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.

   **i 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), and 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 25:

<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>

**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 service provider side every time you change the name format of the identity provider in the administration console for Identity Authentication. 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**

Configure Tenant Settings [page 75]
Troubleshooting for Administrators [page 180]
SAML 2.0 [page 179]

**1.5.2.2 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 means that this logo is displayed in the footer or in the 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.

   **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 *Logo* list item.
4. Upload an image with height 36 pixels.

   **Note**
   
The image file must have one of the following extensions: `.png`, `.gif`, or `.jpeg`.

   **Note**
   
   If the height of the image is larger than 36 pixels, the user forms will show the logo proportionally resized to a height of 36 pixels as the quality will be preserved.

   If the height of the image is lower than 36 pixels, the user forms will resize the image as 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.*

**1.5.2.3 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 (self-registration, on-behalf registration, invitation, forgot password, locked password, reset password) 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:

Table 26: 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. 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.

   i **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.*

1.5.2.4 Configure Trusted Domains

This document describes how service providers that delegate authentication to SAP Cloud Platform Identity Authentication service 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 have to add the domains of these applications as trusted in the administration console for SAP Cloud Platform Identity Authentication service. 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 67].

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.*
1.5.2.5 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.

   **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. Click on 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

Configure Tenant Settings [page 75]
Troubleshooting for Administrators [page 180]
1.5.2.6 Corporate User Store

If you have an existing on-premise user store, you can configure SAP Cloud Platform Identity Authentication service to use the corporate user store in addition to its own cloud user store. This integration will allow 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 account 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.

Authentication Flow

When the Corporate User Store option is configured properly, and a user tries to access a trusted application for the first time with the on-premise credentials, Login Name and Password entered correctly, the 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 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 84]. With subsequent logins, the user is always authenticated against the corporate user store, and the user record is updated.

For the first login 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.

Note

The user in the corporate user store must have the mail attribute.

The tenant administrator needs to monitor and prevent the co-existence of a cloud and on-premise user with one and the same e-mail address. The tenant administrator has to instruct the users to login for the first time with their Login Name, not with the E-Mail.

If a user who has a user record in the cloud user store is deleted in the corporate user store, she or he will not be able to 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 123].

For all these 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 51] and Assign Groups to a User [page 129].

Control Access to Applications and Resources

In the scope of the Corporate User Store scenario, you can manage access to applications and their resources on the basis of the groups that are 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 38].

Note

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 on the basis of membership in a corporate user group by setting different rules via risk-based authentication. For more information, see Configure Risk-Based Authentication [page 51].
1.5.2.6.1 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 SAP Cloud Platform Identity Authentication service with details taken 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 84].

Related Information

Security [page 253]

1.5.2.6.2 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 SAP Cloud Platform Identity Authentication service.

For more details about how to configure these systems, see:

- Configure SAP Cloud Platform [page 84]
- Configure SAP Cloud Platform Identity Authentication Service [page 94]

1.5.2.6.3 Configure SAP Cloud Platform

Context

The configuration of SAP Cloud Platform depends on the type of the user store. You have two options for this: LDAP user store and SAP NW AS Java user store.

Configure SAP Cloud Platform When Connecting to an LDAP User Store

Procedure

1. In the SAP Cloud Platform cockpit, choose Services in the navigation area Identity Authentication Add-On > Enable in the detailed view of the service.
You can log on to the cockpit at the URLs given below. Use the relevant URL for your associated region:

- Europe: https://account.eu1.hana.ondemand.com/cockpit
- United States: https://account.us1.hana.ondemand.com/cockpit
- Asia-Pacific: https://account.ap1.hana.ondemand.com/cockpit

This will enable the extension service of SAP Cloud Platform Identity Authentication service named proxy and provided by an SAP Cloud Platform account named sci.

**Caution**

If you don’t see the Identity Authentication Add-On tile in the cockpit, you need to create a ticket with a subject “Enable Corporate User Store Feature” on SAP Support Portal under the component BC-IAM-IDS. You have to provide information about your SAP Cloud Platform account name and data center.

2. In your consumer account on SAP Cloud Platform, register an OAuth client for the subscribed proxy application provided by the sci account.

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 list.

For more information about how to register an OAuth client, see Registering an OAuth Client.

3. Install an SAP Cloud Platform Connector in your corporate network.

For more information, see Installing the Cloud Connector.

4. 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.

5. Connect SAP Cloud Platform with your corporate user store.

**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 Configuring User Store in the Cloud Connector.

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 contain the users and groups, respectively. For example, if the tree has the following structure:
The user and group paths should appear as in the table below:

<table>
<thead>
<tr>
<th>Table 27:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User Path</td>
<td>ou=People,dc=example,dc=com</td>
</tr>
<tr>
<td>Group Path</td>
<td>ou=People,dc=example,dc=com</td>
</tr>
</tbody>
</table>

6. **Optional:** Change the default attributes or include additional attributes.

**Note**

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 Configuring User Store in the Cloud Connector.

In this section provide the same information as when you specified the SAP Cloud Platform settings in the previous step.

```java
{
   "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 contain Domain suffix, e.g. "john@ACME.COM"",
  "Password": "<Password of this user>"
},

We recommend that you configure this section, if you want to use SSL.

"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>",
"IsActiveDirectory": "<Possible values are "true" (default value if missing) or "false". "true" indicates that the LDAP server is Active Directory>",
"ExcludeUsersAttribute": {
  "AttributeName": "<Name of user attribute that will be used to exclude some users from the result depending on their type. Attribute is treated as bitwise. Such attribute for Active Directory is "UserAccountControl">",
  "AttributeMask": "<Bitwise mask represented as decimal value. In case any of the high bits of this mask match with the corresponding bit of the value of the above attribute, the user will be excluded from the result. Example mask for Active Directory is 67121154 - it is the sum of the following flags ACCOUNTDISABLE(2), WORKSTATION_TRUST_ACCOUNT(4096), SERVER_TRUST_ACCOUNT(8192) and PARTIAL_SECRETS_ACCOUNT(67108864)>"
},

You can keep these default configurations unchanged.

"MaxQueryTime": "60000",
"MaxQueryResults": "1000",
"MaxConnectionPoolSize": "10",
"PoolConnectionTimeout": "300000",
"CacheSize": "1000",
"CacheEntryValidity": "300000",
"MaxNumberOfFailedLogonAttempts": 5,
"UserLockTimeout": 1800000,
"UserObjectClass": "user",
"GroupObjectClass": "group",
"GroupAttributeDisplayName": "cn",
"UserGroupRelation": {
  "SourceClass": "user",
  "SourceAttribute": "memberOf"
},

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.

```json
{
"SingularAttributes": [ 
{
  "SCIMAttribute": "userName",
  "mappings": [ 
   { "LDAPAttribute": { 
     "name": "sAMAccountname"
   }
  ]
 },
  "SCIMAttribute": "name",
  "mappings": [ 
   { "SCIMSubAttribute": "givenName",
     "LDAPAttribute": { 
     "name": "givenName"
   }
 },
   { "SCIMSubAttribute": "familyName",
     "LDAPAttribute": { 
     "name": "sn"
   }
 },
   { "SCIMSubAttribute": "honorificPrefix",
     "LDAPAttribute": { 
     "name": "personalTitle"
   }
   ]
 },
  "SCIMAttribute": "displayName",
  "mappings": [ 
   { "LDAPAttribute": { 
     "name": "displayName"
   }
  ]
 },
  "SCIMAttribute": "locale",
  "mappings": [ 
   { "LDAPAttribute": { 
     "name": "locale"
   }
  ]
 },
  "SCIMAttribute": "timeZone",
  "mappings": [ 
   { "LDAPAttribute": { 
     "name": "timezone"
   }
  ]
 ]
}
```
},
{

},
{

},
{

},
{

{

},

]
"SCIMAttribute": "employeeNumber",
"mappings": [
{
"LDAPAttribute": {
"name": "<LDAP property containing the employee number"
}
}
]
"SCIMAttribute": "division",
"mappings": [
{
"LDAPAttribute": {
"name": "<LDAP property containing the division>"
}
}
]
"SCIMAttribute": "department",
"mappings": [
{
"LDAPAttribute": {
"name": "<LDAP property containing the department>"
}
}
]
"SCIMAttribute": "organization",
"mappings": [
{
"LDAPAttribute": {
"name": "company"
}
}
]
"SCIMAttribute": "costCenter",
"mappings": [
{
"LDAPAttribute": {
"name": "<LDAP property containing the cost center>"
}
}
]

}
],
"MultiValuedAttributes": [
{
"SCIMAttribute": "emails",
"values": [
{
"primary": "true",
"mappings": [
{
"SCIMSubAttribute": "value",
"LDAPAttribute": {
"name": "mail"
}
}

SAP Cloud Platform Identity Authentication Service
SAP Cloud Platform Identity Authentication Service

PUBLIC

89


"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"
}
},
{
"SCIMSubAttribute": "locality",
"LDAPAttribute": {
"name": "l"
}
},
"SCIMSubAttribute": "region",
"LDAPAttribute": {
"name": "st"
}
]
The following table shows the default mapping between the Active Directory user attributes and the SCIM attributes, and the existing mapping between the SCIM attributes and the attributes in the user store of Identity Authentication.

Table 28: 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>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>
</tbody>
</table>
Microsoft Active Directory Attributes | SCIM Attributes | SAP Cloud Platform Identity Authentication Service User Store Attribute
--- | --- | ---
st | Addresses.region | state
postalCode | Addresses.postalCode | zip
co | Addresses.country | country

**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.

d. Save your changes.
This file overwrite the configurations you made in Configuring User Store in the Cloud Connector.

**Next Steps**

Configure SAP Cloud Platform Identity Authentication Service [page 94]

**Configure SAP Cloud Platform When Connecting to an SAP NW AS Java User Store**

**Procedure**

1. In the SAP Cloud Platform cockpit, choose Services tab > Identity Authentication Add-On > Enable in the detailed view of the service.

   **Note**

   You can log on to the cockpit at the URLs given below. Use the relevant URL for your associated region:
   - Europe: https://account.eu1.hana.ondemand.com/cockpit
   - United States: https://account.us1.hana.ondemand.com/cockpit
   - Asia-Pacific: https://account.ap1.hana.ondemand.com/cockpit

   This will enable the extension service of Identity Authentication named `proxy` and provided by an SAP Cloud Platform account named `sci`.

2. In your consumer account on SAP Cloud Platform, register an OAuth client for the subscribed `proxy` application provided by the `sci` account.

   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 drop down list.

For more information about how to register an OAuth client, see Registering an OAuth Client.

3. Install an SAP Cloud Platform Connector in your corporate network.

For more information, see Installing the Cloud Connector.

4. 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.

5. Connect SAP Cloud Platform with your corporate user store.

   Note

   For this scenario, you have to do the following:
   ○ In the configuration of SAP Cloud Platform Connector, configure the host mapping to the on-premise system. For more information, see Configuring 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.
   ○ In the configuration of SAP Cloud Platform cockpit, create a destination to the on-premise system.

   Note

   The relevant prerequisites for this scenario are:
   ○ You have a 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.

   Since Identity Authentication has already deployed the proxy application, you should start from the 2. Configure the On-Premise System section in the documentation.

   For more information, see Using an SAP System as an On-Premise User Store

   When configuring the destination to the on-premise system, make sure of the following:
   ○ The Type is None.
   ○ The protocol of the URL is HTTP.
   ○ The URL of the destination, the host name and the port should coincide with the virtual host name and virtual port from the setup of the access control in SAP Cloud Platform Connector.
   ○ The Proxy Type is OnPremise.
   ○ The Authentication is BasicAuthentication.
Next Steps

Configure SAP Cloud Platform Identity Authentication Service [page 94]

1.5.2.6.4 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.

   **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 Corporate User Store list item.

   **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 account’s data center, enter your SAP Cloud Platform consumer account, and the OAuth client ID and secret.

   **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 consumer account.

   The Account Name field in the administration console for Identity Authentication has to match your SAP Cloud Platform Account Name.

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 login requires Login Name and password. After successful authentication, a new user record is created in Identity Authentication with type employee.
1.5.2.7 Configure Kerberos Authentication

Overview

You configure Kerberos authentication for SAP Cloud Platform Identity Authentication service in order 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 and 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.

2. Identity Authentication returns a response with status code **401 Unauthorized**. The response contains a **WWW-Authenticate: Negotiate** header.

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 login name, and authenticates the user.

**Related Information**

Kerberos: The Network Authentication Protocol

**1.5.2.7.1 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 255].

- The users logging on with Kerberos authentication exist in the cloud user store with the required details. Each user has to have a login 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 68]
1.5.2.7.2 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 SAP Cloud Platform Identity Authentication service.

   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.
1.5.2.7.3 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. 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.

      ![Note]
      
      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 47].

1.5.2.8 Configure IdP-Initiated SSO

Overview
In the IdP-Initiated single sign-on (SSO), the authentication starts at the identity provider (IdP). 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 application protected URL.

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>Parameter</td>
<td>Mandatory</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------</td>
<td>-------------</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>index</td>
<td>No</td>
<td>Enter the index number of the endpoint of the assertion consumer service of the service provider as the target of the SAML response. 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**

User Richard Wilson would like to initiate an SSO process at the cloud identity provider and has configured the default assertion consumer service (ACS) endpoint correctly. He tries to access the identity provider, but because he does not have a valid session and is prompted to provide credentials. Once Richard has logged in at the IdP, a session is created for him and he is automatically redirected to his application (the default ACS URL as specified in the service provider (SP) metadata)).
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 SAP Cloud Platform Identity Authentication service. For more information, see Configure a Trusted Service Provider [page 35].

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.

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.

   - **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 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 106].
### Table 30: Password Policy Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Standard</th>
<th>Enterprise</th>
<th>Custom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content of password (configurable)</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</td>
<td>● Characters from at least three of the following</td>
<td>● Characters from at least three of the following</td>
</tr>
<tr>
<td></td>
<td>groups:</td>
<td>groups:</td>
<td>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>Session time limit</td>
<td>Yes, 12 hours</td>
<td>Yes, 12 hours</td>
<td>Yes, 12 hours</td>
</tr>
<tr>
<td>Indicates when the current session expires</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;Remember me&quot; option</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Indicates whether the browser can store a cookie</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>initiate the number of forgot password e-</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mails specified by the forgot password</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>forgot password e-mails during the deactivation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>period. For example, a user can initiate up to</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>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</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>it can be changed.</td>
<td></td>
<td></td>
<td></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 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>Indicates whether a password history is retained, and how many passwords from the history are retained.</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>
<tr>
<td>Indicates how long the system retains unused passwords for.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

As a tenant administrator, you can do the following:

- Set a password policy for an application. For more information, see [Set a Password Policy for an Application](page 104).
- Create a custom password policy. For more information, see [Configure Custom Password Policy](page 106).
- Delete a custom password policy. For more information, see [Delete Custom Password Policy](page 108).

### 1.5.3.1 Set a Password Policy for an Application

#### Context

As a tenant administrator, you can set a password policy that matches your application logon requirements. 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 [Password Policies](page 102).
Tip
To see the configuration of the password policies in the tenant, go to the Password Policies tile and choose the 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 29].

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.
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 a new one, delete the existing custom policy first, and then create the new one. For more information, see Delete Custom Password Policy [page 108].

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.

<table>
<thead>
<tr>
<th>Configuration Options</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Policy Name</td>
<td>The name of the password policy that appears in the administration console.</td>
</tr>
<tr>
<td>Password Length</td>
<td>The length can be between 8 and 255 characters. The default value is 8 characters.</td>
</tr>
<tr>
<td>Password Lifetime</td>
<td>The lifetime can be between 1 month and 6 months. The default value is 6 months.</td>
</tr>
<tr>
<td>Maximum Duration of User Inactivity</td>
<td>The maximum duration of user inactivity can be between 1 and 6 months. The default value is 6 month.</td>
</tr>
<tr>
<td>Number of Last Used Passwords that Cannot Be Reused</td>
<td>The minimum requirement is the last 5 passwords to be retained. The value cannot be more than 20.</td>
</tr>
<tr>
<td>Number of Allowed Failed Logon Attempts</td>
<td>The number of allowed failed logon attempts can be between 1 and 5. The default value is 5.</td>
</tr>
<tr>
<td>Password Locked Period</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 104].
1.5.3.3 Delete Custom Password Policy

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 106].
- 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 104].

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.

   ![Note](https://<tenant ID>.accounts.ondemand.com/admin)

   The URL has the 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**.

   ![Caution](https://<tenant ID>.accounts.ondemand.com/admin)

   You can only delete the password policy if it is not set as a password policy for any applications in the tenant.

2. Choose the **Password Policies** tile.

3. Press the next to the custom password policy.
Results

Once the password policy has been deleted, the system displays the message `Password policy <name of policy> deleted`.

1.5.4 Configure Privacy Policies

Initially, administration console for SAP Cloud Platform Identity Authentication service displays a default privacy policy.

To set a new customized policy, you first need to create one and then to configure the versions for each language, as you need to 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:
- English
- German
- Spanish
- French
- Japanese
- Korean
- Dutch
- Polish
- Portuguese
- Russian
- Chinese
- Italian
- Welsh
- Hebrew

The application’s language is defined in the following order of importance:
- By the language of the service provider (SP).
- 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`.
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.

   **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.

   **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.*
Next Steps

Add the new custom versions for the languages. For more information, see Add Language Versions of a Privacy Policy Document [page 111].

Related Information

Add Language Versions of a Privacy Policy Document [page 111]
Configure Privacy Policies [page 109]
Define a Privacy Policy Document for an Application [page 112]
Troubleshooting for Administrators [page 180]

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.
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 login 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.

   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 Authentication and Access tab.
5. Under POLICIES, choose Privacy Policy.
6. Select the radio button for the Privacy Policy.
7. Save your selection.

Related Information

Configure Privacy Policies [page 109]
Troubleshooting for Administrators [page 180]
Create a New Application [page 29]

1.5.5 Configure 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:

- English
- German
- Spanish
- French
- Japanese
- Korean
- Dutch
- Polish
- Portuguese
- Russian
- Chinese
- Italian
- Welsh
- Hebrew
The application’s language is defined in the following order of importance:

- By the language of the service provider (SP).
- 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*.

**Related Information**

- Create a New Terms of Use Document [page 114]
- Add Language Versions of a Terms of Use Document [page 115]
- Define a Terms of Use Document for an Application [page 116]

### 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.

**Next Steps**

Add the new custom versions for the languages. For more information, see Add Language Versions of a Terms of Use Document [page 115].

**Related Information**

Add Language Versions of a Terms of Use Document [page 115]
Configure Terms of Use [page 113]
Define a Terms of Use Document for an Application [page 116]
Troubleshooting for Administrators [page 180]

**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 need to 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.

   **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.

   ➤ **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.**

### Related Information

- Create a New Terms of Use Document [page 114]  
- Configure Terms of Use [page 113]  
- Define a Terms of Use Document for an Application [page 116]  
- Troubleshooting for Administrators [page 180]

### 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 login 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.
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 29].

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.

Related Information

Configure Terms of Use [page 113]
Troubleshooting for Administrators [page 180]
Create a New Application [page 29]

1.5.6 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.

Note

For more information about the users that are authenticated with their corporate credentials from the corporate user store, see Corporate User Store [page 82].
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 146].

With user management, you can perform the following activities:

Table 31:

<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 <em>Add User</em> option in the administration console</td>
<td>Create a New User [page 119]</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 68]</td>
</tr>
<tr>
<td></td>
<td>Create users programmatically via API</td>
<td>Create User Resource [page 218]</td>
</tr>
<tr>
<td>Search users</td>
<td>Search users in the administration console</td>
<td>Search Users [page 120]</td>
</tr>
<tr>
<td></td>
<td>Search users via API</td>
<td>Users Search [page 205]</td>
</tr>
<tr>
<td>List and edit user details</td>
<td>List a specific user and edit the information about that user via the admin-</td>
<td>List and Edit User Details [page 122]</td>
</tr>
<tr>
<td></td>
<td>istration console</td>
<td></td>
</tr>
<tr>
<td></td>
<td>List and update user details via API</td>
<td>• User Resource [page 212]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Update User Resource [page 226]</td>
</tr>
<tr>
<td></td>
<td>Update user details via a CSV file import</td>
<td>Import or Update Users for a Specific Application [page 68]</td>
</tr>
<tr>
<td>Delete users</td>
<td>Delete users via the administration console</td>
<td>Delete Users [page 123]</td>
</tr>
<tr>
<td></td>
<td>Delete users programmatically via API</td>
<td>Delete User Resource [page 234]</td>
</tr>
<tr>
<td>Manage the user group assignment</td>
<td>Assign and unassign groups via the administration console</td>
<td>• Assign Groups to a User [page 129]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unassign Users from Groups [page 130]</td>
</tr>
</tbody>
</table>
1.5.6.1 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 146].

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.

   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. Press Add User.

4. Fill in the required fields in the pop-up window.

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>Set password</td>
<td>The tenant administrator sets the password for the user.</td>
</tr>
</tbody>
</table>

   i Note

   The user is prompted to reset the password during the first authentication.
6. Save your entries.

1.5.6.2 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 146].

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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Press More</td>
<td>This will expand the list by 20 users.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This option is available only if the users in the tenant are more than 20.</td>
</tr>
</tbody>
</table>
| **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.  
**Note**  
The search is case insensitive and does not require exact matching.  
The wildcard search is enabled by default and you should not include the wildcard character asterisk (*) in your search criteria. If you place asterisk (*) anywhere in your search string, except at the end, the system will include that character in the search. Asterisk (*) placed at the end of the search string is ignored by the system. |
| **Press Advanced Search and type your search criteria strings in at least one of the search fields** | The system checks the search fields simultaneously, and 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 and does not require exact matching.  
The wildcard search is enabled by default and you should not include the wildcard character asterisk (*) in your search. If you place asterisk (*) character anywhere in your search string, including at the end of the string, the system 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. |
1.5.6.3 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 120].
2. Click the user to view his or her details.
   This operation opens the User Details view.

   Donna Moore

   donna.moore@example.com

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.
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.

6. **Optional**: Choose the Authentication tab to manage the two-factor authentication for the user.

   You can see whether the user has enabled two factor authentication. If enabled you have two options:
   - Deactivate the user devices. For more information, see Deactivate User Devices for Two-Factor Authentication [page 124].
   - Unlock the user passcode when the user needs to log on to the application before the automatic unlock time. For more information, see Unlock User Passcode [page 124].

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 129].
   - Unassign one or more groups that are assigned to the user Unassign Users from Groups [page 130].

1.5.6.4 **Delete Users**

As a tenant administrator, you can delete users in the administration console for SAP Cloud Platform Identity Authentication service.

**Procedure**

1. Find the user that you want to delete.

   For more information about how to find a user in Identity Authentication, see Search Users [page 120].

2. Select the checkbox next to the user or users that you want to delete.

   You are not allowed to delete your own user profile.

3. Press **Delete Users**.

4. Confirm the operation.
1.5.6.5 Deactivate User Devices for 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 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.

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 120].
2. Select the user whose device you want to deactivate.
4. Use the slider next to Status to deactivate two-factor authentication.

1.5.6.6 Unlock User Passcode

You can unlock a user passcode when the user needs to log on to the application before the automatic unlock time, which is 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 two-factor authentication. The passcode is unlocked automatically after 60 minutes.
When the user locks his or her passcode, he or she will not be able to log on only to applications that require passcodes. The applications that do not require two-factor authentication will be accessible only with the user password.

To unlock the user passcode manually, proceed as follows:

**Procedure**

1. Find the user whose 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 120).

2. Select the user that you want to unlock.

   **Note**
   
   You can only unlock locked user passcodes.

3. Choose the Authentication tab.


5. Press Unlock under Passcode Status.

   The system displays the message Account <name of user> unlocked.

### 1.5.7 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 127]</td>
</tr>
<tr>
<td>How to list users in a user group</td>
<td>List Users in User Groups [page 128]</td>
</tr>
<tr>
<td>Create a new user group</td>
<td>Create a New User Group [page 126]</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 68]</td>
</tr>
</tbody>
</table>
### 1.5.7.1 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_146).

#### 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.

1.5.7.2 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 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 146].
- You have created user groups in your tenant. For more details how to create user groups, see Create a New User Group [page 126].

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. 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.
1.5.7.3 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 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 146].
- 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 126]
Assign Groups to a User [page 129]
Edit Administrator Authorizations [page 146]

1.5.7.4 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 SAP Cloud Platform Identity Authentication service.

Prerequisites

You have created user groups in your tenant. For more details how to create user groups, 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.

   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 pop-up, 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 SAML 2.0 assertion. For more information, see Configure the User Attributes Sent to the Application [page 38]

Related Information

Create a New User Group [page 126]

1.5.7.5 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 SAP Cloud Platform Identity Authentication service.

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.

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.
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 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.

Related Information

Create a New User Group [page 126]
Assign Groups to a User [page 129]

1.5.7.6 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 146].

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.

   ! 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.

1.5.8 User Provisioning

As a tenant administrator, you can configure target systems for user provisioning and provision users to these target systems.

Related Information

Configure SAP Jam Target Systems for User Provisioning [page 138]
Provision Users to SAP Jam Target Systems [page 133]
Delete SAP Jam Target System [page 140]

1.5.8.1 Provision Users to SAP Jam Target Systems

Tenant administrators can provision SAP Cloud Platform Identity Authentication service users to SAP Jam targets systems.

Prerequisites

- You are assigned the Manage Users role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 146].
- 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 Provisioning [page 138].

Note

Currently, Identity Authentication only supports user provisioning to SAP Jam instances.

Context

Identity Authentication supports the following scenarios for user provisioning to SAP Jam 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.

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 33: Attribute Mapping Between SAP Cloud Platform Identity Authentication Service and SAP Jam

<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>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>
</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.
The note about locale explains that the format must be "ll_CC" where "ll" is a lowercase two-letter language code and "CC" is the uppercase two-letter country code.

The caution note advises against sending the locale attribute if the language or country attribute is missing.

The note below discusses the use of Identity Authentication as a proxy to delegate authentication to a corporate identity provider. It indicates that users authenticated by the corporate identity provider will not be provisioned during authentication. When a user is deleted, they are automatically deprovisioned from the configured target systems.

To provision users, choose one of the options below and follow the corresponding procedure.
Provision All Users to Selected Target Systems

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.

   **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 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 138].

4. Press *Provision*.

   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.
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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Press More | This will expand the list by 20 users.  

> Note  
This option is available only if the users in the tenant are more than 20.  

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.  

> Note  
The search is case insensitive and does not require exact matching.  
The wildcard search is enabled by default and you should not include the wildcard character asterix (*) in your search criteria. If you place asterix (*) anywhere in your search string, except at the end, the system will include that character in the search. Asterix (*) placed at the end of the search string is ignored by the system.  

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Press Advanced Search and type your search criteria strings in at least one of the search fields | The system checks the search fields simultaneously, and 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 and does not require exact matching.  
The wildcard search is enabled by default and you should not include the wildcard character asterix (*) in your search. If you place the asterix (*) character anywhere in your search string, including at the end of the string, the system 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.|

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 84].

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

Related Information

Create a New User [page 119]
Add Administrators [page 143]
Import or Update Users for a Specific Application [page 68]
Create User Resource [page 218]
Update User Resource [page 226]
Scenarios [page 20]

1.5.8.2 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 146].

Note

Currently, Identity Authentication only supports user provisioning to SAP Jam instances.
Context

To configure a 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 in order to add a new target system to the list.

4. Choose **JAM System**.

5. Make the corresponding entries in the **Target Configurations** and **Authentication Configurations** fields for the target system you want to add.

   All fields are obligatory.

6. Save your changes.

   If the operation is successful, the system displays the message **System <name of system> configuration updated.**

7. (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.
1.5.8.3 Delete SAP Jam Target System

As a tenant administrator, you can delete one or more SAP Jam 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 146].

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.

   Note
   The URL has the \texttt{https://\langle tenant ID\rangle.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{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 \textit{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 \textit{1 target system deleted}.

1.5.9 Manage 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 142]
- Add Administrators [page 143]
- Edit Administrator Authorizations [page 146]
1.5.9.1 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.

   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. For more details, see Related Information.

3. Click on 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

ID Federation with an Identity Authentication Tenant
Edit Administrator Authorizations [page 146]
1.5.9.2 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.

1.5.9.2.1 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. For more details, see Related Information.
3. Press the +Add button on the left hand panel in order to add a new administrator to the list.
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.

<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.

1.5.9.2.2 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.

Note

The URL has the pattern `https://<tenant ID>.accounts.ondemand.com/admin`. 
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. For more details, see Related Information.

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>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>

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

i 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.
1.5.9.3 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.

   Note
   The list also includes the SAP Cloud Platform system, which by default has authorizations to set up the trust with Identity Authentication. For more details, see Related Information.

3. Click on 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.
To be a tenant administrator, a user must be assigned one or more of the following roles:

Table 36: 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>

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 messageTenant administrator <name of tenant administrator> updated.

Related Information

ID Federation with a Identity Authentication Tenant
1.5.10 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 37:

<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 160]</td>
</tr>
<tr>
<td>How to choose a type for the corporate identity provider</td>
<td>Choose Identity Provider Type [page 163]</td>
</tr>
<tr>
<td>How to delete corporate identity providers</td>
<td>Delete Corporate Identity Providers [page 164]</td>
</tr>
<tr>
<td>How to configure the <em>Identity Federation</em> option</td>
<td>Configure Identity Federation with the User Store of SAP Cloud Platform Identity Authentication Service [page 166]</td>
</tr>
<tr>
<td>How to configure your systems for IdP-Initiated SSO with a corporate identity provider</td>
<td>Configure IdP-Initiated SSO with Corporate Identity Providers [page 149]</td>
</tr>
</tbody>
</table>
1.5.10.1 Configure IdP-Initiated 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 SAP Cloud Platform Identity Authentication service 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.

<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 152]</td>
</tr>
</tbody>
</table>
| Tenant administrator     | Tenant of Identity Authentication | • Authenticating identity providers  
                           |                   • (Optional) Request [Multiple Corporate IdP Trust feature] | 2. Configure SAP Cloud Platform Identity Authentication Service [page 153] |
### Prerequisites

The IDP-Initiated SSO option in the tenant of Identity Authentication must be enabled.

**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 99].

#### 1.5.10.11 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.

**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.

1.5.10.1.2 2. Configure SAP Cloud Platform Identity Authentication Service

Context

In the scenario where SAP Cloud Platform Identity Authentication service 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 a Trusted Service Provider [page 35]

   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 application protected URL.

2. Configure a trust with the corporate identity provider. For more information, see Configure Trust with Corporate Identity Provider [page 160].

   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. You have the following options:

   - If your scenario includes more than one corporate identity provider, request the Multiple Corporate IdP Trust feature from an Identity Authentication operator.

   ! Note

   To do this, create a ticket on SAP Support Portal under component BC-IAM-IDS with the following headline “Enable Multiple Corporate IdP Trust feature for tenant <tenant_id>”.

SAP Cloud Platform Identity Authentication Service
SAP Cloud Platform Identity Authentication Service
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 Identity Provider for an Application [page 73].

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.

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 76].

1.5.10.1.3 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.

   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 a Trusted Service Provider [page 35].
2. Add the `sp=<sp_name>` parameter to the assertion consumer service (ACS) endpoint URL. 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>`. Request the Entity ID of the service provider from the tenant administrator of Identity Authentication.

**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` and `index` parameters are not mandatory and can be skipped. For more information about the configuration, see [Configure IdP-Initiated SSO](#page-99).

**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.

### 1.5.10.1.4  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 68].
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 166]. 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 38] and Configure the Name ID Attribute Sent to the Application [page 41].

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)
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).
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).

**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 exists:

- 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 38] and Configure the Name ID Attribute Sent to the Application [page 41].

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 166].
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 38]
   - Configure the Name ID Attribute Sent to the Application [page 41]

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.

1.5.10.2 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, and this procedure completes the logout process.

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 and 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 159].
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.

1.5.10.2.1 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 and can be used by the application to redirect the user after successfully logging out of the application when SAP Cloud Platform Identity Authentication service 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 160).

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.
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 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.

1.5.10.3 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 146].
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://<tenant_ID>.accounts.ondemand.com/saml2/idp/acs?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 76].

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.

   **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 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 Identity Provider for an Application [page 73].
Related Information

SAML 2.0 [page 179]
Edit Administrator Authorizations [page 146]
Configure IdP-Initiated SSO [page 99]

1.5.10.4 Choose Identity Provider Type

This topic shows you how to choose a type for the corporate identity provider.

Prerequisites

You have the Manage Corporate Identity Providers role.

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 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
- MS ADFS 2.0

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 148]
- Edit Administrator Authorizations [page 146]

### 1.5.10.5 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 have the Manage Corporate Identity Providers role. For more information about the different roles and how to edit them, see **Edit Administrator Authorizations [page 146]**.
- 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 **Choose Identity Provider for an Application [page 73]**.

**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 used as authenticating identity provider for an application, you have to choose another authenticating identity provider for that application. For more information, see **Choose Identity Provider for an Application [page 73]**.
To delete one or more identity providers, not used as authenticating identity providers for 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.

   **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.

Once the identity provider has been deleted, the system displays the message Identity provider deleted.

Related Information

Edit Administrator Authorizations [page 146]
Choose Identity Provider for an Application [page 73]

1.5.10.6 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 have the Manage Corporate Identity Providers role. For more information about how to assign administrator roles, see Edit Administrator Authorizations [page 146].
- 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 160].
- You have selected the configured identity provider as the authenticating identity provider for your application. For more information, see Choose Identity Provider for an Application [page 73].
- 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 68].

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 148).

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) 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 41).

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) 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.

   *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 disable or enable 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.

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

   - **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 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**.

   - **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.
1.5.11 Social Identity Providers

1.5.11.1 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 SAP Cloud Platform Identity Authentication service 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.

Note

You need to type https://<tenant_domain>/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.

Related Information

Create a New User Group [page 126]
Assign Groups to a User [page 129]
To perform the social identity provider configuration in the administration console for Identity Authentication, you have to provide the following data:

Table 39: 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>

Table 40: 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>

Table 41: 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>

Table 42: 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.

**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 log in 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 login 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 44].

**Related Information**

Using OAuth 2.0 for Login in Google [page 171]
Choose a verification method in Google [page 171]
Facebook Login [page 171]
Authentication in LinkedIn [page 171]
Authorizing a request in Twitter [page 171]
Enable or Disable Social Sign-On for an Application [page 44]
Remove Social Identity Providers Configuration [page 172]
Social Authentication [page 187]
1.5.11.2 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.

   ![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. Chose 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 login pages of the applications in the tenant.

Related Information

Configure Social Identity Providers [page 169]
1.5.12 Export Change Logs with a History of Administration Operations

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.

Table 43: Sample Change Logs Data

<table>
<thead>
<tr>
<th>Date</th>
<th>Adminstrator'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>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</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>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</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>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</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>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>sp.example.com</td>
<td>UPDATE</td>
<td>Branding Style</td>
<td>Text Color=#ffffff, Background Top Color=#E3E3E3, Border Color=#7B9EB3, show_header=false, Background Bottom Color=#E3E3E3</td>
</tr>
<tr>
<td>16-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</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>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>sp.example.com</td>
<td>UPDATE</td>
<td>Self-Registration</td>
<td>Allowed</td>
</tr>
<tr>
<td>Date</td>
<td>Administra tor'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>P123456</td>
<td>Donna Moore</td>
<td>Privacy Policy Document</td>
<td>53da05f9a4b0732235f24b8a</td>
<td>Company A Privacy Policy</td>
<td>CREATE</td>
<td>Display Name</td>
<td>Company A Privacy Policy</td>
</tr>
<tr>
<td>16-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Terms of Use Document</td>
<td>53da0595e4b0732235f24b04</td>
<td>English Version of Company A Terms of Use</td>
<td>CREATE</td>
<td>Plain Text Terms of Use File</td>
<td></td>
</tr>
<tr>
<td>16-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Terms of Use Document</td>
<td>53da0595e4b0732235f24b00</td>
<td>Company A Terms of Use</td>
<td>CREATE</td>
<td>Display Name</td>
<td>Company A Terms of Use</td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>Company A (company_a_service_provider)</td>
<td>UPDATE</td>
<td>SAML 2.0 Provider Name</td>
<td>company_a_service_provider</td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>Company A (company_a_service_provider)</td>
<td>UPDATE</td>
<td>Authenticating Authority</td>
<td>company_a_tenant_id</td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>Company A (company_a_service_provider)</td>
<td>UPDATE</td>
<td>Assertion Consumer Service Endpoint</td>
<td>service_provider_acs_endpoint, HTTP-POST</td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>Company A (company_a_service_provider)</td>
<td>UPDATE</td>
<td>Single Logout Endpoint</td>
<td>service_provider_slo_endpoint, HTTP-POST</td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>Company A (company_a_service_provider)</td>
<td>UPDATE</td>
<td>Single Logout Endpoint</td>
<td>service_provider_slo_endpoint, HTTP-Redirect</td>
</tr>
<tr>
<td>15-05-2014</td>
<td>P123456</td>
<td>Donna Moore</td>
<td>Service Provider</td>
<td>500964f6e4b0f3cba101f700</td>
<td>Company A (company_a_service_provider)</td>
<td>CREATE</td>
<td>Name ID Attribute</td>
<td>User ID</td>
</tr>
</tbody>
</table>

SAP Cloud Platform Identity Authentication Service

SAP Cloud Platform Identity Authentication Service

PUBLIC 175
### 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.
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 Export Change Logs tile.
   This operation opens the Export Change Logs page.
3. Choose the Export button.

Related Information

Troubleshooting for Administrators [page 180]

1.5.13 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 146].

Context

You can download an 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: status, loginName, mail, firstName, and lastName. If the status of a user is inactive, he or she cannot perform any operations on the tenant.

Example

A tenant administrator downloads a CSV file with the current users in the system. As a result, the administrator receives the following information:

Table 44:

<table>
<thead>
<tr>
<th>status</th>
<th>loginName</th>
<th>mail</th>
<th>firstName</th>
<th>lastName</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>EID00001</td>
<td><a href="mailto:michael.adams@example.com">michael.adams@example.com</a></td>
<td>Michael</td>
<td>Adams</td>
</tr>
</tbody>
</table>
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:

**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 *Export Users* tile.

   This operation opens the *Export Users* page.

3. Choose the *Export* button.

**Related Information**

*Troubleshooting for Administrators [page 180]*

*Edit Administrator Authorizations [page 146]*
1.5.14 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 create an Incident on SAP Support Portal with a component BC-IAM-IDS.

Currently the statistics does 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.

1.5.15 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 provides 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.

Related Information

SAML Specifications

1.5.16 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 45:

<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>
<tr>
<td>Internal error; contact system administrator</td>
<td>Unexpected error occurred.</td>
<td>• Try again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check the browser logs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Contact an operator of Identity Authentication.</td>
</tr>
<tr>
<td>The provided file is of wrong type; specify a different file</td>
<td>You have specified a wrong file format.</td>
<td>You should use the following files:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For service provider metadata, use XML.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For privacy policy and terms of use documents, use plain text files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• For certificate for API authentication, use base64-encoded certificate.</td>
</tr>
<tr>
<td>The imported CSV file contains entries with a duplicate email &lt;email address&gt;. The values under mail column must be unique.</td>
<td>You have provided a CSV file with a mail column that has the same email entries.</td>
<td>Correct the file so that the mail column contains unique values.</td>
</tr>
<tr>
<td>Error Message</td>
<td>Description</td>
<td>Solution</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>The imported CSV file contains entries with a duplicate login name &lt;login name&gt;. The values under loginName column must be unique.</td>
<td>You have provided a CSV file with a loginName column that has the same entries.</td>
<td>Correct the file so that the loginName column contains unique values.</td>
</tr>
<tr>
<td>First &lt;number&gt; users are imported. User import has been interrupted due to an invalid entity.</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 the CSV file contains an incorrect data for that user.</td>
<td>Delete the first &lt;number&gt; users from the CSV file, correct the invalid row, and re-import the updated file.</td>
</tr>
</tbody>
</table>
| 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 email matches with the email 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. |
| First <number> users are imported. User import has been interrupted for user with email address <email address>. | The first <number> 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. | • Correct the email for the login name under the mail column, delete the first <number> users from the CSV file, and re-import the updated file.  
⚠️ Caution  
During CSV import, you cannot change the email of an existing user.  
• Change the user login name because the same login name is used for another user in the database, delete the first <number> users from the CSV file, and re-import the updated file.  
 Norte  
You cannot have two users with the same login name, but with different emails.  
• Contact an operator of Identity Authentication. |
<table>
<thead>
<tr>
<th>Error Message</th>
<th>Description</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Your e-mail activation link is invalid. | The link that the user has followed has expired or has already been used. | • 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 68]. |

### Related Information

Get Support [page 275]

### 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. User services are divided into profile and sign-on services. For configuration of certain profile services, users access the profile page at https://<tenant ID>.accounts.ondemand.com/.

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 based single sign-on.
- 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 184].

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 email 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.

**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.

**Viewing profile data**

Users can open a printable overview of all the data on file for them by clicking the **View My Data** button.

**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 20]
Two-Factor Authentication [page 184]
Social Authentication [page 187]
Use the Remember Me Option [page 189]
Access Applications with Single Sign-On on Mobile Devices [page 190]

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 two-factor authentication.

With two-factor authentication, you are required to provide a one-time password (OTP), also called a passcode, in addition to your primary credentials. Passcodes are time-based and are valid for one login 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.

Related Information

Activate a Device for Two-Factor Authentication [page 185]
Deactivate Devices Configured for Two-Factor Authentication [page 186]
1.6.1.1 Activate a Device for Two-Factor Authentication

To log on to applications that require two-factor authentication, you have to activate a mobile device that will generate passcodes.

Prerequisites

- You have installed a QR code scanner and an SAP Authenticator application on your mobile device.

  **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.

  **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.

  **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

2. Press **Activate** under **Two-Factor Authentication**. This operation expands the **Two-Factor Authentication** section.
3. Call the **Add Account** screen in SAP Authenticator and do one of the following on your mobile device:
   - Tap the **Scan QR Code** button
   - Enter the secret key manually
4. Tap **Add Account** 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.

Related Information

Two-Factor Authentication [page 184]
Deactivate Devices Configured for Two-Factor Authentication [page 186]

1.6.1.2 Deactivate Devices Configured for Two-Factor Authentication

This document shows you how to deactivate your mobile devices that you use to generate 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

3. Enter the passcode generated by the authenticator application in the provided space on the profile page.
4. Press Deactivate.

**Related Information**

Two-Factor Authentication [page 184]
Activate a Device for Two-Factor Authentication [page 185]

### 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>
</table>
| Facebook                | • ID of your user · used to link your Facebook account with your Identity Authentication account  
<pre><code>                     | • your first name, last name, login name, display name, and gender · used to prefill the registration form in case of non-existing user |
</code></pre>
<table>
<thead>
<tr>
<th>Social Identity Provider</th>
<th>Data Used by SAP Cloud Platform Identity Authentication Service</th>
</tr>
</thead>
</table>
| Google                   | • ID of your user - used to link your Google account with your Identity Authentication account  
• your first name, last name, login name, display name, and gender - used to prefill the registration form in case of non-existing user |
| LinkedIn                 | • ID of your user - used to link your LinkedIn account with your Identity Authentication account  
• your first name, last name, and login name - used to pre-fill the registration form in case of non-existing user |
| Twitter                  | • ID of your user - used to link your Twitter account with your Identity Authentication account  
• display name - used to prefill the registration form in case of non-existing user |

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.

   **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:
   - Link your Identity Authentication account with your social network account.
   - Create a new Identity Authentication account that will be linked with your social network account.

   **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

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 and automatically logs you on next time you access the application. 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 check box.
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 184]

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 Two-Factor Authentication [page 185].
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 on the basis of 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]

3. Log on to the application via SAP Authenticator.
4. Select the Remember me check box.
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 184]
Use the Remember Me Option [page 189]
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

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

Table 47: 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;</td>
<td>● Try again;</td>
</tr>
<tr>
<td></td>
<td>● Your account is not activated.</td>
<td>● Open your e-mail and activate your account;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Register on the logon page;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>● Contact your administrator.</td>
</tr>
<tr>
<td>Account is locked; select the link in the e-mail</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;</td>
</tr>
<tr>
<td>that has been sent to unlock your account;</td>
<td></td>
<td>● Contact your administrator.</td>
</tr>
<tr>
<td>An error occurred; try again</td>
<td>An unexpected error occurred.</td>
<td>Try again;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contact your administrator.</td>
</tr>
<tr>
<td>Insufficient password complexity; check</td>
<td>Your password does not comply with the application’s password</td>
<td>Familiarize yourself with the password policy for the application.</td>
</tr>
<tr>
<td>password requirements</td>
<td>policy.</td>
<td></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</td>
<td>According to the application’s policy, you are not allowed to</td>
<td></td>
</tr>
<tr>
<td>24 hours</td>
<td>change the password right now.</td>
<td>• Familiarize yourself with the application’s policy for changing the password;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 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</td>
<td>• Visit the application choose Log On follow Forgot Password link</td>
</tr>
<tr>
<td></td>
<td>already used by you.</td>
<td>• Contact your administrator.</td>
</tr>
</tbody>
</table>

Related Information

Get Support [page 275]
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 SAP Cloud Platform Identity Authentication service. 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 Service [page 200]
- An API to invite users
  For more information, see Invitation REST API [page 198]
- Identity Authentication implementation of the System for Cross-domain Identity Management (SCIM) REST API protocol.
  For more information, see SCIM REST API [page 204].
- 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 235].
- An API to change the predefined master data texts.
  For more information, see Change Master Data Texts [page 241].

Related Information

Troubleshooting for Developers [page 251]
Configure a Certificate for API Authentication [page 49]

1.7.1 API Authentication

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

For more information about the API methods, see Invitation REST API [page 198] and User Management REST API [page 200].

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 29].
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.
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 29]
Invitation REST API [page 198]
User Management REST API [page 200]

### 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 198]
User Management REST API [page 200]
SCIM REST API [page 204]
Change Tenant Texts REST API [page 235]
Change Master Data Texts [page 241]
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][48]

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>
<tr>
<td>inviteeUserId</td>
<td>The user ID of the invitee</td>
</tr>
<tr>
<td>inviterName</td>
<td>The display name of the user who sends the invitation.</td>
</tr>
</tbody>
</table>

**Note**

Only inviteeEmail or inviteeUserId should be used, not both.
<table>
<thead>
<tr>
<th>Required Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>targetUrl</strong></td>
<td>The URL that the user is redirected to after registration.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The <code>targetUrl</code> parameter is optional if a Home URL is set for the application, and the application does not use overlay.</td>
</tr>
<tr>
<td></td>
<td>If <code>targetUrl</code> is not specified, or the application uses overlay, the user is redirected to the application’s Home URL, which must be set.</td>
</tr>
<tr>
<td><strong>sourceUrl</strong></td>
<td>The URL for the invitation link in the e-mail sent to the invitee.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The <code>sourceUrl</code> parameter is optional if a Home URL is set for the application, and the application does not use overlay.</td>
</tr>
<tr>
<td></td>
<td>If <code>sourceUrl</code> is not specified, or the application uses overlay, the user is redirected to the application’s Home URL, which must be set.</td>
</tr>
</tbody>
</table>

Table 49: Optional Parameters for the POST Method

<table>
<thead>
<tr>
<th>Optional Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inviteeFirstName</td>
<td>The first name of the invitee</td>
</tr>
<tr>
<td>inviteeLastName</td>
<td>The last name of the invitee</td>
</tr>
<tr>
<td>footerText</td>
<td>The footer text of the invitation e-mail</td>
</tr>
<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/home_page/",
  "sourceUrl": "http://www.myserviceprovider.com/home_page/"
}
```
Related Information

Add Logon Overlays in Customer Applications [page 248]
Configure an Application’s Home URL [page 31]
Configure a Certificate for API Authentication [page 49]
Troubleshooting for Developers [page 251]

1.7.2.2 User Management REST API

This REST API allows you to implement a request for a user registration and a request for verification of a user password or certificate. You thus allow administrators to register business partners on their behalf or to check user credentials.

1.7.2.2.1 User Registration Service

The user registration service 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 48]

Resource

For this service, you need to use the following URI: https://<tenant ID>.accounts.ondemand.com/service/users

• For user registration, you use a POST method.
• To retrieve an SP user’s URI, you use a GET method. This method requires the following URL parameters:
  ○ name_id=<name ID>
  ○ sp_name=<name of SP>

Representation

You have to specify application/x-www-form-urlencoded content type. All declared parameters in the request must be URL-encoded.
HTTP Method: **POST**

**Parameters**

Table 50: Required Parameters for the POST Method

<table>
<thead>
<tr>
<th>Required Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name_id</td>
<td>The name ID of the user you register.</td>
</tr>
<tr>
<td>email</td>
<td>The email of the user you register.</td>
</tr>
</tbody>
</table>

Table 51: Optional Parameters for the POST Method

<table>
<thead>
<tr>
<th>Optional Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user_profile_id</td>
<td>The user ID</td>
</tr>
<tr>
<td>login_name</td>
<td>The login name of the user</td>
</tr>
<tr>
<td>first_name</td>
<td>The first name of the user you register. The allowed maximum length for the first name is 32 characters.</td>
</tr>
<tr>
<td>last_name</td>
<td>The last name of the user you register. The allowed maximum length for the last name is 64 characters.</td>
</tr>
<tr>
<td>language</td>
<td>The preferred language of the user you register</td>
</tr>
<tr>
<td>valid_from</td>
<td>The “valid from” date</td>
</tr>
<tr>
<td>valid_to</td>
<td>The “valid until” date</td>
</tr>
<tr>
<td>source_url</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>
</tr>
<tr>
<td>target_url</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.</td>
</tr>
</tbody>
</table>
| send_email             | 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. |

**Note**

If the user is new, the activation link is returned with the **201** response.

spCustomAttribute1 spCustomAttribute2 spCustomAttribute3 spCustomAttribute4

Custom attributes are used to store additional information for the SP users. It is allowed to pass five customer attributes for a user.
Optional Parameter | Description
---|---
spCustomAttribute5

**POST Request**

**Example**

**POST Request**

⚠️ Caution

All parameters for the POST method must be written on one line.

```
POST /service/users
Content-Type: application/x-www-form-urlencoded
```

**POST Response**

**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
{
"activationLink" : "https://<tenant ID>.accounts.ondemand.com/ids/activation?token=I1830C497BF9B57B76298E5F117AF39711F59A28838A3276E8B68FFFF54414C8843ACFA395A05401ABE6568FF3659D6EE96"
```
HTTP Method: GET

Table 52: Required Parameters for the GET Method

<table>
<thead>
<tr>
<th>Required Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name_id</td>
<td>The name ID of the SP user that you retrieve the URI for.</td>
</tr>
<tr>
<td>sp_name</td>
<td>The name of the service provider.</td>
</tr>
</tbody>
</table>

GET Request

**Example**

GET Request

GET /service/users?name_id=johns&sp_name=jpaas.developer

GET Response

The URI of the created user is in the location header of the HTTP Response.

**Example**

Location: https://<tenant ID>.accounts.ondemand.com/service/users/0800200c9a66

Related Information

Configure the User Attributes Sent to the Application [page 38]
Troubleshooting for Developers [page 251]
1.7.2.3 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 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 144], and Edit Administrator Authorizations [page 146].

Note

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.

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.

Note

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.

<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>
</tbody>
</table>
### Attribute | Examples | Full Sets
--- | --- | ---
addresses.region | ● [NY]  
● [AB] | ● https://<tenant ID>.accounts.ondemand.com/md/states/us  
● https://<tenant ID>.accounts.ondemand.com/md/states/ca
timeZone | ● [Africa/Abidjan] | ● https://<tenant ID>.accounts.ondemand.com/md/timezones
department | ● [Administration] | ● https://<tenant ID>.accounts.ondemand.com/md/departments
companyRelationship | ● [Consultant] | ● https://<tenant ID>.accounts.ondemand.com/md/relationships
locale | ● [EN] | ● https://<tenant ID>.accounts.ondemand.com/md/languages

**Related Information**

Users Search [page 205]  
User Resource [page 212]  
Create User Resource [page 218]  
Update User Resource [page 226]  
Delete User Resource [page 234]

### 1.7.2.3.1 Users Search

The user search method of the SAP Cloud Platform Identity Authentication service 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 54:

<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>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>

**Note**

If you have more than 100 user, and you want to get the full list, you have to perform multiple requests.

If none of the request parameters are included, the number of items which will be returned per page will be at most 100 starting from index 1.

Supported Operators

Table 55:

<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 56:

<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 login 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>
</tbody>
</table>

Request Example

```plaintext
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
- name_id
- id
- emails.value
- name.honorificPrefix
- name.givenName
- name.familyName
- userName
- addresses[work].streetAddress
- addresses[work].locality

**Note**

The attribute equals to city.

- addresses[work].region
**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`

**Note**
The attribute equals to city.

- `addresses[home].region`

**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`

**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.
- **passwordStatus**
  
  **Note**
  
  Supported values: *initial, enabled, and disabled.*

- **userType**
  
  **Note**
  
  Supported values: *public, partner, customer, and employee.*

### Enterprise User Schema Extension

**Note**

The values of the following attributes are returned when the Enterprise User Schema Extension is used.

- **employeeNumber**
- **costCenter**
- **organization**
  
  **Note**
  
  Equals the *company* attribute from the Core schema.

- **division**
- **department**
  
  **Note**
  
  Equals the *department* attribute from the Core schema.

- **manager**
  
  - **value**
  
  - **$ref**
  
  - **displayName**
  
  **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.

**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 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

Table 57: 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 247].

### Response Example

```json
{
  "schemas": [
    "urn:ietf:params:scim:api:messages:2.0:ListResponse"],
  "totalResults": 1,
  "itemsPerPage": 10,
  "startIndex": 1,
  "Resources": [{
    "userName": "johnsmith",
    "meta": {
      "location": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P0000000",
      "resourceType": "User",
      "version": "1.0",
      "created": "2013-06-18T13:05:51Z",
      "lastModified": "2015-08-21T11:19:50Z"
    },
    "name": {
      "givenName": "John",
      "familyName": "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": "GMT+2",
"userType": "partner",
"active": true,
"groups": [{
  "value": "admin",
  "$ref": "https://<tenant ID>.accounts.ondemand.com/service/groups/55b87ab4e4b0fc7a00bcb070",
  "display": "Administrators"
}]
],

"displayName": "John Smith",
"contactPreferenceEmail": "yes",
"contactPreferenceTelephone": "no",
"industryCrm": "Consumer Products",
"companyRelationship": "Partner",
"company": "SFSF",
"department": "Administration",
"passwordStatus": "disabled",
"corporateGroups": [
  {
    "value": "admin"
  }
],

  "employeeNumber": "JohnA",
  "costCenter": "costCenter",
  "organization": "SFSF",

  "division": "Finance",
  "department": "Administration",
  "manager": {
    "value": "P999913",
    "$ref": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P999913",
    "displayName": "Jane Watson"
  }
},

"urn:sap:cloud:scim:schemas:extension:custom:2.0:User": {
  "attributes":{
    
    "name": "customAttribute1",
    "value": "Home Address2"
  }
}
1.7.2.3.2  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.

i 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 58:

<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

Example

GET /service/scim/Users/P000000
Response

Format: application/scim+json

Response

The response contains user object with the following user attributes:

- meta
- userType
- name_id
- id
- emails.value
- name.honorificPrefix
- name.givenName
- name.familyName
- 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

**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 response, the user status is equivalent to the new status in Identity Authentication.

- displayName
- contactPreferenceEmail
- contactPreferenceTelephone
- industryCrm
- company
- companyRelationship
- department
- groups
- 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.

- passwordStatus

**i Note**
Supported values: initial, enabled, and disabled.

- userType

**i Note**
Supported values: public, partner, customer, and employee.

- socialIdentities

**i 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**

**i Note**
The values of the following attributes are returned when the Enterprise User Schema Extension is used.
- `employeeNumber`
- `costCenter`
- `organization`

  **Note**
  
  Equals the `company` attribute from the Core schema.

- `division`
- `department`

  **Note**
  
  Equals the `department` attribute from the Core schema.

- `manager`
  - `value`
  - `$ref`
  - `displayName`

  **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.

  **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.
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"
    },
    "name": {
        "givenName": "John",
        "familyName": "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",
        "$ref": "https://<tenant ID>.accounts.ondemand.com/service/groups/55b87ab4e4b0fc7a00b0b070",
        "display": "Administrators"
    }],
    "displayName": "JohnSmith",
    "contactPreferenceEmail": "yes",
    "contactPreferenceTelephone": "no",
    "industryCrm": "Consumer Products",
    "companyRelationship": "Partner"
}
```
"company": "SFSF",
"department": "Administration",

"passwordStatus": "disabled",
"corporateGroups": [
  {
    "value": "admin"
  }
],
"socialIdentities": [{
  "socialId": "3375377405",
  "socialProvider": "Twitter",
  "dateOfLinking": "20160420064555Z"
}, {
  "socialId": "138244449858760",
  "socialProvider": "Facebook",
  "dateOfLinking": "20160419143031Z"
}, {
  "socialId": "GLhp_za6Hq",
  "socialProvider": "LinkedIn",
  "dateOfLinking": "20160420064732Z"
}],
  "employeeNumber": "JohnS",
  "costCenter": "costCenter",
  "organization": "SFSF",
  "division": "Finance",
  "department": "Administration",
  "manager": {
    "value": "P999913",
    "$ref": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P999913",
    "displayName": "Jane Watson"
  }
},
"urn:sap:cloud:scim:schemas:extension:custom:2.0:User": {
  "attributes": [
    {
      "name": "customAttribute1",
      "value": "Home Address2"
    },
    {
      "name": "customAttribute2",
      "value": "Telephone2"
    }
  ]
}
1.7.2.3.3 Create User Resource

The create user resource method of the SAP Cloud Platform Identity Authentication service implementation of the SCIM REST API protocol provides information on the creation of a user.

**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`

**Note**
Only one value is supported.

- `sendMail`

**Note**
The parameter supports boolean values `true` and `false`. The default value is `true`. If you do not want to send an e-mail, the value should be passed with value `false`.

- `mailVerified`

**Note**
The parameter supports boolean values `true` and `false`. The default value is `false`.

**Table 59: Possible Combinations**

<table>
<thead>
<tr>
<th>sendMail</th>
<th>true</th>
<th>true</th>
<th>false</th>
<th>false</th>
</tr>
</thead>
<tbody>
<tr>
<td>mailVerified</td>
<td>true</td>
<td>false</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>Result</td>
<td>The user will receive e-mail. He or she will be able to log on.</td>
<td>The user will receive e-mail. He or she has to click the verification link in the e-mail.</td>
<td>The user will be able to log on to the application directly.</td>
<td>The user will not be able to log on.</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>

- `name.honorificPrefix`
- `name.givenName`
- `name.familyName`
- `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`

**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 login. `passwordStatus` will be `initial` as a default value.
If the attribute `password` is provided, user is prompted to change the password on first login. `passwordStatus` will be initial as a default value.

- `phoneNumbers[work].value`
- `phoneNumbers[mobile].value`
- `phoneNumbers[fax].value`
- `timezone`
- `active`

The parameter supports only boolean values `true` and `false`. 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`
- `contactPreferenceEmail`
- `contactPreferenceTelephone`
- `industryCrm`
- `company`
- `companyRelationship`

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`

It is possible to assign `companyGroups` to a user only if the groups are already existing.

- `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.

- `sourceSystem`
- `userType`

Supported values: `public`, `partner`, `customer`, and `employee`. 
Enterprise User Schema Extension

The values of the following attributes are returned when the Enterprise User Schema Extension is used.

- employeeNumber
- costCenter
- organization

Note
Equals the company attribute.

- division
- department

Note
Equals the department attribute from the Core schema.

- manager
  - value
    - Note
      The id of the user’s manager.
  - $ref
    - Note
      The resource URL of the manager.
  - displayName
    - 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.

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
**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.**
- **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",
        "honorificPrefix": "Mr."
    },
    "emails": [{
        "value": "john.smith@sap.com"
    }],
    "addresses": [{
        "type": "work",
        "streetAddress": "100 Universal City Plaza",
        "locality": "Hollywood",
        "region": "CA",
        "postalCode": "90028"
    }]
}
```
"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": "GMT+2",
"groups": [{
"value": "admin"
}],
"displayName": "johnsmith",
"contactPreferenceEmail": "yes",
"contactPreferenceTelephone": "no",
"industryCrm": "Consumer Products",
"companyRelationship": "Partner",
"company": "SFSF",
"department": "Administration",
"password": "Abcd1234",
"userType": "partner",
"active": true,
"passwordStatus": "enabled",
"sendMail": "false",
"mailVerified": "true",
"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"
} },
"urn:sap:cloud:scim:schemas:extension:custom:2.0:User": {
"attributes": [{
"name": "customAttribute1",
"value": "Home Address2"
}]
}
Response

Format: application/scim+json

Response Status Code

Table 61: Success Codes

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
<th>Response Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Created</td>
<td>Indicates success</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.

The URI of the newly created user is in the location header of the HTTP Response.

Response Example

```json
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",  
    "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": "GMT+2",
"userType": "partner",
"active": true,
"groups": [{
  "value": "admin",
  "$ref": "https://<tenant ID>.accounts.ondemand.com/service/groups/55b87ab4e4b0fc7a00bbc070",
  "display": "Administrators"
}],
"displayName": "John Smith",
"contactPreferenceEmail": "yes",
"contactPreferenceTelephone": "no",
"industryCrm": "Consumer Products",
"company": "SFSF",
"department": "Administration",
"mailVerified": "true",
"corporateGroups": [
  {
    "value": "admin"
  }
],
  "employeeNumber": "JohnS",
  "costCenter": "costCenter",
  "organization": "SFSF",
  "division": "Finance",
  "department": "Administration",
  "manager": {
    "value": "P999913",
    "$ref": "https://<tenant ID>.accounts.ondemand.com/service/scim/Users/P999913",
    "displayName": "Jane Watson"
  }
},
"urn:sap:cloud:scim:schemas:extension:custom:2.0:User": {
  "attributes": [
    {
      "name": "customAttribute1",
      "value": "Home Address2"
    }
  ]}
1.7.2.3.4 Update User Resource

The update user method of the SAP Cloud Platform Identity Authentication service 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**
- **name.familyName**
- **userName**
- **addresses[work].streetAddress**
- addresses[work].locality
  
  **Note**
  The attribute equals to city.

- addresses[work].region
  
  **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
  
  **Note**
  The attribute equals to city.

- addresses[home].region
  
  **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
  
  **Note**
  If the `active` parameter and its value are not present in the request, this means that the user status remains unchanged.

- displayName
- contactPreferenceEmail
- contactPreferenceTelephone
- industryCrm
- company
- companyRelationship
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

It is possible to assign companyGroups to a user only if the groups are already existing.

- 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. The following options are possible:
  - If the attribute corporateGroups is provided with a specific value, this value will overwrite the previous one.
  - If the attribute corporateGroups is not provided, this previous value of the attribute will be preserved.
  - If the attribute corporateGroups is provided without a value, the previous value will be deleted.

- password

If attribute password is provided the password will be changed.

- passwordStatus

If the password attribute is provided the passwordStatus can be set to enabled or initial. When this attribute is provided the password attribute is a required parameter.

- userType

Supported values: public, partner, customer, and employee.

- sendMail

The parameter supports boolean values true and false. The default value is true. If you do not want to send an e-mail, the value should be passed with value false.

- mailVerified
**Note**
The parameter supports boolean values `true` and `false`. The default value is `false`.

### Table 62: Possible Combinations

<table>
<thead>
<tr>
<th>sendMail</th>
<th>true</th>
<th>true</th>
<th>false</th>
<th>false</th>
</tr>
</thead>
<tbody>
<tr>
<td>mailVerified</td>
<td>true</td>
<td>false</td>
<td>true</td>
<td>false</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>The user will receive e-mail. He or she will be able to log on.</td>
</tr>
<tr>
<td>The user will receive e-mail. He or she has to click the verification link in the e-mail.</td>
</tr>
<tr>
<td>The user will be able to log on to the application directly.</td>
</tr>
<tr>
<td>The user will not be able to log on.</td>
</tr>
</tbody>
</table>

**Enterprise User Schema Extension**

**Note**
The values of the following attributes are returned when the Enterprise User Schema Extension is used.

- `employeeNumber`
- `costCenter`
- `organization`

**Note**
Equals the `company` attribute from the Core schema.

- `division`
- `department`

**Note**
Equals the `department` attribute from the Core schema.

- `manager`
  - `value`
  - `$ref`
  - `displayName`

**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.
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",
    "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": "GMT+2",
  "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",
  "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"
    }
  },
    "attributes":[
      {  "name":"customAttribute1",
        "value":"Home Address2"
      },
      {  "name":"customAttribute2",
        "value":"Telephone2"
      }
    ]
  }
}

Response

Format: application/scim+json
### Response Status Code

#### Table 63: 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>

**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 247].

### Response Example

**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",
  "name": {
    "givenName": "John",
    "familyName": "Smith",
    "honorificPrefix": "Mr."
  },
  "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": "home"
  }]
}
```
1.7.2.3.5 Delete User Resource

The delete user resource method of the SAP Cloud Platform Identity Authentication service 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 64: Success Codes

<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 247].

Related Information

System for Cross-Domain Identity Management
1.7.2.4 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 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 144], and Edit Administrator Authorizations [page 146].

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 needs to provide in order 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 65:

<table>
<thead>
<tr>
<th>HTTP Method</th>
<th>See</th>
<th>URI</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GET</strong></td>
<td>GET Tenant Texts [page 236]</td>
<td>https://&lt;tenant ID&gt;.accounts.ondemand.com/service/resource?resourceType=RESOURCE_I18N_BUNDLE&amp;locale=&lt;value&gt;</td>
</tr>
<tr>
<td><strong>POST</strong></td>
<td>POST Tenant Texts [page 238]</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 an URL in it. This URL contains the *tenant ID*.

### 1.7.2.4.1 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`
Permissions: You must have a system as administrator 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 144], and Edit Administrator Authorizations [page 146].

URL Parameters

Table 66:

<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>● 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>● Chinese (zh)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Portuguese (pt)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>● Spanish (es)</td>
</tr>
</tbody>
</table>

Request Example

GET /service/resource?resourceType=RESOURCE_I18N_BUNDLE&locale=en

Response

Response Status and Error Codes

Table 67: 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>OK</td>
</tr>
</tbody>
</table>

Table 68: 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>
</tbody>
</table>
### Response Code

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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

```plaintext
class registerSuccess

thankyou=Thank you for registering with {0}
class registerForm

validation.accept.privacy.statement=To accept the privacy statement, click the box above
class accountActivation

ui.label.activationsuccesstext=Thank you for registering and activating your account
ui.label.activationtext=This account can also be used to access other applications
class createForgottenPasswordMail

user=E-Mail

class logon

ui.label=E-Mail

class 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.
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.

class linkSocialSignOnAccount

headline=Link your account with {0}
message.profile=Profile Page
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.

class oauth

network=The selected social sign-on service is currently unavailable. Use a different social sign-on or your credentials to log on.

class 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.
```

### 1.7.2.4.2 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 69: Escape Sequences

<table>
<thead>
<tr>
<th>Value</th>
<th>Escape Sequences</th>
</tr>
</thead>
<tbody>
<tr>
<td>\b</td>
<td>Backspace (ascii code 08)</td>
</tr>
<tr>
<td>\f</td>
<td>Form feed (ascii code 0C)</td>
</tr>
<tr>
<td>\n</td>
<td>New line</td>
</tr>
<tr>
<td>\r</td>
<td>Carriage return</td>
</tr>
<tr>
<td>\t</td>
<td>Tab</td>
</tr>
<tr>
<td>&quot;</td>
<td>Double quote</td>
</tr>
<tr>
<td>\</td>
<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

**Content-Type:** application/json

**Permissions:** You must have a system as administrator 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 144], and Edit Administrator Authorizations [page 146].

**Request Example**

```json
{
    "resourceType": "RESOURCE_I18N_BUNDLE",
    "locale": "en",
    "contentType": "text/html;charset=UTF-8",
    "data": "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.activationsuccessstext=Thank you for registering and activating your account
    accountActivation.ui.label.activationtext=
    createForgottenPasswordMail.user=E-Mail
    logon.ui.label.user=E-Mail
    logon.ui.label.forgotpassword=Forgot/Reset Password
```
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.

To link your account with a social sign-on account, click one of the social network buttons next time you log on.

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.

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.

The site you are attempting to access requires your password. Enter your password and click Continue.

The selected social sign-on service is currently unavailable. Use a different social sign-on or your credentials to log on.

This Google account has not joined Google yet. Join Google and link your account, or log on with an existing account.

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.

Response

Response Status and Error 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>

<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</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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 cli-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ent.</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>
1.7.2.5 Change Master Data Texts

The Change Master Data Texts REST API of SAP Cloud Platform Identity Authentication service 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 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 144], and Edit Administrator Authorizations [page 146].

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 72: Predefined Master Data Texts

<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>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.". If you overwrite the key value pair with "03=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 73:

<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 243]</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 246]</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.

1.7.2.5.1 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 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 144], and Edit Administrator Authorizations [page 146].

URL Parameters

Table 74:

<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:</td>
</tr>
<tr>
<td>locale</td>
<td>Yes</td>
<td>The locale of the resource.</td>
<td>The default languages are:</td>
</tr>
</tbody>
</table>

Use:
- RESOURCE_MD_SALUTATIONS
- RESOURCE_MD_FUNCTIONS
- RESOURCE_MD_DEPARTMENTS
- RESOURCE_MD_RELATIONS
- RESOURCE_MD_INDUSTRIES
- RESOURCE_MD_LANGUAGES
- RESOURCE_MD_COUNTRIES

- Chinese (zh)
- Russian (ru)
- Portuguese (pt)
- Polish (pl)
- Dutch (nl)
- Korean (ko)
- Japanese (ja)
- Italian (it)
- French (fr)
- Spanish (es)
- English (en)
- German (de)
- Welsh (cy)

Request Example

GET /service/resource?resourceType=RESOURCE_MD_SALUTATIONS&locale=en
Content-Type: application/json
Response

Response Status and Error Codes

Table 75: 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. OK</td>
</tr>
</tbody>
</table>

Table 76: 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 than the original in the master data file. It is not necessary to be in sequence.

```json
{
  01=Ms.,
  05=Mr.
}
```
1.7.2.5.2 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 77: Escape Sequences

<table>
<thead>
<tr>
<th>Value</th>
<th>Escape Sequences</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>\b</code></td>
<td>Backspace (ascii code 08)</td>
</tr>
<tr>
<td><code>\f</code></td>
<td>Form feed (ascii code 0C)</td>
</tr>
<tr>
<td><code>\n</code></td>
<td>New line</td>
</tr>
<tr>
<td><code>\r</code></td>
<td>Carriage return</td>
</tr>
<tr>
<td><code>\t</code></td>
<td>Tab</td>
</tr>
<tr>
<td><code>&quot;</code></td>
<td>Double quote</td>
</tr>
<tr>
<td><code>\</code></td>
<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 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 144], and *Edit Administrator Authorizations* [page 146].

**Request Example**

```json
https://<tenantId>.accounts.ondemand.com/service/resource/SAP_DEFAULT
Content-Type: application/json
Body:
{
  "resourceType": "RESOURCE_MD_DEPARTMENTS",
  "locale": "en",
}..."
Response

Response Status and Error Codes

Table 78: 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>

Table 79: 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>

1.7.2.6 General Error Codes

The following table lists error codes that may be returned from any method on any resource URI.

Table 80: General 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>
</tbody>
</table>
### 1.7.3 Add Logon Overlays in Customer Applications

This document describes how service providers that delegate authentication to SAP Cloud Platform Identity Authentication service 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 60].

#### 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 a fullscreen window.

To open the logon page of the application in an overlay instead of in a fullscreen window 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.

<table>
<thead>
<tr>
<th>Response Code</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>
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:
     
     ```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:
     
     ```html
     <script src="https://<tenant ID>.accounts.ondemand.com/ui/resources/javascripts/SAP_IDS.js" />
     ```

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 ○ the name of the resource is not important</td>
</tr>
</tbody>
</table>

   ```html
   <a href="/login.jspa" rel="IDS_Login">Log in</a>
   ```

**Next Steps**

Protect applications against clickjacking when using overlays. For more information, see Configure Clickjacking Protection [page 250].
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

```html
<script src="https://<tenant ID>.accounts.ondemand.com/ui/resources/javascripts/
SAP_IDS.js?locale=en_GB" />
```

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 80].**
- **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:**

Sample Code

```javascript
function_messageHandler(oEvent){
    if(oEvent.data=='SAPFrameProtection*require-origin'){
        oEvent.source.postMessage('SAPFrameProtection*parent-origin','*');
    }
}
```
Related Information

Add Logon Overlays in Customer Applications [page 248]

1.7.5 Troubleshooting for Developers

This section is to help developers with solutions to the REST API response codes.

Error Codes

Table 81:

<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>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 email 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>
</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 275]
1.8 Security

This document contains recommendations about how administrators should secure SAP Cloud Platform Identity Authentication service.

Before You Start

Before you secure Identity Authentication, you should protect the cloud application that trusts Identity Authentication. For more information about protecting SAP Cloud Platform applications, see Securing Applications.

User Administration

Set user permissions in accordance with the scenario you are configuring. For more information, see Scenarios [page 20].

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 67].

User Authentication

Identity Authentication protects your users during authentication in the following ways:

- With SAML 2.0
  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. You have to use the certificate when implementing REST APIs for your application. For more information, see the REST API configurations in Developer Guide [page 194].

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 SSL 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 Password Policies [page 102].

Session Security

Session cookies in Identity Authentication are protected with a Secure Socket Layer (SSL) and with the Secure and HttpOnly attributes. You do not need to make any additional configurations for Identity Authentication.

Network and Communication Security

All communication channels are protected with SSL, and you should configure the cloud application to use SSL 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 173].

Related Information

Security on SAP Community Network
SAP Data Center
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 255]
Integration with SAP Web IDE [page 262]
Integration with SAP Document Center [page 267]
Integration with SAP Identity Management 8.0 [page 272]
Integration with Microsoft Azure AD [page 272]
Configure SAP SuccessFactors Business Execution (SAP SuccessFactors BizX) SSO to use SAP Cloud Platform Identity Authentication

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.

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.
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 an 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 account member of the SAP Cloud Platform cockpit.

**Note**

For more information how to add other users for the account, see [Managing Members](#).

The cockpit is the central point for managing all activities associated with your cloud-based business applications. For more information about the cockpit, see [Cockpit](#).

To deploy applications on SAP Cloud Platform and to make configurations in the cockpit, you need an account that corresponds to your role. For more information, see [Getting an Account](#).

## Access to SAP Cloud Platform Identity Authentication Service

SAP Cloud Platform Identity Authentication service 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 an 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.

**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, as 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](#).
1.9.1.1 Configure SAP Cloud Platform

Prerequisites

- You have an account for SAP Cloud Platform.
  For more information, see Getting an 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.

i Note

If you want to use SAP Cloud Platform in a productive landscape, 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 landscape 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 84:

<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: ID Federation with a Identity Authentication Tenant</td>
</tr>
</tbody>
</table>

i 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 76]
2. Use this metadata to configure the trust on SAP Cloud Platform. For more details about this configuration, see ID Federation with the Corporate 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 account. For more information, see Creating Accounts. Once you have created the new account, add the tenant of Identity Authentication in the new account, and repeat the procedure in the table above to set the trust for each account.

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: ID Federation with a Identity Authentication Tenant.
- You have downloaded the metadata for SAP Cloud Platform as a service provider (SP). For more information, see ID Federation with the Corporate Identity Provider.

Context
This configuration is needed 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 257].
Procedure

1. Set the trust with SAP Cloud Platform. For more details, see Configure a Trusted Service Provider [page 35]
2. Optional: Customize the settings for the application. For more information, see Configure Applications [page 26].

1.9.1.3 Configure Assertion Attributes Mapping

You have to specify how the assertion attributes are sent to SAP Cloud Platform in the SAML 2.0 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 *SAML 2.0*, 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 38]

2. 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 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 SAML Assertion.

The Principal Attribute field is the user attribute that the users will have at SAP Cloud Platform.

6. Save your changes.

Related Information

ID Federation with the Corporate Identity Provider
1.9.1.4 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 SAP Cloud Platform Identity Authentication service 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.

   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 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 an account for SAP Cloud Platform. For more information, see Getting an 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 ID Federation with a Identity Authentication Tenant.
- You have set the trust with SAP Cloud Platform. For more details, see Configure a Trusted Service Provider [page 35].
- 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 60].
- 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 80].
- 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 122].

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 263].
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 264].

### 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. Access the SAP Cloud Platform with the cockpit administrator role.
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.

![Application Permissions](image)

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 122]. 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. Access the SAP Cloud Platform with the cockpit administrator role.

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 SAP Cloud Platform Identity Authentication service 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 SAP Cloud Platform Identity Authentication service 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.

   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 an account for SAP Cloud Platform. For more information, see Getting an 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 ID Federation with a Identity Authentication Tenant.
- You have set the trust with SAP Cloud Platform. For more details, see Configure a Trusted Service Provider [page 35].
- 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 80]. 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 122].
- 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
- Assign Groups to Roles
- Assign Default Groups

Assign Users to Roles

Context

Assign the respective roles for SAP Document Center to individual users of Identity Authentication.

Procedure

1. In the SAP Cloud Platform cockpit with the cockpit administrator role.

   ![Note]
   You can log on to the cockpit at the URLs given below. Use the relevant URL for your associated region:
   - Europe: https://account.eu1.hana.ondemand.com/cockpit
   - United States: https://account.us1.hana.ondemand.com/cockpit
   - Asia-Pacific: https://account.ap1.hana.ondemand.com/cockpit

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.
Note
For more information how to check the User ID, see List and Edit User Details [page 122]. 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 129].
   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 38].

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 SAML 2.0 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 SAML 2.0, 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 38]

2. 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 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 SAML Assertion. The Principal Attribute field is the user attribute that the users will have at SAP Cloud Platform.

6. Save your changes.

Related Information

ID Federation with the Corporate 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 HANA Cloud Platform Identity Authentication. For more information, see SAP HANA Cloud Platform Identity Authentication.

The integration between Identity Authentication and Azure AD is to provide single sign-on (SSO) between applications that use Azure AD as an authenticating identity provider and applications that use Identity Authentication as a 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 Get Started [page 19].

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.

⚠️ Note

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.

➡️ Tip

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 166].

For this scenario, the configurations are made in the administration console for Identity Authentication and in Azure classic portal.

Configure Microsoft Azure AD as Corporate Identity Provider at SAP Cloud Platform Identity Authentication Service

Prerequisites

- You have a subscription for Identity Authentication. For more information how to get Identity Authentication, see Get Started [page 19].

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.

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

   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. 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

Find the information necessary for the manual configuration in the metadata of Azure AD.

Next Steps

1. Choose MS ADFS 2.0 as the type for the configured corporate identity provider. For more information, see Choose Identity Provider Type [page 163].

2. Select the configured identity provider as the authenticating identity provider for the desired application. For more information, see Choose Identity Provider for an Application [page 73].

Configure Microsoft Azure AD

Context

For the configuration of Microsoft Azure AD see Tutorial: Azure Active Directory integration with SAP HANA Cloud Platform Identity Authentication.
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 create an Incident on SAP Support Portal with a component BC-IAM-IDS.

SAP Community Network

You can start a discussion in the Security space.

Related Information

Troubleshooting for Administrators [page 180]
Troubleshooting for Developers [page 251]

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 Release Notes for Identity Authentication [page 5] published regularly.

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

Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP’s gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP’s current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP’s gross negligence or willful misconduct. All links are categorized for transparency (see: http://help.sap.com/disclaimer).